NIST Grant/Contractor Report
NIST GCR 23-039

American Competitiveness Of a More Productive Emerging Tech Economy Act (The American COMPETE Act)

Studies of the State and Impact on the United States Economy of Artificial Intelligence, Internet of Things and Internet of Things in Manufacturing, Quantum Computing, Blockchain Technology, New and Advanced Materials, Unmanned Delivery Services, and Three-Dimensional Printing

Final Report

The National Institute of Standards and Technology (NIST) on behalf of the Secretary of Commerce, with support from the Institute for Defense Analyses Science and Technology Policy Institute (IDA STPI), the Quantum Economic Development Consortium (QED-C), and the Federal Trade Commission (FTC)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.GCR.23-039

NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Grant/Contractor Report
NIST GCR 23-039

American Competitiveness Of a More Productive Emerging Tech Economy Act (The American COMPETE Act)

Studies of the State and Impact on the United States Economy of Artificial Intelligence, Internet of Things and Internet of Things in Manufacturing, Quantum Computing, Blockchain Technology, New and Advanced Materials, Unmanned Delivery Services, and Three-Dimensional Printing

Final Report

The National Institute of Standards and Technology (NIST) on behalf of the Secretary of Commerce, with support from the Institute for Defense Analyses Science and Technology Policy Institute (IDA STPI), the Quantum Economic Development Consortium (QED-C), and the Federal Trade Commission (FTC)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.GCR.23-039

July 2023

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

NIST GCR 23-039
July 2023

Disclaimer

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Copyright, Use, and Licensing

How to Cite this NIST Technical Series Publication

The National Institute of Standards and Technology on behalf of the Secretary of Commerce, with support from the Institute for Defense Analyses Science and Technology Policy Institute, the Quantum Economic Development Consortium, and the Federal Trade Commission (2023) American Competitiveness Of a More Productive Emerging Tech Economy Act (The American COMPETE Act) – Final Report. National Institute of Standards and Technology, Gaithersburg, MD, NIST GCR 23 039. https://doi.org/10.6028/NIST.GCR.23-039

Abstract

Under DIVISION FF, Title XV, §1501 of the Consolidated Appropriations Act of 2021 (Public Law 116-260)—the "American Competitiveness Of a More Productive Emerging Tech Economy Act" (the "American COMPETE Act")—the United States Congress directed the Secretary of Commerce, in coordination with the Federal Trade Commission and other agencies, to prepare studies on the following technology areas that are expected to be critical to the global competitiveness, economic growth, and national security of the United States in the coming decades: Artificial Intelligence, Internet of Things and Internet of Things in Manufacturing, Quantum Computing, Blockchain Technology, New and Advanced Materials, Unmanned Delivery Services, and Three-Dimensional Printing (included here as Additive Manufacturing). This document compiles chapters addressing each technology area.

Keywords

Additive Manufacturing; Artificial Intelligence; Internet of Things and Internet of Things in Manufacturing; Quantum Computing; Blockchain Technology; New and Advanced Materials; Unmanned Delivery Services; Additive Manufacturing; Three-Dimensional Printing; Economic Growth; Global Competitiveness; National Security; Economic Security.

Table of Contents

Acknowledgments

On behalf of NIST: Kevin A. Kimball; Matthew S. Hoehler; Anne Lane; Elham Tabassi; Connie LaSalle; Kevin Jurrens; Mark VanLandingham; James Warren; Naomi Lefkovitz; Nada Golmie; Chris Greer; Matthew Scholl; Dylan Yaga; Kevin Stine; Andrew Wilson; Karen Reczek.

On behalf of IDA and STPI: William E. J. Doane; Keith W. Crane; Kevin Garrison; Emily R. Grumbling; Luba Katz; Howard R. Last; Margaret B. Murphy; Thomas D. Olszewski; Todd D. Ringler; Jeffrey A. Snyder; Olivia S. Sun; Jessica G. Swallow; Steven P. Wartik; Gifford J. Wong; Jacob B. Bartel; Nathan N. L. Dinh; Marilyn G. Harbert; Gabriella G. Hazan; Matthew A. Ishimaru; Javier F. Ortiz; Logan M. Pratico; Casey C. Roepke; Erin N. Saybolt; Sarah E. Swiersz; Andrew B. Ware; Rina L. Zhang.

And to those who responded to the public request for information or to requests for comments from Federal Agencies.

Artificial Intelligence

Chapter Contents

List of Tables

1. Artificial Intelligence

Summary

In the Consolidated Appropriations Act of 2021 (Public Law 116-260, Division FF, Title XV, §1501), Congress tasked the National Institute of Standards and Technology (NIST) to prepare a series of reports on critical and emerging technologies and their impact on the U.S. economy, including artificial intelligence (AI). NIST is the lead author of this report, and began working on this report before the latest generation of advanced AI systems were made public. As a result, this report does not necessarily capture the Administration's latest views and initiatives on AI. In addition, given the speed with which advancements and the commercial use of AI is evolving, this report does not necessarily reflect all of the Federal Trade Commission's (FTC) recent enforcement activities and views involving AI. As prescribed in the legislation, this chapter addresses:[1]

- industry sectors that implement and promote the use of AI,
- public-private partnerships (PPPs) focused on promoting adoption of AI,
- industry-based bodies developing and issuing standards for AI,
- the status of mandatory and voluntary AI standards, both Federal and industry-based,
- Federal agencies with expertise and jurisdiction in industry sectors implementing AI,
- interagency activities relevant to AI,
- Federal regulations, guidelines, mandatory standards, voluntary standards, and other policies concerning AI implemented by Federal agencies and industry-based bodies,
- Federal resources that exist for consumers and small businesses to evaluate the use of AI,
- risks to the AI supply chain and marketplace,
- AI-related risks to the national security, including economic security,[2] of the United States, and
- emerging risks and long-term trends in AI.

[1] AI technologies, uses, markets, and policies are developing at a rapid rate. While this chapter aims to provide complete information, it is likely that some content will no longer be current and that some recent Administration activities might not be reflected herein by the time of publication.

[2] The Consolidated Appropriations Act of 2021 refers to "economic and national security," and economic security is understood to be part of national security for the purposes of authorities such as the Consolidated Appropriations Act of 2021 and Section 232 of the Trade Expansion Act of 1962 (Public Law 87-794).

1.1. Overview

Advances in computing hardware and algorithms, along with increasing availability of large volumes of data, have enabled major progress in the field of artificial intelligence (AI) over the past few decades. In order to realize the potential benefits of this rapidly advancing technology area, it is imperative to mitigate both the current and potential risks posed by AI to individuals, society, and national security.

1.1.1. Definition of "Artificial Intelligence"

The term "artificial intelligence" can refer to a discipline and its sub-disciplines,[3] the presence of "intelligent" attributes in an artificial system, AI technologies, or AI systems (specific information technology systems that use AI technologies for their applications). NIST's working definition of "AI system," adapted from the Organisation for Economic Co-Operation and Development (OECD), is: "an engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy."[4] Statutory definitions of AI have been codified in the National AI Initiative Act of 2020 and in the FY2023 National Defense Authorization Act (full definitions are provided in Box 1 in section 1.2.2 of this chapter).

"AI" does not refer to a single technology; rather, AI systems can comprise or leverage a range of different tools and technologies, including algorithms, software, hardware, design patterns, and standards that enable them to carry out tasks that would otherwise require intelligent human behavior. These tasks can include perceiving real and virtual environments; abstracting such perceptions into models through analysis in an automated manner; and using model inference to formulate options for information or action.[5] There is currently no rigid threshold for what is or is not AI, and the term may be used loosely in practice, but it is generally inferred that AI requires advanced algorithms, software, or hardware, and typically requires substantial data to develop—especially for ML models, which "learn" parameters by optimization of model parameters upon application to representative data.

AI systems and technologies are already having a huge influence on the global and U.S. economies. AI research, development, and deployment have made major strides (although phased, rather than continuous ones) since the field emerged in 1956 and progress has accelerated over the past two decades—largely due to improvements in computational capacity, the availability of large quantities of data used to develop AI models, and algorithmic advances. The field continues to progress rapidly such that parts of this chapter may be outdated by the time it is released. In recent years, the private sector has played an increasingly dominant role in the R&D that leads to deployed AI

[3] E.g., natural language processing, machine learning, deep learning, reinforcement learning, planning, plan recognition, image understanding, navigation, and more.

[4] Adapted from OECD Recommendation on AI 2019 and ISO/IEC 22989:2022. This definition is very similar to that defined in the National AI Initiative Act, NAIIA Division E, Sec. 5001 - 15 U.S.C. §9401(3).

[5] NAIIA Division E, Sec. 5001 - 15 U.S.C. §9401(3)

technologies and systems. While the United States has historically led the world in AI progress, the global AI technology landscape is highly competitive.

AI systems and technologies have great potential to be applied for use cases with economic and societal benefit. However, the growing adoption of AI could also have significant societal harms, including risks to individual privacy, civil rights, and civil liberties; national security, market consolidation and harms to competition; labor market shifts; and environmental costs. In particular, the development and deployment of AI can meaningfully impact the American public's rights, opportunities, and access to critical resources and services. Focusing on near-term benefits of AI without establishing proper safeguards for AI or planning for longer-term needs could lead to substantial harms or limit future benefits. Therefore, maintaining U.S. leadership in AI for the benefit of all Americans requires ensuring that AI technologies are developed and deployed in a manner that protects privacy, civil rights, civil liberties, human safety, and the environment as a clear national priority.

1.1.2. Industry Sectors and Public-Private Partnerships

Use of AI is widespread: every U.S. industry sector contains some firms that implement or promote the use of AI. Public-private partnerships to accelerate AI research and development (R&D) and promote the adoption and use of AI include the National AI Research Institutes, led by the National Science Foundation (NSF). As of December 2022, 18 institutes have been funded in whole or in part by the U.S. Department of Agriculture (USDA), the Department of Education (ED), the Department of Defense (DoD), the Department of Homeland Security (DHS), and NSF, with some receiving private sector support. These institutes are working to advance AI R&D on topics ranging from the foundations of machine learning (ML) to AI for environmental science. Each institute is led by an academic or other research organization, typically with multiple additional partners drawn from several sectors, including companies, Federal or national labs, nonprofit organizations, educational institutions, research organizations, and non-Federal government organizations.

1.1.3. Industry-Based Standards

There are numerous Standards Development Organizations (SDOs) active across the information and communications technology ecosystem that create widely-used voluntary consensus standards—however, they are not solely industry-based. Many of these SDOs are engaged with private and public sector stakeholders working on the development of standards relevant to AI. Because many AI methods are already widely or increasingly deployed, numerous voluntary standards have been published or are under development for AI, addressing AI concepts, definitions, and terminology; governance, ethical uses, and social concerns; security, privacy, and trustworthiness; environmental efficiency, engineering practices, reference architectures; and testing, evaluation, validation, and verification (TEVV)—both in general and for specific AI areas and applications. SDOs have been extremely active in these areas, including the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and the Institute of Electrical and Electronics Engineers Standards Association (IEEE SA). The

American National Standards Institute (ANSI) serves as the U.S. member body to the ISO, and the U.S. National Committee represents the United States in IEC. Other entities involved in AI standards include the International Telecommunication Union (ITU) and the European Telecommunications Institute (ETI). A variety of not-for-profit or sector-specific groups and trade associations have begun working on voluntary standards, certifications, common practices, or guidance for specific AI applications or use-cases, and private sector entities often develop de facto standards that may become more broadly adopted and subsequently inform formal standards development processes.

1.1.4. Federal Government Standards and Regulations

Today, few Federal regulations explicitly address AI technologies. However, many Federal agencies have authority to regulate commercial use of AI technologies under other existing authorities or due to their general jurisdiction, including related to data and IT use more broadly. While there is no comprehensive regulatory framework governing the use of AI in the United States, several policy documents have laid out principles for commercial and government use and stewardship of AI. For example, the Office of Management and Budget (OMB) Memorandum M-21-06 ("Guidance for Regulation of Artificial Intelligence Applications") provides guidance for Federal oversight of public and private sector AI-related activities, recommending non-regulatory approaches where possible. Executive Order 14091 ("Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government"), released February 16, 2023, calls on agencies to enhance protections for the public against AI bias and algorithmic discrimination, create and use AI systems to advance equity consistent with applicable law, and consult with agency civil rights offices in decisions related to AI and automated systems.

The White House's 2022 *Blueprint for an AI Bill of Rights* lays out principles to guide the design, use, and deployment of AI systems and protect the American public's civil rights, civil liberties, privacy, equal opportunities, and access to critical resources or services. Executive Order 13960 ("Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government"), the Department of Defense's *Ethical Principles for AI* and *Responsible AI Strategy and Implementation Pathway*, and the Intelligence Community's *Principles of AI Ethics* and *AI Ethics Framework* provide principles and frameworks to guide the Federal use of AI. Many other Federal departments and agencies are also instituting AI governance, adapted from these higher-level frameworks, to address specific needs within their organization. As announced in May 2023, OMB will be releasing draft policy guidance on the use of AI systems by the U.S. Government for public comment.

Individual Federal agencies are also engaged in establishing regulatory guidance or frameworks for the use of AI or algorithms. For example, the Food and Drug Administration (FDA) is working to advance a regulatory and oversight framework for the use of AI-based software as a medical device, and has released guidance related to regulation of certain medical devices and software that could leverage AI. The Consumer Financial Protection Bureau (CFPB) has clarified that a written explanation of why adverse actions are taken against an applicant must be provided even if the decision was made using a complex algorithm. The FTC released an advanced notice of proposed rulemaking under Section 18 of the FTC Act to examine whether rules addressing algorithmic decision making are appropriate. The Equal Employment Opportunity Commission launched an Artificial Intelligence and Algorithmic Fairness initiative to help ensure that AI, ML, and other emerging technologies comply with EEOC-enforced laws when used in hiring and other employment decision making, and has issued two technical assistance publications addressing AI implications under the federal equal employment opportunity statutes. A variety of other, non-AI-specific Federal standards or regulations—for example, such as the requirement that technology be accessible to persons with disabilities in accordance with Section 508 of the Rehabilitation Act—may apply to AI use cases.

The United States also engages with other nations and international organizations regarding research, development, deployment, principles, and standards for AI. Key efforts have been led by the OECD and the U.S.-EU Trade and Technology Council and are intended to help lay a common foundation for international coordination and national policies.

1.1.5. Interagency Activities

The U.S. Government coordinates AI-related activities and decision making across agencies through several entities. As directed by the National AI Initiative Act of 2020, the National AI Initiative Office (NAIIO) serves as a point of contact for Federal AI activities. NAIIO collaborates with the Networking and Information Technology R&D (NITRD) National Coordination Office on AI R&D programs, and supports interagency coordination efforts. Several committees and subcommittees of the White House National Science and Technology Council (NSTC) convene agency representatives for strategic planning and information sharing, including the Select Committee on Artificial Intelligence, the Subcommittees on Machine Learning and AI (MLAI-SC) and Networking and Information Technology R&D (NITRD), the NITRD Interagency Working Group on AI, and the NITRD Video and Image Analytics Team. NSTC, NAIIO, and NITRD entities have released a variety of AI R&D strategic planning documents and budget supplements that were coordinated across Federal agencies; these publications and a larger list of Federal AI R&D and related activities are available via ai.gov.

The AI Standards Coordination Working Group of the Interagency Committee on Standards Policy, co-chaired by NIST and DHS, works to promote effective and consistent Federal AI policies related to AI standards. The General Services Administration's (GSA) AI Center of Excellence partners directly with Federal agencies and industry to support the development of AI-based solutions. GSA's AI and Robotic Process Automation Communities of Practice bring together practitioners from across the Federal Government to develop and share best practices and lessons learned. GSA's Digital Worker Identity Playbook is a practical guide to manage digital worker identities. OMB—including its Office of the Federal Chief Information Officer, the Chief Information Officer Council, and the Office of Information and Regulatory Affairs—also facilitates general information sharing and coordination of Federal agency activities related to AI. The White House Office of Science and Technology Policy (OSTP) together with the Domestic Policy Council coordinate across agencies around instituting safeguards or ensuring compliance with requirements to protect the American public from the potential harms of AI, with a focus on equity. The Equal Employment Opportunity Commission (EEOC) and the Department of Labor's (DOL) Office of Federal Contract Compliance Programs (OFCCP) are collaborating on an initiative to promote equal employment opportunity for workers and job applicants, including in the use of automated systems. Finally, many agencies have a Responsible AI Official (RAIO) to manage requirements around trustworthy AI and serve as an agency's point of contact. RAIOs regularly communicate with and serve as subject matter experts on trustworthy AI and other Federal AI initiatives.

1.1.6. Federal Government Resources

NIST has released several documents intended to support individuals and groups working on or deploying AI systems, including the draft AI Risk Management Framework (final release anticipated in 2023) and the special publication *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence* (NIST SP 1270). In addition, NIST has published other frameworks that could be leveraged in the context of AI. These include: The Cybersecurity Framework; the Secure Software Development Framework; and the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management. The Federal Trade Commission has released a report, business guidance, and blog posts addressing AI use by businesses, including policy and legal context and key principles and approaches for responsible AI use. GAO’s AI Accountability Framework provides principles and practices as recommendations for Federal agencies and other implementers of AI. The principles and associated practices outlined in the White House’s *Blueprint for an AI Bill of Rights* are also a resource for entities developing or deploying AI systems on protecting the American public from the potential harms of AI and other automated systems.

NIST and other Federal agencies have also made available several technical tools and other resources for evaluation of AI algorithms, such as the Face Recognition Vendor Test for characterizing performance of automated face recognition technologies. A wide variety of federally funded R&D testbeds could be leveraged to develop or test AI systems, or to experiment with their application in specific domain areas; a comprehensive list is available via the AI Researchers Portal at ai.gov. As called for in the National AI Initiative Act, the National AI Research Resource (NAIRR) Task Force developed a roadmap and implementation plan for establishing a new national cyberinfrastructure to broaden access to data, computational, and other resources in order to strengthen and democratize the U.S. AI innovation ecosystem. Other efforts to improve access to Federal data for approved R&D purposes include the COVID-19 Open Research Dataset (CORD-19) and the National Secure Data Service demonstration program.

1.1.7. Risks to the AI Supply Chain and Marketplace

The AI innovation ecosystem relies on human talent, specialized or large quantities of data, software and algorithms, and cloud or on-premise computing capabilities driven by general-purpose and AI-specific computer hardware. While the hardware used for developing, training, and deploying AI systems faces traditional supply-chain risks, AI software and algorithms are inherently information-based rather than physical and thus belie many traditional notions of supply chain. For example, software and precursor functions or code segments—while often sourced from different entities—can be shipped electronically and easily duplicated, unlike physical goods.

The vibrancy of the U.S. AI innovation ecosystem depends on the availability of a robust pool of technical talent for AI research, development, and deployment in all sectors. However, today much of the Nation's talent is drawn to the private sector—especially the largest technology companies, which can offer higher salaries and more sophisticated AI R&D resources than other organizations, limiting the concentration of expertise in academia needed to develop future talent and in smaller companies that might diversify the landscape. Furthermore, current immigration law makes it difficult for U.S.-trained foreign talent to stay and work in the United States after completing their degrees. Finally, failure to nurture, educate, and train the Nation's full diversity of talent to contribute to the AI disciplines not only constrains the AI workforce supply but also risks exclusion of perspectives and knowledge that can help to identify and mitigate bias and discrimination and other individual or societal harms that could be introduced across the stages of AI research, development, and deployment.

The AI software supply chain faces risks associated with both open-source and proprietary software. The wide availability of open-source code, libraries, or other software elements lowers the barrier to developing AI systems and supports wide vetting of code, including by effectively crowd-sourcing the identification and correction of flaws or security vulnerabilities. However, open-source software can introduce security risks into AI systems if the vulnerabilities are not actively detected and corrected. On the other end of the spectrum, keeping code or data proprietary can make it challenging to properly audit the performance of an AI system.

The AI hardware ecosystem also faces several risks. Currently, the United States relies heavily on microelectronics manufacturers in foreign countries; geopolitical or other disruptions in those regions would affect the U.S. AI industry. The Nation has limited manufacturing capacity for microelectronics in general and relies entirely on foreign manufacture of the most cutting-edge microelectronics systems—though recent or ongoing Federal initiatives, such as the Creating Helpful Incentives to Produce Semiconductors (CHIPS) for America Act (passed as part of the FY 2021 National Defense Authorization Act), aim to bolster this capacity.

Decades of advances in computational power have enabled the development of the large, powerful ML models available today. Training and using such models can consume a large amount of energy, which comes with environmental and financial costs—and current advances in computer hardware capacity are lagging increases in computational resource demands for further model improvements. Failure to seek alternate pathways for enhancing AI performance may limit progress in the near or long term. The high demand for and cost of computational resources for AI (especially in the case of large AI models) also raises the barrier to participation among those with limited resources, which could result in concentrating AI R&D and commercialization among the largest technology companies. Similarly, high quality data required for AI R&D, which can include proprietary data, are not equally available to all. In particular, large companies with resources to gather and curate data for AI, or that collect or have available large quantities of data as a result of their business functions, have an inherent advantage in training ML models. At the same time the use of data—especially data about individuals—present risks to privacy, civil rights and civil liberties. In January 2023, a Federal Task Force co-chaired by NSF and OSTP released a roadmap and implementation plan for establishing a National AI Research Resource (NAIRR) to help strengthen democratize the U.S. AI innovation ecosystem in way that protects privacy, civil rights, and civil liberties by making resources such as compute, data, software, training, and testing capabilities broadly available to researchers affiliated with U.S. academic and nonprofit organizations, and some small- and medium-sized U.S. businesses that receive Federal R&D funding.

Deployed AI systems may not always prove trustworthy in practice. Major failures could cause harms to consumers or the public. Such failures or potential public distrust in AI technologies—warranted or not—could affect demand for and adoption of AI. Ongoing development of principles and frameworks for ethical, fair, equitable, secure, and trustworthy AI aim to help AI stakeholders mitigate risks. Some regions of the world and within the United States have instituted policies to help protect the privacy of individuals and mitigate risks of widespread data collection and use, such as the General Data Protection Regulation in the European Union (EU) and similar legislation in States such as California, Colorado, and Virginia. However, variation in legal or regulatory policies for data protection can create complicated compliance regimes or uncertainty for the private sector. Current antitrust law is flexible enough to address many of the issues presented by the rapid rate of AI adoption, but may face challenges in certain areas where new forms of tacit collusion are emerging.

1.1.8. Risks to the American Public’s Civil Rights, Civil Liberties, and Privacy

AI systems have the potential to meaningfully impact the American public's rights, opportunities, and access to critical resources and services. Decisions made in the research, design, development, deployment, funding, acquisition, and governance of AI technologies can have implications for the public’s civil rights, civil liberties, and privacy in a variety of ways. Following a set of robust safeguards and procedures—such as those outlined in the NIST *AI Risk Management Framework*—can help mitigate or prevent harms associated with AI systems. The White House’s 2022 *Blueprint for an AI Bill of Rights* provides five key principles and associated practices for protecting the privacy, civil rights, and civil liberties of everyone in America against AI-related risks.

The dependence of common AI methods—in particular, Deep Learning (DL)—on large amounts of data for training and for TEVV is a particular source of concern. Key risks span questions of consent to collection, sharing, and use of data for AI R&D and deployment, the potential for incomplete, biased, or poorly curated data sets and models to lead to incorrect or harmful model assumptions or development, and the potential for AI models to perpetuate or exacerbate historical bias reflected in training or TEVV data. Biases in data and algorithms can lead to cumulative harm, disparate impacts, or unlawful discrimination against individuals or groups from protected classes, such as race, ethnicity, religion, disability status, gender, or age. In addition, the combination of data from multiple sources to create suitable training sets could uncover confidential information, data otherwise kept confidential could be "leaked" or reconstructed from deployed AI models, and AI models could infer sensitive information and cause harm or lead to unfair or discriminatory practices. These risks are most pronounced with sensitive data or "fragile" models from which sensitive data may be inferred.

AI systems can be opaque or not easily explainable, which can make oversight challenging if they are ineffective or cause disparate outcomes. AI deployed for decision-making—especially for access to critical resources or services—without proper validation, monitoring, or oversight, risks loss of individual or community agency or recourse for adverse outcomes. AI models are also vulnerable to discordant or malicious inputs and other manipulation—either intentional or inadvertent—whose outputs could lead to harms.

1.1.9. Risks to the National Security, Including Economic Security, of the United States

Weaknesses within the AI ecosystem pose inherent risks and could be exploited by foreign governments or third parties in a way that harms U.S. national security, including economic security. First, the broad applicability and power of AI presents opportunities for AI to be misused, designed, or altered for malicious purposes—whether at the system, model, algorithm, or data level. For example, there are substantial concerns about the use of AI to surveil and discriminate against marginalized or vulnerable groups, promote misinformation, or advance disinformation campaigns. Incorporation of AI into cyber or armed conflicts poses risks of escalation. Prevailing AI standards, norms, principles, and practices will influence the extent to which AI helps to uphold or undermine human rights and democratic principles around the world.

AI-specific cybersecurity vulnerabilities could be exploited by adversaries to disrupt a critical function or compromise system safety or security, or to steal sensitive information, with economic and security implications commensurate with the criticality of the use case and context. Such vulnerabilities could arise incidentally or be deliberately created by a bad actor through compromise of some input to the AI's development—such as by maliciously altering hardware, data, or code—on top of the risks associated with unintentional system failure. AI also introduces additional complexity into systems, which can sometimes make it difficult to diagnose and mitigate attacks and failures.

In addition to compromising key inputs to the development of an AI system, a foreign government or third party could also reduce access to AI R&D resources within the United States—for either economic or adversarial reasons—and limit the competitiveness or capabilities of U.S. entities in almost any domain because of the widespread applicability of AI. Economic or strategic disadvantages could result from decisions by entities that control key AI resources—such as hardware, software, data, or talent—to retain them for their own use or limit their availability to others. On the human resources front, policies that limit or aim to reduce the AI and related talent available within the United States would similarly affect the AI ecosystem and national security, including economic security, writ large. In particular, reluctance of AI talent to work for the U.S. Government could pose additional national security risks. There are multiple barriers to hiring qualified data scientists, software engineers, and data engineers in the Federal Government that would have to be overcome.

1.1.10. Other Emerging Risks and Long-term Trends

The history of AI has revealed that periods of excitement and productivity may be tempered by lulls in progress. Large statistical AI models have recently made stunning advances—for example, recently released models for natural language (so-called “large language models”) and image generation may rival human authors and artists in some ways. These models present new challenges related to authorship, academic integrity, misinformation, and disinformation; could replace some human intellectual or creative work; and pose new questions about copyright for creative works. Development of these models typically requires enormous computer and data resources, limiting competition to a small number of large technology companies. Many of these models are closely held by commercial entities and have little oversight from the public.

However, improvements in AI performance might not be sustainable simply by continuing to increase model size and apply more computing power on larger data sets. Sustained progress will require advances in hardware, software, algorithms, and data methods—including to address limitations of relying on historical data for modeling changing phenomena such as climate change—and possibly even fundamental computer science. In addition, too heavy a focus on today’s most mature and popular AI models, techniques, datasets, or benchmarks risks neglecting work that could enable future development of new commercial products and solutions to societal problems; a broad R&D portfolio can help to ensure future progress and benefits of AI. In parallel, proactive research, assessment, understanding, and planning related to societal implications of AI and plans for mitigating AI risks will be necessary for AI benefits to be realized safely and equitably.

Information technology and AI have become increasingly integrated into daily life and into major societal functions. Over the long term, this trend is likely to continue—though the boundaries of what is considered “AI” may change. While there is substantial uncertainty about when or whether artificial general intelligence—AI that is applicable to any context and even capable of operating completely autonomously—may be a realistic possibility, the field may progress in this direction, which could present risks related to AI alignment with human values and priorities.

The market value of AI has increased the commodification of data derived from individual experiences—which are often gathered without consent and can be used to influence future behavior. AI has affected and will continue to affect labor markets and the nature of work, with the potential to make work more precarious, cause unemployment, surveil workers, or increase inequality—including when access to technology is limited. Alternatively, technology can augment or support humans in their work functions, or replace humans in carrying out less desirable tasks. AI also has the potential to concentrate wealth if a small number of entities control most of the key AI resources.

AI is inherently sociotechnical, and societal norms and technical capabilities will evolve over time. AI R&D and deployment will influence—and be influenced by—ongoing societal change. Whether these changes are positive or negative will likely depend on the pace and nature of these transitions, the extent to which practices and their implications are transparent and consistent with individual and societal values and democratic norms, the extent to which lawmakers and developers are willing to balance technological growth with protection of privacy and civil rights and civil liberties affected by AI systems, the ability of members of the public to inform AI-related policies, and the extent to which policy interventions ease any hardships incurred.

1.1.11. Recommendations

The following recommendations address:

- Growing the U.S. economy through the secure and responsible advancement of AI;
- Strengthening the United States' global position in the adoption of trustworthy and rights-respecting AI;
- Mitigating current and emerging risks to a competitive AI marketplace and supply chain for AI;
- Mitigating current and emerging risks to the American public's privacy, civil rights and civil liberties, and other potential harms of AI; and
- Advancing societal priorities and addressing societal concerns associated with the expeditious adoption of AI.

Recommendation 1: Congress should take action to establish or strengthen data privacy and protection laws that safeguard privacy, civil rights, and civil liberties; support a competitive AI innovation ecosystem; and help advance the responsible adoption of trustworthy and rights-preserving AI technologies.

Recommendation 2: The U.S. Government should invest in education and research to support the development of sociotechnical researchers and practitioners necessary to design and deploy AI systems for positive societal impact, mitigate residual risks to safety, security, civil rights and civil liberties, and support trustworthy and equitable AI ecosystems across all sectors of the economy.

Recommendation 3: Congress should reauthorize the National AI Initiative Act of 2020 (NAIIA), 15 U.S.C. §§9401 *et seq*., regularly in order to enable the United States to meet changing needs across sectors as the landscape of AI evolves, and expand it to include emphasis on the need to protect the American public's civil rights, civil liberties, privacy, and safety.

Recommendation 4: Congress should empower the NAIIO to provide strong Federal coordination and leadership for AI activities in partnership with associated agencies across the executive branch, such as NIST in its Federal AI standards coordination role.

Recommendation 5: The U.S. Government should establish a formal public-private forum to support R&D and TEVV coordination across agencies with input from the private sector and enable U.S. leadership in trustworthy and responsible AI research, development, and standards.

Recommendation 6: The United States should lead global efforts to develop technically sound AI standards to enable continued innovation, ensure that global markets are open and fair, and promote AI development and use in a way that protects privacy, civil rights, civil liberties, and human rights. These efforts should consider gaps in and the most effective incentives for participation among U.S. companies and institutions, as well as R&D aligned to trustworthy AI standards development and principles.

Recommendation 7: The U.S. Government should support more equitable, secure, and privacy-enhanced access to research data sets—consistent with the original purpose of collection and while safeguarding privacy, civil rights, and civil liberties in their use—and computational resources to support AI innovation by research institutions, small- and medium-sized companies, and the general public. Examples include implementing the recommendations of the NAIRR Task Force.

Recommendation 8: Any efforts of Congress to modernize copyright, patent subject matter eligibility, or tech-transfer laws should take into consideration how such adjustments would best support the commercialization of innovative AI breakthroughs and a competitive AI innovation ecosystem while protecting the American public's privacy, civil rights, and civil liberties.

Recommendation 9: The United States should expand AI-related upskilling, cross-training and certification programs, and other programs designed to help individuals apply AI to expand their capabilities and productivity across all education and experience levels, for example through public-private partnerships and developing new interagency AI training programs.

Recommendation 10: The United States should expand and ensure accessibility of AI R&D and education activities across all relevant academic disciplines at Minority-Serving Institutions including but not limited to at Historically Black Colleges and Universities, Hispanic Serving Institutions, Women's colleges, and community colleges to help ensure a diverse future AI workforce positioned to meet industry, government, academic, and societal needs.

Recommendation 11: The United States should reform immigration law to make it easier for non-U.S. citizen AI graduate students and researchers to study and remain and work in the United States in order to retain the best and most diverse talent, with appropriate safeguards for security.

Recommendation 12: Fully fund the President's budget to support AI activities and programs, such as for: interagency coordination; protecting the American public and consumers against potential AI-related harms; AI R&D and standards development; R&D for next-generation computer hardware; increasing availability of AI testing, evaluation, verification, and validation resources; developing and operationalizing AI models as mandated in government; and strengthening U.S.-based manufacturing of leading-edge microprocessors, including graphics processing units (GPUs), which are an essential part of the AI infrastructure. This investment would serve as a critical component to develop safeguards and guardrails to mitigate risks in the AI ecosystem more broadly. Such guardrails should be embedded in each individual major AI initiative that the U.S. Government undertakes or funds. This will ensure that consideration of trustworthy and responsible AI is a part of the development process for all major initiatives, rather than an afterthought.

1.2. Background

1.2.1. Purpose and Structure of This Chapter

The Consolidated Appropriations Act of 2021 (Public Law 116-260) mandated that the Secretary of Commerce and Federal Trade Commission prepare a series of studies on critical and emerging technologies, including AI, and their impact on the U.S. economy. As prescribed by statute (provided in Appendix B), this chapter highlights the current[6] landscape within which AI technologies may be commercially deployed. These observations are based on a review of reports, laws and policy documents, technical literature, interviews with Federal employees, and submissions in response to a public Request for Information (RFI). It also provides several high-level recommendations for enhancing the Nation's ability to benefit from AI technologies. The research and writing for this chapter were first completed in early 2022. Since this time there have been numerous AI technology, market, and policy developments. While this document has been updated to reflect many major developments, it is likely that some content will no longer be current and that some recent Administration activities might not be reflected herein by the time of publication.

Section 1.2 provides general context about AI technologies and recent Federal efforts aimed at advancing U.S. competitiveness in these fields. Section 1.3 catalogs the status of major standards, regulations, guidance, frameworks, and principles governing commercial AI use, as well as key Federal and private sector authorities, collaborations, and other activities that support the responsible deployment of AI technologies in industry. Section 1.4 describes key (1) risks associated with the AI marketplace and supply chain, (2) risks to national security, including economic security, associated with the exploitation of the AI supply chain by foreign governments or third parties, and (3) emerging risks and long-term trends for the AI industry—all based on a survey of AI market and ecosystem studies. Section 1.5 lays out recommendations to address risks and harness opportunities for the safe development and deployment of trustworthy AI.

[6] Content was first developed in February 2022, and updated subsequently with new developments as noted in-place throughout the chapter.

1.2.2. Context on Artificial Intelligence Technologies

There is no single accepted definition of AI. AI is sometimes described as the quality associated with an information technology system capable of tasks that, had they been conducted by a human, would be considered intelligent behavior. The term AI is sometimes used to refer to an academic discipline and its interrelated subfields, such as natural language processing, machine learning (including deep learning), reinforcement learning, planning, plan recognition, and image understanding. It also may refer broadly to a range of technologies. AI technologies are generally deployed for automation of processes, in full or in part, or to assist humans in carrying out tasks. Numerous technical definitions and taxonomies for AI exist.

The most current definition of AI used by NIST [1] is[7]

> *an engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy.*

This definition aligns with the one codified in the National Artificial Intelligence Initiative Act of 2020 15 U.S.C. §9401 (3), which is provided in Box 1. These definitions are very similar to the one adopted by the OECD.[8] Another definition of AI is codified in Section 238 of the FY 2019 National Defense Authorization Act. US. Statutory definitions of AI are provided in Box 1.

The term AI was coined by John McCarthy in 1956 [3]. Over the years, attention to and excitement about AI has waxed and waned, leading to periods of heavy government and commercial investment alternating with investment "winters" when AI performance and capabilities fell short of proponents' expectations [4–6].

AI is not a single technology or even a set of related technologies. AI systems can conduct a range of different tasks such as perception (vision, voice recognition, etc.), learning, natural language processing, and planning [7]. Hence, discussions about implementing and promoting AI or AI standards are necessarily broad. In general, AI technologies involve computer software (programs that implement AI algorithms[9]), and must be deployed in computer hardware (physical devices with processing power such as a computer or a smartphone). Often data are also necessary to train and test the AI system before it is usable. The term "AI model" is often used to refer to the set of algorithms that describe the complete AI software system.

In recent years there have been numerous successful demonstrations of AI systems that perform useful or human-like functions, leading to a significant increase in attention and investment. These demonstrations include GPT-3 (and later versions) [8], Google Search [9], AlphaGo [9], WATSON Jeopardy! [10], and Facebook image classification. Once an

[7] Adapted from the Recommendation of the OECD Council on AI Organisation of Economic Co-operation and Development, "OECD AI Recommendations 2021" (Organisation of Economic Co-operation and Development (OECD), 2021), https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449 and ISO/IEC standard 22989:2022.

[8] OECD is an intergovernmental economic organization spanning the United States and 27 other nations that have been facilitating coordination of AI principles development, including through a Global Partnership on AI (GPAI).

[9] An algorithm is a set of well-defined instructions for performing a computation or solving a problem.

AI system has been demonstrated and is widely adopted, the public sometimes considers it as simply another instance of information technology, rather than AI.

ML is a prevalent current approach used in AI research, development, and deployment, involving the use of algorithms that draw inferences from patterns in data as opposed to AI systems that use explicitly programmed rules for processing information. ML can be supervised, semi-supervised, or unsupervised.

Box 1. Statutory Definition of Artificial Intelligence: NAIIA Division E, Sec. 5001 - 15 U.S.C. §9401 (3)

The term "artificial intelligence" means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to—

(A) perceive real and virtual environments;

(B) abstract such perceptions into models through analysis in an automated manner; and

(C) use model inference to formulate options for information or action.

John S. McCain National Defense Authorization Act for Fiscal Year 2019 (P.L. 115-232) defines AI as including:

(1) Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.

(2) An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action.

(3) An artificial system designed to think or act like a human, including cognitive architectures and neural networks.

(4) A set of techniques, including machine learning, that is designed to approximate a cognitive task.

(5) An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting.

In supervised machine learning (SML), machines are given training examples as inputs that humans have labeled with an associated output—for example assigning it to a particular class—from which the SML system "learns" to map previously unseen inputs to outputs. Artificial "neural networks"—networks of nodes with weighted connections designed to emulate biological neurons in a brain (and first developed in the 1940s)—are commonly used as the inference engine, the part of the system that deduces new information based on input data.[10] Successful training of an SML system can require

[10] Changing the weights, or "parameters," in connections within a neural network changes the behavior of the network; learning processes can tune the neural network to a specific problem.

large amounts of labeled training data and can have limited application to outputs not included in the training set. For example, if an SML system is trained to classify lions, tigers, and bears, it will not be able to accurately classify a Dalmatian.[11] The explosion of available computing power and the ready availability of data from the internet (some of it already labeled) have enabled the development of SML for many problems. At the same time, more complex problems require exponentially higher amounts of computing power, and the availability of labeled training data can be a limiting factor.

Unsupervised machine learning (UML) also requires training data, but rather than relying on pre-assigned labels, a UML system groups examples based on patterns extracted from the data set. A human can then label each group appropriately. There are also semi-supervised techniques that require some of the training data to be labeled, but not all. Another major ML paradigm is reinforcement machine learning (RML, also known simply as reinforcement learning) where the system learns and improves by adapting its parameters in ways that reinforce successful outputs by maximizing a cumulative reward function. While RML typically requires a large amount of computational power for simulations and explicit reward functions may be difficult to specify, it does not require labeled training data.

DL, a powerful approach to implementing ML, uses layers of neural networks for inference through optimization of large numbers of parameters. Since the late 2000s, the availability of fast GPUs has enabled DL to be applied to a range of AI tasks with major improvements in AI performance [11]; DL systems are now widely deployed in commercial systems. Many large-scale DL models that train on internet-scale data use self-supervision—somewhere in between UML and SML—in which labels used for supervised learning are generated by a model rather than by humans. Generative modeling is an important deep learning paradigm for which methods include generative adversarial networks (GAN), variational autoencoders (VAE), and diffusion models. In a GAN, two neural networks compete, with one attempting to generate new data that are indistinguishable from the training data and the other attempting to distinguish the new data. In a VAE, a neural network is trained to compress (encode) data such that it can be decoded accurately. Diffusion models are trained to map how observed variables connect to so-called "latent" or inferred variables in a way that can enable, for example, adding and then removing noise from training images to achieve a new image with desired content.

There are numerous other AI methods and techniques, and a full taxonomy is not provided here. While much of the enthusiasm about AI today is focused on DL (including so-called "large language models" such as GPT-4 and other generative language or image models), this is not the only area of ML, which is in turn not the only area of AI. For example, expert systems based on explicit instructions is also an important area of the discipline.

A long-term goal of some individuals in the discipline of AI is to design so-called artificial general intelligence (AGI) that is applicable to any problem. This technology has not been realized and is not likely to be realized in the immediate future [12], and recent predictions for a realistic timeline for AGI have varied widely. All working AI

[11] Such a system could be fine-tuned to classify Dalmatians with a small number of examples since the classification tasks are similar.

systems are currently narrow in scope. While this is not problematic when developed for a narrowly defined problem (e.g., AlphaGo excels at playing Go) the same AI system may not perform well if retrained for a different problem. Also, if a system is reused without retraining, it may not perform well even for a similar problem (e.g., an image recognition algorithm trained to identify cats being used to identify dogs). This inability to perform well outside of the original training or optimization context is called brittleness and is a well-known limitation of current AI techniques.

1.3. Observations

This section characterizes the range of industrial uses of AI technologies; industry and private sector activities to promote the advancement, adoption, and use of AI; current standards, policies, and guidelines that govern or inform the commercial deployment of AI; and Federal coordination activities and resources for the public. These findings were identified via literature review and discussions with Federal Government experts.

1.3.1. Industry

1.3.1.1. Industry Sectors That Implement, Develop and Promote the Use of Artificial Intelligence

AI is currently used to automate or assist a variety of business processes—including data analysis, customer service, marketing, and hiring—that are common across all sectors.[12] As a result, every sector contains some firms that implement or promote the use of AI.[13]

However, levels of AI use and the nature of use cases vary by industry. A 2020 McKinsey survey of industry found that AI adoption was highest in the sectors of high technology and telecommunications, automotive and assembly, and financial services [13]. More than 70% of interviewed high-tech and telecommunication firms implemented AI in some fashion, along with 60% of automotive and financial services companies. In comparison, fewer than 40% of healthcare/pharmaceutical and retail firms reported the adoption of AI. According to a 2021 update of the McKinsey survey, the automotive industry most often implemented AI in manufacturing processes, while financial and high-tech firms most often used AI for risk analysis, marketing, sales, and the development and operation of products and services [14]. In comparison, the retail, healthcare, and professional services sectors reported comparatively lower rates of AI adoption across most business functions. Firms in these sectors still implemented AI, primarily for marketing, sales, and product and service development.

Sectors produce advances in AI at different rates as well. The U.S. Patent and Trademark Office (USPTO) found that the majority of the top 30 U.S. AI patent holding companies are in the information and communication technology sector [15]. These 30 companies,

[12] This report uses sector definitions from the North American Industrial Classification System (NAICS). See Appendix C for more information about NAICS sectors.

[13] In this chapter, "promotion" is understood to mean "contributing to the growth of." In this sense, research, development, and implementation are all forms of promotion because they contribute to the growth of the AI industry and AI capabilities.

led by IBM, Microsoft, and Google, were granted 29% of all AI-related patents between 1976 and 2018.

The functions AI systems perform vary across sectors. A 2021 McKinsey survey found that no one AI capability was employed substantially more often than others [14]. The most commonly implemented AI capabilities documented by McKinsey were robotic process automation, natural language text understanding, computer vision, and virtual agents, which were common across most sectors.

Industries typically reported adopting AI capabilities that correspond to their main business functions. For instance, sectors that rely on manufacturing and distribution of physical goods, such as the retail, consumer goods, and automotive industries, tend to adopt physical robotics and automated driving systems. Sectors that process large amounts of data and serve many customers—such as financial services, telecommunications, healthcare, and professional services—often adopt natural language processing capabilities such as text and speech generation and understanding, with the quality of the available data a key constraint on use cases. A terse sample of sector-specific uses of AI is provided in Sec. 1.3.1.7

1.3.1.2. Public-Private Partnerships Focused on Promoting the Adoption and Use of Artificial Intelligence

There is no universally accepted definition of public-private partnerships, but they can generally be understood as “cooperative institutional arrangements between public and private sector actors” [16]. For the purposes of this chapter, a public-private partnership is defined as any coordinated activity that combines resources (e.g., funding, infrastructure, or expertise) from both the public (Federal Government) and private sectors toward a shared goal of accelerating science and technology R&D and deployment. This definition does not include standard contracting and acquisition activities.

In 2019, the National AI Research and Development Strategic Plan Update called for expanding the number of public-private partnerships to accelerate advances in AI R&D [17]. Since then, large-scale activities that can be considered public-private partnerships have been established for the purpose of advancing AI research, development, and deployment. The National AI Research Institutes, established to support R&D in various subfields of AI, are led by NSF with participation from other Federal agencies for the purpose of enabling longer-term research and U.S. leadership in AI. These institutes promote research, development, and deployment of AI by working to expand the utility and capabilities of AI, including in sector-specific applications. The 18 National AI Research Institutes funded as of the time of this writing are listed in Table 1.

Table 1Other multisector partnerships, listed in Table 2, focus on specific goals related to AI and intellectual property, international cooperation, cybersecurity, research advancement, and tools to support Veterans and first responders. These partnerships often aim to build relationships between different AI stakeholders, including governments and researchers, producers, implementers, and end-users of AI. For example, the U.S. Patent and Trademark Office (USPTO) has in recent years undertaken numerous activities regarding AI and IP through engagement with stakeholders from all sectors [18; 19] through the Partnership on AI and Emerging Technologies [20]. In 2019, USPTO held a conference on IP considerations in AI and issued requests for information from the public on AI and IP, posting the results online and summarizing submitted comments in a 2020 report entitled "Public Views on Artificial Intelligence and Intellectual Property Policy" [21]. A second report, released around the same time, explores the diffusion of AI into different areas of discovery via analysis of U.S. patents [22]. USPTO also issued, in response to a query from four members of Congress, a request for information on the implications of current legal theory and practice related to patent subject matter eligibility for innovation, including in AI. The submitted comments, which reflect a variety of opinions on current doctrine, are summarized in its June 2022 report to Congress, "Patent eligible subject matter: Public view on the current jurisprudence in the United States" [22].

Many of the activities listed in this section are primarily funded by the Federal Government and involve the private sector primarily in a supplemental capacity. The National AI Research Institutes fall into this category.

While not strictly public-private partnerships, two activities recently announced by the White House aim to promote the informed and responsible use of AI by increasing engagement of and transparency for the public related to potential implications of AI. First, OSTP has released a Request for Information seeking input on "national priorities for mitigating AI risks and protecting individuals' rights and safety, and harnessing AI to improve lives" to help inform ongoing strategic planning [23]. Second, the White House announced an independent commitment from leading developers of AI technologies to participate in an independent evaluation of AI system performance in relation to the elements of the White House *Blueprint for an AI Bill of Rights*. This exercise, planned for the 2023 DEFCON conference, is designed to inform researchers and the public about the impacts of AI models, and enable any issues identified to be fixed [24].

Finally, the Department of Commerce announced on June 22, 2023 plans for a new Public Working Group on Generative AI. The group is intended to include volunteers from multiple sectors to inform guidance on how the NIST AI Risk Management Framework can support development of generative AI technologies. In the longer term, the group is expected to help inform how generative AI can be deployed for positive societal benefits [25].[14]

[14] Given the rapidly evolving research, technology, market, and policy landscapes for AI, it is possible that this section will be out of date by the time of publication of this Chapter.

Table 1. National AI Research Institutes with Public-Private Cooperation.

U.S. Federal Department or Agency[a]	Name[b]	Establishment Date	Lead Partner Organization	Other Partner Organizations	Purpose
NSF, NIST	The TRAILS (Trustworthy AI in Law and Society) Institute[c] [26]	May 3, 2023	University of Maryland	3 academic institutions	Bring attention to AI ethics and human rights and communities whose voices have been marginalized into mainstream AI
NSF, DHS S&T	AI Institute for Agent-based Cyber Threat Intelligence and Operation (ACTION)[c] [27]	May 3, 2023	University of California, Santa Barbara	11 academic institutions [28]	Develop novel approaches that leverage AI to perform security tasks that anticipate adversary actions
USDA	AI Institute for Climate-Land Interactions, Mitigation, Adaptation, Tradeoffs and Economy (AI-CLIMATE)[c] [29]	May 3, 2023	University of Minnesota	5 academic institutions and 1 tribal nation consortium [30]	Advance AI and incorporate knowledge from agriculture and forestry sciences to curb climate effects
NSF, DoD	AI Institute for Artificial and Natural Intelligence (ARNI)[c] [31]	May 3, 2023	Columbia University	7 academic institutions, 4 industry collaborators, 1 independent research institute, and 1 medical institute	Connect progress in AI to progress made in understanding the brain
NSF	AI Institute for Societal Decision Making (AI-SDM)[c] [32]	May 3, 2023	Carnegie Mellon University	7 academic institutions, 1 hospital, and 1 nonprofit [33]	Develop human-centric AI for decision-making and inter-disciplinary training
NSF, Department of Education	AI Institute for Inclusive Intelligent Technologies for Education (INVITE)[c] [34]	May 3, 2023	University of Illinois, Urbana-Champaign	7 academic institutions and 2 industry partners [35]	Promote effective learning by developing AI to support student persistence, academic resilience, and collaboration

U.S. Federal Department or Agency[a]	Name[b]	Establishment Date	Lead Partner Organization	Other Partner Organizations	Purpose
NSF, Department of Education	AI Institute for Transforming Education for Children with Speech and Language Processing Challenges (AI4ExceptionalEd)[c] [36]	May 3, 2023	University at Buffalo	8 academic institutions [37]	Advance AI technologies to enhance understanding of children's speech and language development
NSF	AI Institute for Intelligent Cyberinfrastructure with Computational Learning in the Environment (ICICLE) [38]	November 1, 2021	Ohio State University	9 academic institutions, 4 industry partners, and 28 other academic, nonprofit, research, and government organizations [39]	Develop intelligent cyberinfrastructure with an emphasis on transparency and resilience.
NSF	AI Institute for Learning-Enabled Optimization at Scale (TILOS) [38]	November 1, 2021	University of California-San Diego	5 academic institutions and 19 industry collaborators [40]	Develop learning-enabled optimization technologies.
NSF	AI Institute for Adult Learning and Online Education (ALOE) [38]	November 1, 2021	Georgia Research Alliance	7 academic institutions, 1 nonprofit, and 3 industry partners [41]	Develop AI systems and algorithms to improve adult education and online learning.
NSF, DHS	AI Institute for Edge Computing Leveraging Next Generation Networks (Athena) [38]	October 1, 2021	Duke University	6 academic institutions and 5 industry partners [42]	Develop AI-driven edge computing technology.
NSF	AI Institute for Future Edge Networks and Distributed Intelligence (AI-EDGE) [38]	October 1, 2021	Ohio State University	10 academic institutions, 3 DoD labs, and 4 industry partners [43]	Develop technologies for distributed and networked intelligent systems.
NSF	AI Institute for Engaged Learning [38]	October 1, 2021	North Carolina State University	3 academic institutions, 1 nonprofit organization, and “a national network of K-12 schools, museums, and nonprofit organizations” [44]	Conduct use-inspired research on learning and collaboration in an AI-driven narrative learning environment.
NSF	AI Institute for Collaborative Assistance and Responsive	October 1, 2021	Georgia Institute of Technology	4 academic institutions and 2 industry sponsors [45]	Develop human-AI interaction behavior models and use those models to improve collaboration,

U.S. Federal Department or Agency[a]	Name[b]	Establishment Date	Lead Partner Organization	Other Partner Organizations	Purpose
	Interaction for Networked Groups (AI-CARING) [38]				communication, and user experience.
NSF	AI Institute for Advances in Optimization [38]	October 1, 2021	Georgia Institute of Technology	5 academic institutions, 1 national lab, 1 education partner, and 5 industry partners [46]	Research mathematical optimization problems using AI, with a focus on algorithms for distributed electric grids and supply chains.
NSF, DHS	AI Institute in Dynamic Systems [38]	October 1, 2021	University of Washington	8 academic institutions and 1 industry partner [47]	Enable real-time learning in dynamic systems, with an emphasis on safety and control.
USDA-NIFA, NSF	AI Institute: AIIRA: AI Institute for Resilient Agriculture[d]	July 15, 2021	Iowa State University	6 academic institutions, 4 commodity groups, 1 State government group, 1 national lab, 2 Federal research centers, 2 international groups, 8 startups, 8 industry partners, and 11 other organizations [48]	Use AI to increase agriculture resiliency through predictive crop modeling.
USDA-NIFA, NSF	AI Institute: Agricultural AI for Transforming Workforce and Decision Support (AgAID)[d]	July 6, 2021	Washington State University	7 core academic institutions, 23 other academic partners, 11 government or nonprofit partners, and 16 industry partners [49]	Foster partnerships between AI and agriculture communities for technology transfer and innovation.
NSF	AI Institute: AI Research Institute for Fundamental Interactions [38]	November 1, 2020	Massachusetts Institute of Technology	3 academic institutions, 1 international lab, 3 national labs, 1 scientific collaboration group and 2 academic labs [50]	Develop the next generation of AI technologies to support new discoveries in the field of physics, including knowledge transfer and workforce development efforts.
USDA-NIFA, NSF	AI Institute: Next Generation Food Systems [51]	September 1, 2020	University of California, Davis	5 academic institutions, 1 university system division, 1 Federal agency, 2 academic research centers, 19 industry	Develop innovative applications of AI technologies as well as the next-generation workforce to address

U.S. Federal Department or Agency[a]	Name[b]	Establishment Date	Lead Partner Organization	Other Partner Organizations	Purpose
				partners and 2 foundations [50]	challenges across the US food supply chain.
NSF	Molecule Maker Lab Institute (MMLI): An AI Institute for Molecular Discovery, Synthetic Strategy, and Manufacturing [38]	September 1, 2020	University of Illinois at Urbana-Champaign	3 academic organizations, 1 industry partner [50]	Create tools powered by AI to advance research and manufacturing efforts for small molecule manufacturing.
NSF	AI Institute: Institute for Foundations of Machine Learning [38]	September 1, 2020	University of Texas at Austin	1 academic institution, 1 local government, and 5 industry partners [52]	Develop mathematical tools and algorithms for complex machine perception tasks.
NSF	AI Institute: Institute for Student-AI Teaming [38]	September 1, 2020	University of Colorado Boulder	8 universities, 3 K-12 education partners, and 3 industry partners [53]	Study AI in education to improve human-AI interaction and assist students and educators.
NSF	AI Institute: Artificial Intelligence for Environmental Sciences (AI2ES) [38]	September 1, 2020	University of Oklahoma Norman Campus	7 academic institutions, 1 federally funded research and development center, 1 Federal agency, and 7 industry partners [54]	Develop AI for environmental science data and research, with a particular focus on trustworthiness.
USDA-NIFA, NSF	AI Institute: Artificial Intelligence for Future Agricultural Resilience, Management, and Sustainability (AIFARMS) [55]	August 21, 2020	University of Illinois at Urbana-Champaign	4 academic institutions, 1 independent research center, 1 national lab, and 3 industry partners [56]	Advance AI by using it to address challenges in agriculture. Focuses on autonomous systems for sustainability, livestock management, designing climate-resilient agricultural systems, and reducing risk in crop production.

[a] This column includes only departments and agencies that provide substantial direct funding for the activities of the institute. Other Federal departments and agencies may collaborate with institutes on specific work. These departments and agencies are considered “Other Partner Organizations.”; [b] Each of these institutes has received funding on the order of millions of dollars or more; current funding levels may be found by searching for “AI Institute” in the NSF Award Search web portal (https://www.nsf.gov/awardsearch/) and the USDA NIFA Reporting Portal (https://portal.nifa.usda.gov/lmd4/recent_awards); [c] Updated May 2023; [d] The USDA NIFA CRIS public-facing database of funded projects does not provide hyperlinks to records for these projects. However, these project records can be accessed by searching the USDA NIFA AI Institute program code “A7303” in the CRIS database at https://cris.nifa.usda.gov/;

Table 2. Other Public-Private Partnerships Focused on Promoting the Adoption and Use of AI.

U.S. Federal Department or Agency	Name	Date Established	Lead Organization	Other Partner Organizations	Purpose
USPTO	AI and Emerging Technology (ET) Partnership[a] [20]	June 7, 2022	USPTO	Academia, independent inventors, small businesses, industry, other government agencies, nonprofits, and civil society	Engage the AI/ET community on ongoing and future USPTO AI/ET efforts and gather public views on various IP policy issues that uniquely affect the AI/ET community.
VA	AI Tech Sprints [57]	January 4, 2021	VA National Artificial Intelligence Institute	Challenge.gov and competitive teams from outside government	Incentivize and share data for competitive teams to create AI-enabled tools that help address real-world challenges faced by Veterans.
DOE, DOD, NOAA, First Net Authority, PNNL	First Five Consortium [58; 59]	September 18, 2020	Microsoft	7 industry partners and 3 academic partners	Use AI to mitigate the impact of natural disasters by supporting first responders.
OSTP, State	Global Partnership on Artificial Intelligence (GPAI) [60]	June 15, 2020	OECD	24 member states and the EU	Foster international cooperation in AI research.
NIST	National Cybersecurity Center of Excellence (NCCoE) [61; 62]	February 21, 2012	NIST	A state government, a local government, and over 21 industry partners listed	Accelerate the widespread adoption of integrated cybersecurity capabilities. Engages in research and has provided guidance on adversarial ML.
NIH, The White House	COVID-19 Open Research Dataset Challenge (CORD-19) [63; 64]	March 2020	Allen Institute of AI	One university and five private sector organizations	Spur researchers to develop AI-based tools for data and text mining of the world's largest collection of research publications on COVID-19, in order to help the medical community.

U.S. Federal Department or Agency	Name	Date Established	Lead Organization	Other Partner Organizations	Purpose
DOL/ODEP	Partnership on Employment and Accessible Technology (PEAT)[a] [65]		Wheelhouse Group	DOL/ODEP and collaborating technology stakeholders	Foster collaborations with technology stakeholders to create inclusive technology policies and practices.
NIST	Exploring Research Frontiers by Incorporating AI and ML [58]		NIST	Academia, other government laboratories, and industrial entities	Incorporate AI in NIST's research efforts, including for innovative measurements, predictive systems, and autonomous measurement platforms.

[a] Updated December 2022.

1.3.1.3. Industry-Based Bodies that Develop Technical Standards for Artificial Intelligence

There are numerous Standards Development Organizations (SDOs) active across the information and communications technology enterprise that create voluntary standards. Many of these SDOs are not solely industry-driven, and engage with a variety of private and public sector stakeholders working on the development of standards relevant to AI. SDOs generally have a record of engagement, broad buy-in, and expertise that are likely to be influential in shaping the trajectory of AI technologies. The actual standard development work of an SDO is typically conducted by a specialized working group where experts convene to discuss and execute the creation of new standards according to an established process. SDOs gather a wide range of input to increase the rigor and improve the likelihood of adoption of their standards [66]. SDOs can play a significant role in shaping the development and implementation of technical systems worldwide, especially those with a standards development process involving subject-matter experts and an established history of technological contributions, and may be referenced in treaties, contracts and other agreements [67].

Standards developed by SDOs can become market-relevant through the buy-in of the public and private sectors, and governments often engage substantially with these entities. Under the U.S. National Technology Transfer and Advancement Act (NTAA), signed into law in 1996, U.S. Federal agencies and departments are required to use technical standards "developed or adopted by voluntary standards bodies" and to engage with these standards bodies in the development of technical standards when consistent with agency responsibilities and in the public interest. OMB Circular A-119 provides Federal agencies with guidance on implementation of NTAA requirements, providing flexibility to agencies to decide individually which standards are the best match for their use. Existing standards may become mandatory when referenced in regulations [68]. In general, standards benefit from testing prior to adoption and the work of maintaining and updating standards comes with financial costs.

Key entities working to develop international AI standards include the Joint Technical Committee 1 (JTC 1) between the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), and the Institute of Electrical and Electronics Engineers Standards Association (IEEE SA). Additional entities developing or supporting AI standards development include organizations such as the International Telecommunication Union (ITU) & the European Telecommunications Institute, not-for-profit organizations like the Consumer Technology Association (CTA), the Object Management Group and the Association for the Advancement of Medical Instrumentation. Within the United States, ANSI provides accreditation for standards development processes, certifying voluntary, consensus-based American National Standards [69].

Individuals who wish to engage in ISO and IEC standards development processes may do so via their national standards body (NSB) [70]. In part due to the high costs of such participation, the National Security Commission on AI recommended that Congress establish a grant program to enable small- and medium-sized U.S. companies to engage in international standards development activities [71]. While technical standards can influence technology deployment, the details of such standards are not necessarily made accessible to the general public. Many SDOs follow a business model based on the sale of standards which are copyrighted by the SDOs. Many U.S. SDOs have also taken steps to increase availability, including through read-only options allowing individuals to preview standards. The details of published ISO standards must be purchased for use by organizations developing AI and related technologies.[15]

In general, topic-specific working groups of SDOs convene to address specific technical areas, draft technical specifications, iterate on draft specifications to come to consensus, and eventually publish the new standards for adoption across industries. These working groups are not fixed; at any given time, new groups may be formed, others engaged in ongoing work, and some that may be retired. The following sections describe major SDOs and their working groups that are currently focusing on AI-related standards development. While some of these working groups are AI-specific, others may focus on other topics but are nonetheless working on AI-specific standards. Standards development by these organizations requires alignment with best antitrust practices to avoid abuses of the process which, for example, could lead one or more industry participants to gain an unfair competitive advantage over other participants.

ISO and IEC

ISO is a non-governmental organization founded in 1947 and composed of 164 members representing their countries and national standards bodies; ISO bridges many stakeholder groups in order to cooperatively develop standards across technical and industrial sectors [72]. IEC, founded in 1906, is composed of members and experts from 174 countries who work to coordinate and publish international standards that facilitate trade and interoperability in the electrical and electronic goods space [73]. ISO and IEC standards are widely recognized and adopted for regional and national standards. These standards facilitate trade worldwide through their reference in contracts and trade agreements as examples of international standards, due in large part to their compliance with the World Trade Agreement's Technical Barriers to Trade (TBT) agreement [74].

ISO/IEC Joint Technical Committee 1 (JTC 1) focuses on developing standards for the information technology sector. Within JTC 1, there are five subcommittees with working groups that are developing AI-relevant standards: Subcommittee 27 (SC 27), Subcommittee 32 (SC 32), Subcommittee 37 (SC 37), Subcommittee 38 (SC 38), and Subcommittee 42 (SC 42). ISO/IEC subcommittees may comprise advisory groups (AG), ad-hoc groups (AHG), joint working groups (JWG), coordination groups (CG) and working groups (WG).

Subcommittee 42 (SC 42) serves as the primary focal point for JTC 1's standardization activities for AI and also provides guidance to other groups outside SC 42 concurrently developing AI-related standards [75]. SC 42 oversees two advisory groups (AG), four ad-hoc groups (AHG), one joint working group (JWG), and five working groups (WG).

Unlike Subcommittee 42, Subcommittees 27, 32, 37, and 38 were created with other technology areas in mind, but each includes individual working groups that are contributing standards in support of further progress in the field of AI. SC 27 develops standards in the area of information security, cybersecurity and privacy protection, and currently oversees

[15] Some standards incorporated into Federal regulations are made available as read-only online by ANSI's Incorporated by Reference (IBR) portal: https://ibr.ansi.org/Faq/Default.aspx .

five working groups that are developing AI-related standards [76]. SC 32 advances standardization for data management and interchange across different information systems environments, and oversees two working groups that are developing AI-related standards [77]. SC 37 creates standards for the biometrics technologies field and currently oversees six working groups that are developing AI-related standards [78]. SC 38 produces standards for cloud computing and distributed platforms, and oversees one coordination group and two working groups that are developing AI-related standards [79]. All ISO/IEC working groups developing AI-related standards are presented in Table 3.

Table 3. Joint Working Groups of ISO/IEC Joint Technical Committee 1 Working on AI-related Standards (As of February 2022).

ISO/IEC Group	Topical Area	Purpose
SC 27/ WG 1 Information security management systems [76]	Information communications technology security management systems	Advance standardization for managing information and communications technologies, including security systems, processes and services.
SC 27/ WG 2 Cryptography and security mechanisms [76]	Cryptography and security mechanisms	Specify security techniques, principles, and protocols relevant to cryptography and other security mechanisms.
SC 27/ WG 3 Security evaluation, testing and specification [76]	Evaluation, testing and specification for information security management systems	Advance foundational standards critical to information technology security, including evaluation criteria and methodology for security systems.
SC 27/ WG 4 Security controls and services [76]	Security controls, processes and services	Guide the development and implementation of information security controls.
SC 27/ WG 5 Identity management and privacy technologies [76]	Identity management and privacy technologies	Produce frameworks to address aspects of identity management and privacy.
SC 32/ WG 2 MetaData [77]	Metadata and other information	Define the languages, methodology and protocols relevant to metadata and related data sharing.
SC 32/ WG 3 Database language [77]	Languages and services for databases	Set the languages and guidance around language use for databases.
SC 37/WG 1 Harmonized Biometric Vocabulary [78]	Harmonized Biometric Vocabulary	Define common terminology and concepts towards the development of biometric technologies, standards and policies.
SC 37/WG 2 Biometric Technical Interfaces [78]	Programming interfaces for biometric applications	Advance standardization for the interfaces of biometric applications and the data transfers between systems.
SC 37/WG 3 Biometric Data Interchange Formats [78]	Interchange formats for biometric data	Produce biometric data interchange formats to enable harmonization across different biometric technologies.
SC 37/WG 4	Technical implementation of biometric systems	Set foundational guidance, requirements and best practices towards the implementation of biometric systems.

ISO/IEC Group	Topical Area	Purpose
Technical Implementation of Biometric Systems [78]		
SC 37/WG 5 Biometric Testing and Reporting [78]	Performance testing and reporting for biometric technologies	Develop methodologies for testing and reporting performance of biometric technologies.
SC 37/WG 6 Cross-Jurisdictional and Societal Aspects of Biometrics [78]	Cross-jurisdictional and societal aspects of biometrics technologies	Identify cultural, societal and ethical issues relevant to biometric technologies.
SC 38/ CG 1 Liaison coordination group for JTC 1/SC 27 [79]	Information security, cybersecurity, and privacy protection	Together with SC 27, coordinates efforts around standard development for protections around information and information and communications technologies.
SC 38/ WG 3 Cloud Computing Fundamentals (CCF) [79]	Fundamentals of cloud computing technologies, services, and usage	Establish the foundational set of definitions, guidance, frameworks, and relevant technologies under the umbrella of cloud computing.
SC 38/ WG 5 Data in cloud computing and related technologies [79]	Data for cloud computing and distributed platforms	Produce standards and frameworks related to data policies and practices for cloud computing, including data handling, data flow, and data processing.
SC 42/ AG 1 AI Management Systems Standard Advisory Group [75]	AI management systems	Review the viability of standards for an AI Management System.
SC 42/AG 2 AI Systems Engineering Advisory Group [75]	AI systems engineering practices and opportunities for standardization	Advise JTC 1/SC 42 on study items including gap analysis between current engineering practices & ISO/IEC standards with AI best practices.
SC 42/AHG 1 Dissemination and Outreach Ad-Hoc Group [75]	AI standardization activities across ISO/IEC	Develop information on JTC 1/SC 42 activities for broader dissemination and outreach to relevant stakeholders and communities.
SC 42/AHG 2 Liaison with SC 38[75]	Cloud computing and distributed platforms	Together with SC 38, addresses cloud computing and distributed platforms.
SC 42/AHG 4 Liaison with SC 27 [75]	Information security, cybersecurity and privacy protection	Together with SC 27, addresses information security, cybersecurity and privacy protection.
SC 42/AHG 5 AI standardization landscape and roadmap [75]	AI standardization landscape and roadmap	Develop information on JTC 1/SC 42 activities within the AI standardization landscape and roadmap space.
SC 42/JWG 1 Governance Implications of AI Joint Working Group [75]	Governance of the use of AI systems at organizations	Together with SC 40, addresses governance implications of the use of AI by organizations.

ISO/IEC Group	Topical Area	Purpose
SC 42/WG 1 Foundational Standards Working Group [75]	Fundamentals of AI systems and lifecycle	Advance foundational standards in AI, including concepts & terminology, a framework for AI systems, and studying the AI lifecycle.
SC 42/WG 2 Data Working Group [75]	Big Data and AI	Advance foundational standards for data in AI, big data, and data analytics.
SC 42/WG 3 Trustworthiness Working Group [75]	Trustworthiness of AI systems	Advance standardization in AI trustworthiness, including bias in AI, risk management, and ethical & social concerns.
SC 42/WG 4 Use Cases and Application Working Group [75]	Use cases and applications of AI	Advance use cases and applications in AI, including projects in AI system lifecycle processes and guidelines for AI applications.
SC 42/WG 5 Computational Approaches and Computational Characteristics of AI Systems Working Group [75]	Computational approaches and computational characteristics of AI systems	Advance computational approaches for AI systems, including assessments for ML classification performance and reference architecture of knowledge engineering.

IEEE SA

IEEE was founded in 1884 with an initial focus on the electrical engineering and related technologies such as electric power and wired communications. IEEE has since become the largest professional technical organization worldwide, with more than 400,000 individual members across 160+ countries, as of December 2021 [80].The IEEE Standards Association (IEEE SA) is an activity area of IEEE, which creates standards and protocols across engineering, computing, and technology use cases, and has grown increasingly active in the AI space [81]. Within IEEE SA, 18 active working groups are developing AI-relevant standards and protocols; these are listed in Table 4.

Table 4. Working Groups of the IEEE SA Developing AI-related Standards (As of February 2022).

IEEE SA Working Group	Topical Area	Purpose
P2247 Adaptive Instructional Systems (AIS) Working Group [82]	Adaptive instructional systems (AISs)	Investigate gaps in standards for adaptive instructional systems, with the aim of generating new projects to address these gaps.
P2817 Verification of Autonomous Systems - Guidelines Working Group [83]	Verification of autonomous systems guidelines	Promote the development of autonomous systems through proposed verification processes and other guidance.
P2830 Shared Machine Learning Working Group [84]	Shared ML	Provide a framework for ML models based on trusted and aggregated data.

IEEE SA Working Group	Topical Area	Purpose
P2840 Responsible AI Licensing Working Group [85]	Response AI	Propose considerations around responsible AI, including standard definitions, and laws relevant to data and privacy.
P2841 Deep Learning Working Group [86]	Deep learning	Establish best practices for the development and implementation of deep learning systems.
P2850 Intelligence Cities Operation System Working Group [87]	Operation systems for intelligent cities	Promote efforts towards intelligent cities by advancing interoperability of technical infrastructure and data.
P2863 Organizational Governance of Artificial Intelligence Working Group (OGAI WG) [88]	Organizational governance of AI systems	Provide recommendations for responsible, transparent, and effective development and implementation of AI systems in organizations.
P2894 Explainable Artificial Intelligence Working Group [89]	Explainable AI (XAI)	Advance standardization and adoption for explainable AI techniques and systems.
P2895 Trading Human-Generated Data Working Group [90]	Human-generated data	Establish rules and parameters around data contracts, including data collection, use and trading.
P2937 AI System and Application Test Working Group [91]	Testing for AI systems and applications	Specify the performance-testing methodology for AI systems and infrastructures.
P2945 Face Recognition Working Group [92]	Facial recognition technologies	Advance technical and architectural requirements for the development of facial recognition systems.
P2961 Collaborative Edge Computing Working Group [93]	Collaborative edge computing	Set guidelines and a framework towards collaborative edge computing, including shared definitions, categories and a method for performance evaluation.
P2986 Security and Privacy for Federated Machine Learning Working Group [94]	Privacy and security for federated ML	Promote security and privacy recommendations for federated ML systems.
P3652 Federated Machine Learning Working Group [95]	Federated ML	Facilitate the application of federated ML systems, especially for organizations in the industrial sector.
P7000 Engineering Methodologies for Ethical Life-Cycle Concerns Working Group (EMELC-WG) [96]	Addressing ethical risks for the systems and software lifecycles	Produce standards and recommendations to enable the integration of ethics-oriented considerations throughout the product and systems lifecycles (development through disposal).
P7006 Personal Data AI Agent Working Group [97]	Personalized AI	Set the requisite technical elements related to personalized AI systems

IEEE SA Working Group	Topical Area	Purpose
P7007 Ontologies for Ethically Driven Robotics and Automation Working Group [98]	Ethically-driven robotics and automated systems ontologies	Advance ethically-driven robots and automated systems through the creation of ontologies containing definitions and concepts related to AI.
P7008 Ethically Driven Nudging for Robotic, Intelligent and Autonomous Systems Working Group [99]	Ethically-driven nudging for robotic, intelligent and autonomous systems	Promote the development of ethically-driven robotic, intelligent and autonomous systems through the establishment of common definitions, concepts and guidelines.

ITU-T

The ITU was founded as a United Nations specialized agency for information and communications technologies in 1865; since then, communications technologies have evolved from the telegraph to radio to the internet. Currently, ITU is composed of more than 20,000 members representing 193 nations and coming from across the public and private sectors. The ITU Telecommunication Standardization Sector (ITU-T) convenes study groups of international experts to develop ITU-T recommendations that serve as standards for global information and communication technology infrastructure [100]. ITU-T has begun to advance AI standardization efforts. Both AI WGs and non-AI WGs of the ITU-T are engaged in development of AI-related standards; these entities are listed in Table 5 [101].

Table 5. Working Groups of the ITU Developing AI-Related Standards (As of February 2022).

ITU-T Group	Topical Area	Purpose
Focus Group FG-AI4Ad [102]	AI for Autonomous and Assisted Driving	Produce standards and deliverables in the area of AI for autonomous and assisted driving, with the aim of enabling an open environment and broad harmonization for AI-enabled driving.
Focus Group FG-AI4EE [103]	Environmental Efficiency for AI and other Emerging Technologies	Develop standards and reports related to assessing environmental performance for AI technologies, with the aim of establishing a collaborative environment for all interested stakeholders.
Focus Group FG-AI4H [104]	AI for Health (AI4H)	Partner with the World Health Organization to establish a common standard for evaluating AI-enabled solutions for healthcare applications.
Focus Group FG-AI4NDM [105]	AI for Natural Disaster Management (AI4NDM)	Partner with the World Meteorological Organization and UN Environment Programme to develop a community of stakeholders and experts addressing AI applications for natural disaster management.
Focus Group FG-AN [106]	Autonomous Networks	Draft specifications and reports in the area of autonomous networks, with the aim of establishing a collaborative environment within ITU for all related pre-standards activities.

ITU-T Group	Topical Area	Purpose
Focus Group FG-ML5G [107]	ML for Future Networks including 5G	Establish standards and frameworks specific to the application of ML for future networks, including algorithms, architectures and data formats.
Study Group 11 (SG11) [108]	Signaling requirements, protocols, test specifications	Develop specifications, protocols and testing parameters for telephone network signaling, with the aim of enabling the interoperability of information and communications technology components & applications.
Study Group 12 (SG12) [109]	Performance, quality of service (QoS), and quality of experience (QoE)	Produce standards targeting the performance, quality of service, and quality of experience for networks and services.
Study Group 13 (SG13) [110]	Future networks, with focus on IMT-2020, cloud computing and trusted network infrastructures	Produce standards and technical requirements that cover next-generation networks, including aspects to enable the Internet of Things (IoT), cloud computing, and other aspects of mobile telecommunications.
Study Group 16 (SG16) [111]	Multimedia coding, systems and applications	Lead ITU standardization efforts for multimedia, including areas such as media coding, videoconferencing, and e-health.
Study Group 17 (SG17) [112]	Information and communications technologies (ICTs) security	Coordinate standardization and guidance efforts related to ICT security across ITU and cooperates with additional SDOs and consortia. Their aim is to build confidence and trust in the applications and services that use ICTs.
Study Group 2 (SG2) [113]	Operational aspects of service provisions and telecommunications management	Serve as the home for several foundational standards for telecom services, networks, and equipment, with the aim to define the next generation of telecommunications networks.
Study Group 20 (SG20) [114]	IoT and Smart Cities and Communities (SC&C)	Provide standards for IoT technologies, with an emphasis on enabling the coordination of technology development, promoting interoperability of IoT applications, and providing the technological foundation for concepts such as Smart Cities.
Study Group 9 (SG9) [115]	Broadband cable and TV	Work to study and provide recommendations in the area of cable and hybrid television/telecommunication systems, with the aim of harmonizing next-generation technologies and interactive services.
Study Group 3 (SG3) [116]	Tariff and accounting principles including related telecommunication economic and policy issue	Study the intersection of telecommunications services & networks with the economic and financial sphere, with particular interest in newer concepts such as big data and digital identity.

ANSI

ANSI is a private, non-profit organization that oversees and provides a framework for U.S. voluntary standards development for numerous industries and technology areas. While not an SDO itself, ANSI is the official member body representing the United States in ISO and in IEC through the U.S. National Committee to the IEC. [68]. Within the United States, ANSI represents the U.S. national committees (USNC). Each U.S. TAG/USNC directly correlates to an ISO and IEC technical committee, and each will contribute to standards development by communicating their positions via ANSI [117]. ANSI oversees the International

Committee for Information Technology Standards (INCITS) as the U.S. TAG corresponding to the ISO/IEC JTC 1, which focuses on information technology standards.

European Telecommunications Standards Institute

The European Telecommunications Standards Institute (ETSI), founded in 1988, creates standards in the information and communications technologies space and has lines of effort focused on AI. ETSI—along with the European Committee for Standardization and the European Committee for Electrotechnical Standardization—form the European system for technical standards development [118]. ETSI's membership and impact extends beyond Europe, there are over 900-member organizations from over 60 countries, 68 of which are based in the United States. ETSI has an operational coordination group (OCG AI) for all the AI standardization activities across the ETSI community. OCG AI does not develop standards directly, but instead serves to identify common activities and facilitate cooperation between the ETSI groups that can contribute to AI-related standards. ETSI is composed of two major categories of technical groups: (1) Technical Committees and ETSI Projects and (2) Industry Specification Groups, as well as ETSI Partnership Projects. While participation in the first category of technical groups is reserved to ETSI members, in the second category standards work can include members and non-members [119]. Table 6 presents the ETSI groups—two partnership projects, four technical committees/centers, and eight industry specification groups—that are or have been developing AI-related standards, regardless of whether the groups are focused exclusively on AI.

Table 6. ETSI Groups Developing AI-Related Standards (As of February 2022).[a]

ETSI Group	Topical Area	Purpose
3rd Generation Partnership Project (3GPP) [120]	3rd generation Mobile and Cellular Telecommunications	Create standards covering cellular telecommunications technologies, networks, and systems. This includes the planning, deployment, maintenance, and optimization of 5G networks.
Context Information Management (CIM) Industry Specification Group [121]	Interoperable Software for Context Information Management	Produce specifications that enable easier information exchange between vertical applications. CIM has an emphasis on promoting interoperability, especially for use cases including Smart Cities.
eHealth Technical Committee [122]	Information and Communications Technologies for Health	Provide standards, deliverables, and coordination across ETSI and other SDOs in the electronic health space. Key areas within the eHealth technical committee are (1) systems & data security, (2) service quality, (3) interoperability & validation-by-testing, and (4) usability.
Core Network and Interoperability Testing (INT) Technical Committee [123]	Test Specifications to Enable Interoperability Testing of Core Network	Produce test specifications (purposes, descriptions, and cases) necessary to test core networks for interoperability.
Network Functions Virtualisation (NFV) Industry Specification Group [124]	Network Functions Virtualisation	Provide reports and specifications for the virtualization of network functions, including architectural frameworks, deployment templates, and studies on NFV performance. These specifications also support deployment for 5G.

ETSI Group	Topical Area	Purpose
Permissioned Distributed Ledger (PDL) Industry Specification Group [125]	Permissioned Distributed Ledgers	Publish foundational standards and reports for permissioned distributed ledgers (PDL), in order to enable an open, trusted, PDL ecosystem for future use cases.
Smart Machine-to-Machine (SmartM2M) Technical Committee [126]	Machine-to-Machine Services/Internet of Things (IoT)	Develop standards for the advancement of machine-to-machine (M2M) technologies, services, and applications. SmartM2M has published requirements towards the Smart Cities and Smart Agriculture use cases.
Augmented Reality Framework (ARF) Industry Specification Group [127]	Interoperability of AR Components, Applications and Systems	Focus on developing a framework for interoperable augmented reality (AR) components, with the aim of enabling an AR ecosystem that is more transparent, reliable, and open.
Cyber Security (CYBER) Centre of Excellence [128]	Cyber Security Standardization	Create standards addressing cybersecurity challenges, with the aim of enabling a common cybersecurity ecosystem, as well as protecting personal data and communications.
Experiential Network Intelligence (ENI) Industry Specification Group [129]	Networking Orchestration of Autonomous Networks	Focus on developing a Cognitive Network Management architecture, as well as related use-case requirements and proof-of-concepts.
Multi-access Edge Computing (MEC) Industry Specification Group [130]	Multi-Access Edge Computing	Define standards and platforms for multi-access edge computing (MEC), in order to enable an open environment that integrates applications from multiple entities across the value chain.
One Machine-to-Machine (OneM2M) Partnership Project [131]	M2M and IoT	Bring together several SDOs, consortia, and numerous organizations around developing specifications to support oneM2M technology, applications, and services.
Securing AI (SAI) Industry Specification Group [132]	Using AI to Enhance Security, Attack Mitigation using AI, Securing AI from Attack	Develop technical standards and reports to advance the security of AI technologies, including attack prevention, mitigation, and enhanced system protections.
Zero-touch Network & Service Management (ZSM) Industry Specification Group [133]	End-to-End Automation of Network and Service Management	Produce reports and specifications to promote the adoption of zero-touch network & service management (ZSM) architecture. The ultimate aim is to enable end-to-end automation for organizations.

[a] Content drawn from [119].

Object Management Group

The Object Management Group (OMG) is an international nonprofit founded in 1989 with the mission of developing technological standards across numerous industries (such as finance, government, and healthcare). OMG standards are created with the participation of members, who are subject-matter experts from across government, academia, and industry [134]. Many of the standards that OMG has published have been submitted and ratified as ISO standards The OMG Artificial Intelligence Platform Task Force was consolidated in

2019, with the broad mission to advance foundational standards in AI. Since then, OMG has developed AI-relevant standards in the areas of knowledge representation and reasoning and non-interface-oriented robotics [135].

Table 7 presents the working group at OMG developing AI-relevant standards or documents.

Table 7. OMG Group Developing AI-Related Standards (As of February 2022).

OMG Group	Topical Area	Purpose
Artificial Intelligence Platform Task Force [136]	Foundational AI capabilities, including ML, deep learning, AR, VR, NLP, etc.	Enable interoperability between users and technology suppliers in the AI space, through the development of specifications publication of use-case documents or other collaborative efforts.

Responsible AI Institute (RAI)

The RAI (formerly called AI Global), is a nonprofit organization developing and administering an accredited industrial certification program to support the development of recognizably responsible and trusted AI systems across industries. RAI has developed the Responsible Artificial Intelligence certification, which aims to provide a common method for characterizing the bias, fairness, and explainability of a given AI system. RAI has identified five key areas for initial focus, (1) fair lending, (2) fraud detection, (3) automated diagnosis and treatment, (4) health recommendation systems, and (5) automated hiring [137]. The institute also provides other resources and programs, such as the RAI Community Portal that provides a library of AI standards, models, datasets and other resources for responsible AI [138].

1.3.1.4. Sector Specific Industry Entities Pursuing Standards for AI Development

In addition to the SDOs described above, there are other standards or trade organizations working toward AI standards specific to an industrial sector. These groups may have a role in establishing common practices or contributing to AI standards development within their sector. Several examples are described in the following sub-sections.[16]

Consumer Technology Association

The Consumer Technology Association (CTA) is a U.S.-based standards and trade organization that represents consumer technology companies. Since its founding in 1924, CTA has published 135 standards in the computing and technology space through the work of over 70 committees, subcommittees, and working groups. The trade association has formed an Artificial Intelligence Committee to publish voluntary standards to be adopted by industry. CTA's Artificial Intelligence Committee focuses on standards, best practices, and technical reports for AI technologies [139]. There is one working group within this committee, the Artificial Intelligence in Health Care group (focusing on areas such as consumer health and fitness technology). Table 8 presents the working groups at CTA developing AI-relevant standards or documents.

[16] Many of these examples relate to medical and healthcare-related uses of AI, consistent with the fact that the medical device industry is a highly-regulated sector.

Table 8. CTA Group Working on AI-Related Standards (As of February 2022).

CTA Group	Topical Area	Purpose
Artificial Intelligence in Health Care [140]	AI applications for healthcare technologies, such as consumer health and fitness technology	Develop technical standards, produce best practices and share other documents to support the application of AI for healthcare.

SAE International

SAE International is an association of professional engineers and technical experts from transportation-related industries, including automotive, commercial vehicles, and aerospace [141]. In 2014, the organization introduced a taxonomy describing six levels of driving automation for use as a voluntary standard for on-road motor vehicles, and updated it in 2021 [142].

Health AI Partnership

A partnership between Duke Health, the Mayo Clinic, the University of California, Berkeley, DLA Piper, and the Gordon and Betty Moore Foundation was established to help standardize best practices for medical AI (AI software used in the medical and healthcare industries). In December 2021, the group initiated in a 12-month project to gather information about medical AI from different care delivery systems and collect information from stakeholders, including users, regulators, policy experts, and health payers. It plans to develop and release an open source, publicly available, online education curriculum to support the incorporation of medical AI into care delivery systems, to include practices for procurement, integration, and lifecycle management [143].

The Association for the Advancement of Medical Instrumentation-British Standards Institution (AAMI-BSI) Initiative on Artificial Intelligence

The Association for the Advancement of Medical Instrumentation (AAMI) is a nonprofit organization committed to advancing the safety and efficacy of health technology. AAMI creates standards for the medical device industry, and has a standards committee focused on AI. The British Standards Institution (BSI) is the United Kingdom's national standard body. BSI creates standards across every economic sector, including the aerospace, healthcare, and information & communications technology sectors.

Together, AAMI and BSI have formed the AAMI/BSI Initiative on Artificial Intelligence, a collaborative effort to address existing challenges at the intersection of the healthcare technology space and the application of AI & ML. In 2020, the Initiative released a white paper based on stakeholder workshops, *Machine Learning AI in Medical Devices: Adapting Regulatory Frameworks and Standards to Ensure Safety and Performance*. This paper provides recommendations on the development and deployment of new standards, regulation, and common approaches to ML for medical device applications [144].

The International Medical Device Regulators Forum (IMDRF)

The International Medical Device Regulators Forum (IMDRF) was established in 2011, with the convening of medical device regulators from around the world. IMDRF works towards advancing medical device harmonization on an international scale, building off the efforts of its predecessor organization, the Global Harmonization Task Force on Medical Devices [145]. As of February 2022, there are seven IMDRF working groups, each tasked with developing technical documents for a particular area of the medical device ecosystem [146].

The Artificial Intelligence Medical Devices working group focuses on accelerating alignment in the management of AI-based medical devices. Thus far, this working group has published a document establishing key terminology for ML-enabled medical devices [147]. IMDRF groups working on AI-relevant standards or documents are listed in Table 9.

Table 9. IMDRF Groups Working on AI-Related Standards (As of February 2022).

IMDRF Group	Topical Area	Purpose
Artificial Intelligence Medical Devices	AI and ML-enabled medical devices	Advancing technological alignment and harmonization for AI-enabled medical devices, through the cooperation of medical device regulators from across the world.

Private Companies

Private companies also create de facto standards important for their operations in the absence of formal standards; SDO processes can be slow, may not be fully open, and may require funding to support individual or organizational participation. Such standards can take the form of adopted processes, tools such as open-source software, or frameworks, and can influence industry practices and the subsequent establishment of formal standards or guidelines—for example, because they have already been tested or adopted in the originating company. Examples include Microsoft's data sheets or adversarial ML threat taxonomy, the SHapley Additive exPlanations (SHAP) package for model explanation, OpenAI's Gym, AI "model cards" deployed at Facebook and Google, and frameworks for machine learning such as TensorFlow and PyTorch.

1.3.1.5. Nonprofit Industry Entities and Coalitions Supporting Development of Standards and Practices for AI Deployment

Beyond the work of SDOs, numerous non-profit private sector entities and coalitions are working to address pressing issues related to the deployment of AI, especially those with broader societal implications. Examples include the AAMI-BSI Initiative on Artificial Intelligence, the Center for Democracy and Technology, the Center on Privacy and Technology at Georgetown Law, Data & Society, the Data & Trust Alliance, the Electronic Frontier Foundation, the Electronic Privacy Information Center, EqualAI, the Institute for Human-Centered AI at Stanford University, The One Hundred Year Study on Artificial Intelligence, and the Partnership on AI (PAI). For additional examples, see the entities that provided input to the Office of Science and Technology Policy to inform the development of its Blueprint for an AI Bill of Rights [148] and that provided input to the NAIRR Task Force [149].

1.3.1.6. Status of SDO Standards Focused on AI

As AI techniques and capabilities continue to mature and be deployed in applications, work to develop standards has been growing. Numerous standards are under development, and activities are evolving rapidly. The EU Observatory for ICT Standardization maintains a database of technical standards that includes those related to AI [150]. This section provides an overview of SDO AI standards published or currently under development at the time of this writing. In addition, the Federal Government has produced a variety of resources to support individuals, small businesses and other organizations that may use AI; these are discussed in Sec. 1.3.6 of this Chapter. As AI techniques and capabilities continue to mature and be deployed in applications, work to develop standards has been growing. Numerous standards are under development, and activities are evolving rapidly. The EU Observatory for ICT Standardization maintains a database of technical standards that includes those related to AI [150]. This section provides an overview of SDO AI standards published or currently under development at the time of this writing. In addition, the Federal Government has produced a variety of resources to support individuals, small businesses and other organizations that may use AI; these are discussed in Sec. 1.3.6 of this Chapter.

ISO/IEC Standards

There are six main stages of ISO/IEC standard development: (1) proposal, (2) preparatory (working draft, WD), (3) committee (committee draft ballot, CD), (4) enquiry (draft international standard ballot, DIS), (5) approval (final draft international standard ballot, FDIS), and (6) publication. In the proposal stage, a new work item proposal (NWIP) is submitted for voting at the technical committee or subcommittee level. In the preparatory stage, the working group assigned to the item will work on drafts until expert consensus is reached. In the committee stage, the first committee draft is distributed to relevant technical committees or subcommittees for comment and votes; this process of drafting, commenting and voting is repeated until consensus is reached. In the enquiry stage, a draft international standard is distributed for wider ISO member comment and votes. In the approval stage, the final draft international standard is submitted for a final vote to ISO members. The final stage, publication, is reached when the final draft has been approved as an International Standard [151].

As of February 2022, ISO/IEC working groups had engaged on 52 AI-relevant standards in various stages of the development process, including 31 under development and 21 published in final form. Of these AI-relevant standards, 9 are affiliated with SC 27 (information security, cybersecurity and privacy protection), 1 is affiliated with SC 32 (data management and interchange), 10 are affiliated with SC 38 (cloud computing and distributed platforms), and 32 are affiliated with SC 42 (artificial intelligence). These 52 listed AI-relevant standards, along with their objectives and statuses, are described in Table 10 below.

Table 10. Status of ISO/IEC AI-Related Standards.

ISO/IEC Standard	Main Objective	Status as of December 2022[a]
22123-2.4 Cloud computing, part 2: concepts [152]	Advance fundamental concepts for the development of cloud computing technologies and other distributed platforms.	Under Development
23894 Risk management [153]	Provide guidelines and processes around risk management for organizations working with AI.	Under Development
24029-2 Methodology for the use of formal methods [153]	Provide guidelines and methods for the assessment of neural network robustness.	Under Development
25059 Square: quality model for AI systems [153]	Provide a model for measuring and evaluating the quality of an AI system.	Under Development
27046.4 Big data security and privacy, implementation guidelines [154]	Offer guidelines to address challenges in big data security and privacy.	Under Development
42001 AI management system [153]	Describe the requirements and guidance around a proposed AI management system.	Under Development
5140 Concepts for multi-cloud and other interoperation of multiple cloud services [155]	Provide common definitions and concepts for the development of cloud services.	Under Development
5259-1 Data qualify for analytics and ML: part 1 [153]	Establish foundational concepts around data quality for analytics and ML.	Under Development
5259-2 Data quality for analytics and ML: part 2 [153]	Provide a data quality model and guidance for analytics.	Under Development
5259-3 Data quality for analytics and ML: part 3 [153]	Describe the requirements and guidance around data quality for analytics and ML.	Under Development
5259-4 Data quality for analytics and ML: part 4 [153]	Lay out common organizational approaches for high quality training and evaluation data.	Under Development
5338 AI system lifecycle processes [153]	Support the definition, maintenance of AI system lifecycle processes used at organizations.	Under Development
5339 Guidelines for AI applications [156]	Provide guidelines for the development and use of AI applications.	Under Development
5392 Reference architecture of knowledge engineering [157]	Describe a reference architecture of knowledge engineering in AI, including roles, components, and activities.	Under Development

ISO/IEC Standard	Main Objective	Status as of December 2022[a]
5469 Functional safety and AI systems [153]	Provide an overview of information and methods around the application of AI in safety-relevant functions.	Under Development
5471 Quality evaluation guidelines for AI systems [158]	Provide quality evaluation guidelines for AI systems.	Under Development
5928 Taxonomy for digital platforms [159]	Advance the technical specifications for various types of digital platforms.	Under Development
6254 Objectives and approaches for explainability of ML models and AI systems [160]	Describe approaches and guidance towards achieving AI and ML explainability.	Under Development
8200 Controllability of automated artificial intelligence systems [161]	Describe a framework for automated AI systems' controllability, including relevant principles, and approaches.	Under Development
24668:2022 Process management framework for big data analytics [162]	Establish a process reference model for big data analytics.	Published November 17, 2022
27559:2022 Privacy enhancing data de-identification framework [163]	Advance a framework around the process of de-identifying data, including common definitions and guidance.	Published November 16, 2022
4213:2022 Assessment of machine learning classification performance [164]	Provide methodologies for measuring classification performance for ML models, systems, and algorithms.	Published October 13, 2022
27556:2022 User-centric privacy preferences management framework [165]	Address the handling of personally identifiable information through a user-centered framework.	Published October 10, 2022
24368:2022 Overview of ethical and societal concerns[166]	Address ethical and societal concerns around AI.	Published August 19, 2022
22989:2022 Artificial intelligence concepts and terminology [167]	Establish terminology for AI & AI-related concepts; can be used for all types of organizations and in development of future AI standards.	Published July 19, 2022
23053:2022 Framework for Artificial Intelligence Systems Using Machine Learning [168]	Describe a framework for a generic AI system using ML technology.	Published June 20, 2022
3445:2022 Audit of cloud services [169]	Advance standardization efforts around the practice of auditing cloud services.	Published March 9, 2022

ISO/IEC Standard	Main Objective	Status as of December 2022[a]
38507:2022 Governance implications of the use of artificial intelligence by organizations [170]	Provide a broad guidance for organizations using AI in tools or systems.	Published April 8, 2022
19944-2:2022 Data flow, data categories and date use, part 2: guidance on application and extensibility [171]	Establish technical guidelines around data identification, processing and sharing, applicable to use cases such as facial recognition and the IoT.	Published April 1, 2022
23751:2022 Data sharing agreement (DSA) framework [172]	Establish the foundational concepts and definitions for the creation of data sharing agreements (DSAs).	Published February 15, 2022
24745:2022 Biometric information protection [173]	Update the 24745:2011 standard that set protection guidance for biometric information.	Published February 8, 2022
24372:2021 Information technology — Artificial intelligence (AI) — Overview of computational approaches for AI systems [174]	Review cutting-edge computation approaches for AI systems, including: main computational characteristics, algorithms/approaches used, and reference cases.	Published December 7, 2021
21838-2:2021 Information technology — Top-level ontologies (TLO) — Part 2: Basic Formal Ontology (BFO) [175]	Offer foundational definitions, concepts, and specifications for the coordinated development of future domain-specific ontologies and the data systems that rely on those ontologies.	Published November 30, 2021
24027:2021 Information technology – Artificial Intelligence (AI) – Bias in AI systems and AI aided decision making [153]	Provide guidance around bias in AI systems, including methods to assess bias.	Published November 5, 2021
24030:2021 Information technology – Artificial Intelligence (AI) – Use Cases [176]	Review use cases of AI applied across different sectors and domains.	Published May 11, 2021
24029-1:2021 Artificial Intelligence (AI) — Assessment of the robustness of neural networks — Part 1: Overview [153]	Detail existing methods for assessing neural network robustness.	Published March 10, 2021
22123-1:2021 Information technology — Cloud computing — Part 1: Vocabulary [177]	Define the common terminology and vocabulary within the cloud computing field.	Published February 16, 2021

ISO/IEC Standard	Main Objective	Status as of December 2022[a]
27570:2021 Privacy protection — Privacy guidelines for smart cities [178]	Provide guidance for the privacy-oriented development of technologies, processes, and policies within the smart cities field.	Published January 28, 2021
19944-1:2020 Cloud computing and distributed platforms ─ Data flow, data categories and data use — Part 1: Fundamentals [179]	Describe the ecosystem and interactions related to cloud services, along with a proposed structuring system for data use statements to improve user privacy and overall transparency.	Published October 26, 2020
20547-4:2020. Information technology — Big data reference architecture Part 4: Security and privacy [180]	Specify big data reference architecture considerations and guidance around security and privacy.	Published September 23, 2020
20547-1:2020 Information technology — Big data reference architecture — Part 1: Framework and application process [181]	Describe the framework of the big data reference architecture and provide a process for a user to apply the framework for their own area.	Published August 20, 2020
24028:2020 Information technology – Artificial Intelligence (AI) – Overview of trustworthiness in artificial intelligence [153]	Review topics around AI trustworthiness, such as approaches to transparency, threats & risks to AI systems.	Published May 28, 2020
20547-3:2020. Information technology — Big data reference architecture Part 3: Reference Architecture [182]	Provide specifics around the big data reference architecture for the purpose of a common understanding around the language, existing standards to build on, and technical components, processes, and systems around big data.	Published March 4, 2020
23167:2020 Information technology — Cloud computing — Common technologies and techniques [183]	Review the most common technologies and techniques that are used in cloud computing applications.	Published February 11, 2020
20546:2019. Information technology — Big data — Overview and vocabulary [184]	Provide foundational terminology and definitions around big data.	Published February 28, 2019
22678:2019 Information technology — Cloud computing — Guidance for policy development [185]	Produce guidance for the development of governance documents or regulations around cloud service providers and cloud services.	Published January 10, 2019
20889:2018 Privacy enhancing data de-identification terminology and classification of techniques [186]	Set the common terminology and techniques specific to the practice of data de-identification for any type of organization.	Published November 6, 2018

ISO/IEC Standard	Main Objective	Status as of December 2022[a]
20547-5:2018. Information technology — Big data reference architecture Part 5: Standards roadmap [187]	Review existing and developing standards around big data.	Published February 9, 2018
20547-2:2018 Information technology — Big data reference architecture Part 2: Use cases and derived requirements [188]	Provide uses cases for big data from across different domains, including technical considerations.	Published January 10, 2018
29134:2017 Information technology — Security techniques — Guidelines for privacy impact assessment [189]	Produce guidelines for the application of internal privacy impact assessments across numerous types of organizations.	Published June 28, 2017
29190:2015 Information technology — Security techniques — Privacy capability assessment model [190]	Advance a standardized methodology for organizations conducting internal assessments of privacy capability.	Published August 10, 2015

[a] Standards identified in February 2022; status updated December 2022.

IEEE SA Standards Focused on AI

IEEE SA also has several standards under development, as described in

Table 11. There are six primary steps in the IEEE SA standards development lifecycle: (1) initiating the project, (2) mobilizing the working group, (3) drafting the standard, (4) balloting the standard, (5) gaining final approval, (6) maintaining the standard [191]. The public can only view the active Project Authorization Requests (PARs) for standards that are currently in the development pipeline, prior to the balloting stage; PARs provide key information for the project including the purpose, need for project, and stakeholders [192]. Creating a PAR is the initiating step of a new IEEE SA standards project; PARs must include which working groups are responsible for the effort. The precise status of an IEEE standard is not publicly displayed, but a PAR will include the expected date for submitting the draft for ballot and a final expiration date the project must meet. As of April 2022, there were 65 AI-related standards in development (53) or published (12) by IEEE SA.

Table 11. Status of AI-Related Standards in Development or Published by IEEE SA (As of February 2022).

IEEE SA Standard	Main Objective	Status as of December 2022[a]
P2049.1 Standard for Human Augmentation: Taxonomy and Definitions [193]	Establish the common definitions and taxonomy related to human augmentation technologies.	Under Development
P2049.2 Standard for Human Augmentation: Privacy and Security [194]	Set the technical requirements and methods related to privacy and security-conscious use of human augmentation technologies.	Under Development
P2049.3 Standard for Human Augmentation: Identity [195]	Provide the technical requirements and methods related to identity verification by human augmented technologies.	Under Development
P2049.4 Standard for Human Augmentation: Methodologies and Processes for Ethical Considerations [196]	Offer methodologies for developing ethically-driven human augmented technologies.	Under Development
P2247.1 Draft Standard for the Classification of Adaptive Instructional Systems [197]	Classify adaptive instructional systems through defined parameters and components.	Under Development
P2247.2 Interoperability Standards for Adaptive Instructional Systems (AIS) [198]	Define the interactions of AIS components and to provide guidance around the use of data and data structures.	Under Development
P2247.3 Recommended Practices for Evaluation of Adaptive Instructional Systems [199]	Define methods for the evaluation of AIS and provide guidance for their use.	Under Development
P2247.4 Recommended Practice for Ethically Aligned Design of Artificial Intelligence (AI) in Adaptive Instructional Systems [200]	Offer recommendations around the design of AI as used by AIS.	Under Development
P2671 Standard for General Requirements of Online Detection Based on Machine Vision in Intelligent Manufacturing [201]	Set general requirements for machine vision-based online detection, such as data format, data transmission processes, and performance metrics.	Under Development
P2672 Guide for General Requirements of Mass Customization [202]	Set common definitions, technical requirements and applications for user-oriented mass customization.	Under Development
P2751 3D Map Data Representation for Robotics and Automation [203]	Build on the 1873-2015 standard, in order to provide 3D map data for robotics and automated systems.	Under Development
P2802 Standard for the Performance and Safety Evaluation of Artificial Intelligence Based Medical Device: Terminology [204]	Establish definitions and methodologies for the development of AI-based medical devices, including areas of safety and performance.	Under Development

IEEE SA Standard	Main Objective	Status as of December 2022[a]
P2807 Framework of Knowledge Graphs [205]	Provide a framework of knowledge graphs, including technical requirements and AI-related applications.	Under Development
P2807.1 Standard for Technical Requirements and Evaluation of Knowledge Graphs [206]	Define the technical requirements and evaluation criteria for financial knowledge graphs.	Under Development
P2807.2 Guide for Application of Knowledge Graphs for Financial Services [207]	Offer guidelines and technical requirements related to financial knowledge graphs.	Under Development
P2807.4 Guide for Scientific Knowledge Graphs [208]	Provide guidelines and technical requirements related to scientific knowledge graphs.	Under Development
P2817 Guide for Verification of Autonomous Systems [209]	Review best practices around verification processes for autonomous systems.	Under Development
P2840 Standard for Responsible AI Licensing [210]	Provide definitions, specifications, and policies relevant to the development of a responsible AI license.	Under Development
P2841 Framework and Process for Deep Learning Evaluation [211]	Provide a framework for the evaluation of deep-learning systems and algorithms.	Under Development
P2850 Standard for an Architectural Framework for Intelligent Cities Operation System [212]	Define a framework for computational operation systems, specifically applied to intelligent cities.	Under Development
P2863 Recommended Practice for Organizational Governance of Artificial Intelligence [88]	Provide governance criteria for the development and use of AI, including specifics on areas like transparency, safety and accountability.	Under Development
P2874 Standard for Spatial Web Protocol, Architecture and Governance [213]	Enable key features around the IoT, including support for access, permissions and rights management.	Under Development
P2888.6 IEEE Draft Standard for Holographic Visualization for Interfacing Cyber and Physical Worlds [214]	Define formats relevant to holographic interfaces, such as holographic printing file formats, encoding formats and representation schemes.	Under Development
P2894 Guide for an Architectural Framework for Explainable Artificial Intelligence [215]	Specify an architectural framework and guidelines towards the area of explainable AI, including definitions, application scenarios and performance evaluations.	Under Development
P2895 Standard Taxonomy for Responsible Trading of Human-Generated Data [216]	Provide the taxonomy and definitions for the field of human augmentation technologies, including wearables and implants.	Under Development

IEEE SA Standard	Main Objective	Status as of December 2022[a]
P2937 Standard for Performance Benchmarking for AI Server Systems [91]	Provide a methodology for performance testing different types of AI server systems.	Under Development
P2941 Draft Standard for Artificial Intelligence (AI) Model Representation, Compression, Distribution and Management [217]	Establish the technical requirements and formats for the representation, compression, distribution and management of AI models.	Under Development
P2945 Standard for Technical Requirements for Face Recognition Systems [92]	Detail the technical requirements for facial recognition systems.	Under Development
P2961 Guide for an Architectural Framework and Application for Collaborative Edge Computing [218]	Introduce a new ML framework, with the emphasis on cloud and edge computing.	Under Development
P2975 Standard for Industrial Artificial Intelligence (AI) Data Attributes [219]	Provide common definitions for the area of industrial AI data, along with key data attributes.	Under Development
P2986 Recommended Practice for Privacy and Security for Federated Machine Learning [220]	Offer best-practices for implementing privacy and security for federated ML systems.	Under Development
P2995 IEEE Draft Trial-Use Standard for a Quantum Algorithm Design and Development [221]	Set a standardized method to the design of quantum algorithms.	Under Development
P3110 IEEE Draft Standard for Computer Vision - Algorithms, Application Programming Interfaces, and Technical Requirements for Deep Learning Framework [222]	Establish the technical and functional requirements for an application programming interfaces (API) model of computer vision systems.	Under Development
P3119 IEEE Draft Standard for the Procurement of Artificial Intelligence and Automated Decision Systems [223]	Define a new process model tailored to government entities' procurement of AI and Automated Decision Systems (ADS).	Under Development
P3135 IEEE Draft Standard for Specifying Requirements for Neurofeedback Systems Design [224]	Set requirement specifications around the development and design of neurofeedback systems.	Under Development
P3141 IEEE Draft Trial-Use Standard for 3D Body Processing [225]	Provide a quality assessment framework for 3D body processing technology, including assessment metrics, tools and workflows.	Under Development
P7003 Algorithmic Bias Considerations [226]	Offer protocols to develop algorithms that minimize bias.	Under Development

IEEE SA Standard	**Main Objective**	**Status as of December 2022**[a]
P7004 Standard for Child and Student Data Governance [227]	Provide methodologies and best-practices related to the collection, storage and use of child and student data.	Under Development
P7004.1 Recommended Practices for Virtual Classroom Security, Privacy and Data Governance [228]	Provide best practices for child and student data governance, in accordance to IEEE P7004, including guidelines for compliance assessment.	Under Development
P7008 Standard for Ethically Driven Nudging for Robotic, Intelligent and Autonomous Systems [229]	Set the concepts and functions for the development of ethically-driven robotic, intelligent and autonomous systems.	Under Development
P7009 Standard for Fail-Safe Design of Autonomous and Semi-Autonomous Systems [230]	Provide the methodologies and technological foundation for the design of autonomous and semi-autonomous systems.	Under Development
P7010.1 Recommended Practice for Environmental Social Governance (ESG) and Social Development Goal (SDG) Action Implementation and Advancing Corporate Social Responsibility [231]	Provide best practices for environmental social governance and social development goal implementation, in accordance to IEEE 7010, including recommendations for common processes, data collection, and policy development.	Under Development
P7011 Standard for the Process of Identifying and Rating the Trustworthiness of News Sources [232]	Advance the use of standards to rate and review the accuracy of news stories and news purveyors.	Under Development
P7012 Standard for Machine Readable Personal Privacy Terms [233]	Address the application of personal privacy terms for machine use.	Under Development
P7014 Standard for Ethical considerations in Emulated Empathy in Autonomous and Intelligent Systems [234]	Create a model for implementing ethical-driven design in developing autonomous and intelligent systems.	Under Development
P7015 Standard for Data and Artificial Intelligence (AI) Literacy, Skills, and Readiness [235]	Provide an operational framework for the design, progress-tracking and outcome evaluation of AI-literacy policy interventions.	Under Development
P7030 Draft Recommended Practice for Ethical Assessment of Extended Reality (XR) Technologies [236]	Establish conceptual and technical definitions around extended reality (XR) technologies, as well as an ethical assessment methodology tailored to studying XR systems.	Under Development
P7130 IEEE Draft Standard for Quantum Technologies Definitions [237]	Define terminology for common use in the quantum technologies space.	Under Development

IEEE SA Standard	Main Objective	Status as of December 2022[a]
2801-2022 Recommended Practice for the Quality Management of Datasets for Medical Artificial Intelligence [238]	Review best practices around the use of quality management systems of datasets applied to the field of medical AI.	Published July 5, 2022
3333.1.3-2022 Draft Standard for the Deep Learning Based Assessment of Visual Experience Based on Human Factors [239]	Set deep learning-based assessments for content analysis and quality-of-experience.	Published May 27, 2022
1872.2-2021 Draft Standard for Autonomous Robotics (AuR) Ontology [240]	Build on standard 1872-2015 to create more ontologies for autonomous robotics.	Published May 12, 2022
7001-2002 Draft Standard for Transparency of Autonomous Systems [241]	Advance measures for assessing the transparency of autonomous systems.	Published March 4, 2022
7002-2022 Draft Standard for Data Privacy Process [242]	Set policy requirements for collection of personal data.	Published February 9, 2022
2089-2021 IEEE Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children [243]	Offer a framework for implementing age-appropriate and children-conscious measures for digital services.	Published November 30, 2021
7005-2021 IEEE Standard for Transparent Employer Data Governance [244]	Set methodologies to promote the transparent collection, storage and utilization of employee data.	Published November 19, 2021
7007-2021 IEEE Ontological Standard for Ethically Driven Robotics and Automation Systems [245]	Provide standardized ontologies towards the ethically-driven development of robotics and automated systems.	Published November 12, 2021
2842-2021 IEEE Recommended Practice for Secure Multi-party Computation [246]	Establish technical requirements for secure multi-party computation.	Published November 5, 2021
2830-2021 IEEE Standard for Technical Framework and Requirements of Trusted Execution Environment based Shared Machine Learning [247]	Create a framework for ML training using encrypted data collected from multiple sources.	Published October 22, 2021
7000-2021 IEEE Standard Model Process for Addressing Ethical Concerns During System Design [248]	Describe a systematic approach for identifying and addressing ethical considerations across each stage of AI development.	Published September 15, 2021

3652.1-2020 IEEE Guide for Architectural Framework and Application of Federated Machine Learning [249]	Set common practices for data use and model-building for federated ML systems.	Published March 19, 2021
2660.1-2020 Recommended Practices on Industrial Agents: Integration of Software Agents and Low Level Automation Functions [250]	Offer a recommended practice around the application of industrial agents to the interface of cyber-physical systems.	Published January 29, 2021
7010-2020 IEEE Recommended Practice for Assessing the Impact of Autonomous and Intelligent Systems on Human Well-being [251]	Offer a method for assessing the impact of autonomous and intelligent (A/IS) systems on human well-being.	Published May 1, 2020
1855-2016 IEEE Standard for Fuzzy Markup Language [252]	Introduce a specification language for modeling a fuzzy logic system in human- and computer-readable formats.	Published May 27, 2016
1873-2015 IEEE Standard for Robot Map Data Representation [253]	Provide environmental map data for mobile robots that perform navigational tasks.	Published October 26, 2015
1232.3-2014 Guide for The Use of Artificial Intelligence Exchange and Service Tie to All Test Environments (2014) [254]	Provide specific guidance for developers working with the Artificial Intelligence Exchange and Service Tie to All Test Environments (AI-ESTATE).	Published October 10, 2014

[a] Standards identified in February 2022; status updated December 2022.

Consumer Technology Association Standards Focused on AI

CTA has worked on several standards related to AI. CTA's Artificial Intelligence Committee serves as the activity area dedicated to developing standards, recommendations and publications related to AI [140]. "ANSI/CTA" standards are created through CTA's convening of subject matter experts and published with the accreditation of ANSI. Outside this arrangement, CTA has also independently published one standard, and ANSI has accredited one additional standard along with NIST. These standards are presented in Table 12.

Table 12. AI-Related Standards in Development or Published by ANSI or CTA (As of February 2022).

Standard Number	**Main Objective/Standard Description**	**Date Published**
CTA-2096 Guidelines for Developing Trustworthy Artificial Intelligence Systems [255]	Provide guidelines for AI developers working to create trustworthy systems.	November 5, 2021
ANSI/CTA-2090 The Use of Artificial Intelligence in Health Care: Trustworthiness [256]	Set foundational requirements for the application of AI in health care.	February 2, 2021

Standard Number	Main Objective/Standard Description	Date Published
ANSI/CTA-2089.1 Definitions/Characteristics of Artificial Intelligence in Health Care [257]	Define terminology relevant to AI and AI-related technologies/applications specific to the health care field.	February 25, 2020
Special Publication (NIST SP) - 500-290e3 [ANSI/NIST] Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information [258]	Establish data formats for the exchange of fingerprint, facial and other types of biometric information.	August 22, 2016

Object Management Group Standards under Development or Published

OMG is a nonprofit technology standards consortium, with a dedicated Artificial Intelligence Platform Task Force to advance standardization efforts in AI. OMG has published several voluntary standards relevant to AI systems, in the areas of general knowledge representation and reasoning and non-interface-oriented robotics standards, as indicated in Table 13.

Table 13. AI-Related Standards Published by OMG (As of February 2022).

OMG Document Number	Main Objective/ Standard Description	Date Published
ptc/2021-04-02 Application Programming Interfaces for Knowledge Platforms (API4KP) [135]	Addresses the development and application of knowledge platforms for organizations.	April 2021
Formal/2021-01-01 Decision Modeling and Notation (DMN) [259]	Provides a shared modeling language and notation around business decisions and business rules.	March 2021
Formal/2019-10-02 [SMSC/19-10-02] Semantics of Business Vocabularies and Rules (SBVR) [260]	Provides the semantics of business vocabulary and business rules for exchange among organizations or development of ontologies.	October 2019
Formal/18-09-02 Distributed Ontology, Modeling, and Specification Language (DOL[a]) [261]	Addresses the integration and interoperability of ontologies, models and specifications.	October 2018
Formal/2018-05-05 Robotic Interaction Service Framework (RoIS) [262]	Provides a framework for message and data exchange within human-robot interactions.	July 2018
Formal/2016-04-01 Finite State Machine Component for RTC (FSM4RTC) [263]	Defines further specifications for the Robotic Technology Component.	April 2016
Formal/2014-09-02 Ontology Definition Metamodel (ODM) [264]	Defines the metamodels, profiles and mappings corresponding to international standards, in order to aid the development of ontologies applicable to many potential users.	September 2014

OMG Document Number	Main Objective/ Standard Description	Date Published
Robotic Technology Component (RTC) [265]	Defines the component model for robotics software development.	September 2012

[a] Here, "DOL" is the abbreviation for the name of the standard, and does not indicate the Department of Labor.

SAE International

SAE International first released SAE J3016^{TM}, Recommended Practice: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, in 2014, and updated it in 2021. The Practice describes six levels of driving automation, from 0 to 5, along three dimensions: (1) what the human in the driver's seat must do, (2) what the driver support or automated driving features do, and (3) examples of these features. [142]

1.3.1.7. Description of Ways that Entities or Industry Sectors Develop, Implement, and Promote the Use of Artificial Intelligence

Many business practices common across all sectors—such as data analysis, customer service, advertising, and hiring—can be automated or augmented through the implementation of AI. Outside of those applications, AI is used for different business or product functions in each sector. Table 14 provides examples of sector-specific implementations of AI. These examples are illustrative, not exhaustive, and reflect only a handful of currently deployed AI applications.

Table 14. Examples of Ways that Industry Sectors Implement and Promote the Use of AI.

NAICS Code	Sector	Examples of AI Implementation and Promotion in This Sector
11	Agriculture, Forestry, Fishing and Hunting	Computer vision for livestock monitoring [71]; prediction and forecasting for precision agriculture [71]; targeted crop watering and soil management [266]
22	Utilities	Service optimization [14]; demand prediction [267]; consumption monitoring and reduction [267]
23	Construction	Monitoring of construction sites [268]; augmented planning [268]
31–33	Manufacturing	Process automation [268]; quality control [268]; throughput optimization [14]; predictive maintenance [14]; supply chain management [14]
42	Wholesale Trade	Inventory and delivery management [267]; customer relationships management [268]; demand forecasting [268]
44–45	Retail Trade	Inventory and delivery management [267]; marketing [268]; lead generation [268]; customer relationship management [268]; automated recommendation [268]; visual search [14]
48–49	Transportation and Warehousing	Automated vehicles in warehouses and on roads [268]; unmanned aircraft systems and mobile robots [268]; avionics and other measurement systems [268]; adaptive traffic management [268]
51	Information	Content recommendation [268]; biometric analysis [268]; speech and facial recognition [268]; human-computer interaction [14]; machine translation [14]
52	Finance and Insurance	Autonomous or augmented decision processes for lending and insurance [268]; credit rating [268]; investment algorithms and

NAICS Code	Sector	Examples of AI Implementation and Promotion in This Sector
		recommendations [268]; personal finance [268]; fraud detection and prevention [266]; risk management [14]
54	Professional, Scientific, and Technical Services	Molecular and drug discovery in scientific research [14]; automated case history analysis in law [266]
56	Waste Management	Automation of waste recycling [269]
61	Educational Services	Augmented instruction and assessment [268]; digital tutors [266]
62	Health Care and Social Assistance	Augmented imaging and diagnostics [268]; targeted treatment [266]; smart scheduling [267]; insurance processing [267]; physiological monitoring [268]; public health [268]
71	Arts, Entertainment, and Recreation	Automated recommendations [268]
72	Food Services	Forecasting inventory and demand; tracking staffing and sales; kiosk ordering; recommendations [270]

1.3.2. Federal Agencies with Jurisdiction

Today, there is no framework of mandatory industry regulations that explicitly targets non-government development and use of AI technologies. However, many Federal agencies have authority to regulate industrial activities that leverage AI technologies, depending on how existing authorities are applied. In addition, many agencies have missions that strongly overlap with different industrial sectors.

Table 15 lists Federal entities that have been specifically charged with providing oversight or guidance over the use of AI, the industry sectors they are responsible for, and the charging authority.

Table 15. Federal Entities Charged with Providing Oversight or Guidance over the Use of AI in Specific Sectors.

Department/ Agency	Sector (NAICS)	Authority	Description
EOP-OMB	Public Administration (92)	EO 13859 §6	The President directed OMB to develop guidance for the regulation of AI in the private Sector.
EOP-OMB	Public Administration (92)	EO 13960 §4	The President directed OMB to provide policy guidance to support better use of AI in government.

Table 16 lists agencies that have been directed to conduct a specific AI-related activity, for example, establish a Federal advisory committee or research program, along with the authority under which the agency was tasked.

Table 16. Federal Entities Required by Law or Directed by Executive Order to Conduct a Specific Activity Regarding AI.

U.S. Federal Department or Agency	Activities	Authority	Description
All agencies	Advance equity in AI	EO 14091 §4(b)	"When designing, developing, acquiring, and using artificial intelligence and automated systems in the Federal Government, agencies shall do so, consistent with applicable law, in a manner that advances equity."
GSA	AI Center of Excellence	AI in Government Act 2020 §103	Create a program within GSA to facilitate and improve the adoption of AI in Federal Government.
OMB, OSTP	Guidance for agency use of AI	AI in Government Act 2020 §104	Issue memorandum to inform agencies on development of policies regarding acquisition and use of AI technologies; recommended approaches to remove barriers to using AI; and identify best practices for identifying, assessing, and mitigating any discriminatory impact or bias from use of AI.
OPM	Update of Job Series	AI in Government Act 2020 §105	Identify key skills and competencies for AI related positions.
DOC, NOAA	Center for Artificial Intelligence	15 U.S.C.§9442	Coordinate and facilitate AI research across NOAA and expand external partners.
DOC	National Artificial Intelligence Advisory Committee (NAIAC)	15 U.S.C. §9414	Convene a Federal Advisory Committee to advise the President and the National AI Initiative Office on matters related to the Initiative.

U.S. Federal Department or Agency	Activities	Authority	Description
DOC	NAIAC Subcommittee on Law Enforcement	15 U.S.C. §9414(e)	Convene a Federal Advisory Committee to advise the President on matters relating to AI use in law enforcement.
DOC, NIST	Risk Management Framework for AI	15 U.S.C.§278 h-1(c)	Engage the public and private sector to develop a voluntary risk management framework for trustworthy AI systems.
DOE	AI Research Program	15 U.S.C. 9461	Advance cross-cutting R&D to advance AI relevant to DOE.
EOP-NSTC	Select Committee on Artificial Intelligence	EO 13859 §3 15 U.S.C. §9413	Coordinate activities in AI by implementing agencies. Serves as Interagency Committee named in the NAIIA.
EOP-OSTP	National Artificial Intelligence Initiative Office	15 U.S.C. §9412	Serve as point of contact for Federal AI activities. Promote access to and early adoption of technological innovations in AI.
GSA	Presidential Innovation Fellows program	EO 13960 §7	Establish an AI track to attract experts from industry and academia to undertake a period of work at an agency.
NSF	NASEM Artificial Intelligence Impact Study	NAIIA 2020 §5105	Commission a study on workforce impacts, needs, and opportunities caused by adoption of AI.
NSF, OSTP	National AI Research Resource Task Force	15 U.S.C. §9415	Develop a coordinated roadmap and implementation plan for creating and sustaining a National Artificial Intelligence Research Resource.
NSF and other participating agencies	National AI Research Institutes	15 U.S.C. §9431	Establish research institutes that focus on cross-cutting challenges in AI or applications to specific sectors.

Several recent Federal efforts address key areas related to AI and international trade. First, the International Trade Administration in the Department of Commerce issued in August of 2022 a Request for Comments “to gain insight on the current global AI market and stakeholder concerns regarding international AI policies, regulations, and other measures which may impact U.S. exports of AI technologies” [271]. In addition, new export controls have been issued for semiconductor technologies (the basis for computer hardware) by the Department of Commerce’s Bureau of Industry and Security [272].[17]

Table 17 provides a list of agencies that have general regulatory or non-regulatory jurisdiction over industry sectors with significant AI activity. In some cases, the agencies listed here are already involved in working with their sector(s) regarding AI. In other cases, they have not yet done so but are believed to have the jurisdiction to do so. This table excludes agencies that have been charged with providing oversight over the use of AI (listed

[17] Updated December 2022.

in Table 15) and agencies that have been ordered to conduct a specific AI-related activity (listed in Table 16). It also excludes agencies that have a primarily or exclusively foreign mandate and hence do not have jurisdiction over a U.S. industry sector.

Table 17. Agencies with General Jurisdiction or Oversight Functions for a Sector That Has AI Activity.

U.S. Federal Department or Agency	Sector (NAICS)
CFPB	Finance and Insurance (52)
CFTC	Finance and Insurance (52)
CPSC	Retail Trade (44-45)
DHS	Utilities (22), Manufacturing (31–33), Wholesale Trade (42), Transportation and Warehousing (48–49), Information (51), Public Administration (92)
DOC-BIS	All Sectors
DOC-NIST	All Sectors
DOC-USPTO	All Sectors
DoD	Manufacturing (31–33), Wholesale Trade (42), Public Administration (92)
DoD-DARPA	Public Administration (92)
DOE	Mining, Quarrying, and Oil and Gas Extraction (21), Utilities (22)
DOJ	All Sectors
DOJ-ATF	Manufacturing (31–33)
DOL	All Sectors
DOT	Transportation and Warehousing (48–49)
ED	Educational Services (61)
EEOC	All Sectors[a]
EPA	Administrative and Support and Waste Management and Remediation Services (56); Mining, Quarrying, and Oil and Gas Extraction (21); Construction (23); Transportation and Warehousing (48–49); Utilities (22)
FCC	Information (51)
FDIC	Finance and Insurance (52)
FFIEC	Finance and Insurance (52)
FRB	Finance and Insurance (52)
FTC	All Sectors
GSA	Public Administration (92)
HHS	Agriculture, Forestry, Fishing and Hunting (11), Health Care and Social Assistance (62)
HHS-FDA	Manufacturing (31–33)
HHS-ONC	Health Care and Social Assistance (62)
NASA	Public Administration (92)
ODNI-IARPA	Public Administration (92)
OPM	Public Administration (92)
SEC	Finance and Insurance (52)
Treasury	Finance and Insurance (52)
Treasury-OCC	Finance and Insurance (52)
Treasury-OFAC	Finance and Insurance (52)

U.S. Federal Department or Agency	Sector (NAICS)
Treasury-OIS	Public Administration (92)
U.S. Access Board	All Sectors
USDA	Agriculture, Forestry, Fishing and Hunting (11)
VA	Health Care and Social Assistance (62)

[a] The Federal Trade Commission has broad authority to protect consumers, workers, and honest businesses across almost all industry sectors with limited exceptions. Additionally, the Department of Justice's Antitrust Division and the Federal Trade Commission enforce laws that prevent firms from creating or exploiting market power that would distort or reduce innovation. This mandate applies broadly across industries including those associated with AI.

1.3.3. Interaction of Federal Agencies with Industry Sectors

Table 18 lists the agencies that have significant interactions with each industry sector that uses AI (a reorganization of the information in Table 16–Table 17). In many cases, this is because the agency has general jurisdiction over that sector.

Table 18. Agencies That Have Significant Interactions with Industry Sectors That Use AI.

Sector	Name	U.S. Federal Department or Agency
11	Agriculture, Forestry, Fishing and Hunting	DOC-BIS, DOC-NIST, DOC-USPTO, HHS, USDA, EPA, FTC
21	Mining, Quarrying, and Oil and Gas Extraction	DOC-BIS, DOC-ITA, DOC-NIST, DOC-USPTO DOE, EPA, FTC, DOI
22	Utilities	DOC-BIS, DOC-ITA, DOC-NIST, DOC-USPTO DHS, DOE, FTC
23	Construction	DOC-BIS, DOC-ITA, DOC-NIST, DOC-USPTO, FTC
31–33	Manufacturing	DOC-BIS, DOC-ITA, DOC-NIST, DOC-USPTO, DHS, DoD, DOJ-ATF, FTC, HHS-FDA
42	Wholesale Trade	DOC-BIS, DOC-ITA, DOC-NIST, DOC-USPTO, DHS, DoD, FTC
44–45	Retail Trade	CPSC, DOC-BIS, DOC-ITA, DOC-NIST, DOC-USPTO, FTC
48–49	Transportation and Warehousing	DOC-BIS, DOC-ITA, DOC-NIST, DOC-USPTO, DHS, DOT, FTC
51	Information	DOC-BIS, DOC- ITA, DOC-NIST, DOC-USPTO, DHS, FCC, FTC
52	Finance and Insurance	CFPB, CFTC, DOC-BIS, DOC-ITA, DOC-NIST, DOC-USPTO, FDIC, FFIEC, FRB, FTC, SEC, Treasury-OCC, Treasury-OFAC, Treasury
53	Real Estate and Rental and Leasing	DOC-BIS, DOC-NIST, DOC-USPTO, FTC
54	Professional, Scientific, and Technical Services	DOC-BIS, DOC-ITA, DOC-NIST, DOC-USPTO, FTC
55	Management of Companies and Enterprises	DOC-BIS, DOC-NIST, DOC-USPTO, FTC

Sector	Name	U.S. Federal Department or Agency
56	Administrative and Support and Waste Management and Remediation Services	DOC-BIS, DOC-ITA, DOC-NIST, DOC-USPTO, EPA, FTC
61	Educational Services	DOC-BIS, DOC-ITA, DOC-NIST, DOC-USPTO, ED, FTC
62	Health Care and Social Assistance	DOC-BIS, DOC-ITA, DOC-NIST, DOC-USPTO, FTC, HHS, VA
71	Arts, Entertainment, and Recreation	DOC-BIS, DOC-ITA, DOC-NIST, DOC-USPTO, FTC
72	Accommodation and Food Services	DOC-BIS, DOC-ITA, DOC-NIST, DOC-USPTO, FTC
81	Other Services (except Public Administration)	DOC-BIS, DOC-ITA, DOC-NIST, DOC-USPTO, FTC
92	Public Administration	DOC-BIS, DOC-NIST, DOC-USPTO, DoD, DoD-DARPA, DHS, EOP-OMB, FTC, GSA, NASA, ODNI-IARPA, OPM, Treasury-OIS

1.3.4. U.S. Federal Government Interagency Activities

1.3.4.1. National Science and Technology Council (NSTC) Groups

The White House National Science and Technology Council (NSTC) helps to coordinate the process of science and technology policymaking across the Federal Government in alignment with the President’s priorities and policy agenda. The NSTC aims to ensure that science and technology are taken into consideration in development of Federal policies and programs, and to advance international cooperation in science and technology. NSTC participants include senior (including several cabinet-level) officials from Federal science and technology agencies organized into six main committees (S&T Enterprise, Environment, Homeland and National Security, Science, STEM Education, and Technology), along with numerous subcommittees and a few select committees.

Three NSTC entities contribute to coordination and planning of Federal AI R&D efforts: The Select Committee on Artificial Intelligence (SCAI, a special NSTC committee including members at the cabinet level), the Subcommittee on Machine Learning and AI (MLAI-SC), and the AI R&D Interagency Working Group (IWG) of the Subcommittee on Networking and Information Technology R&D (NITRD), as indicated in Table 19. The NITRD and MLAI subcommittees fall under the NSTC Committee on Technology.

Table 19. NSTC Groups Focused on AI.

Activity/Entity	Participating U.S. Federal Departments or Agencies	Description
NSTC Select Committee on Artificial Intelligence (SCAI) [273; 274]	DOC, NSF, DOE, USDA, DOC, DoD, ED, DHS, DOI, DOJ, State, DOT, Treasury, VA, FDA, NIH, NSA, NASA, NSF, ODNI, EOP-NSC, EOP-OMB, EOP-OSTP (co-chair)	Established in 2018 by White House Charter; rechartered in 2021. Also serves as the Interagency Coordination Committee identified in the NAII A. "[A]dvises the White House on interagency AI R&D priorities and improving the coordination of Federal AI efforts to ensure continued U.S. Leadership in this Field." Focuses on AI R&D, competitiveness, education, workforce, and societal implications; additional co-chairs rotate between DOC, NSF, and DOE.
NSTC Subcommittee on Machine Learning and AI (MLAI-SC) [275]	DOC (co-chair), DoD, ED, DOE (co-chair), HHS, DHS, DOJ, DOL, State, DOT, VA, USAID, CIA, GSA, NSF (co-chair), NSA, ODNI, SSA, EOP-CEA, EOP-DPC, EOP-OMB, EOP-OSTP (co-chair), EOP-OVP, EOP-NEC, EOP-NSC.	Carries out tasks from the SCAI; "updates and maintains the National AI R&D Strategic Plan; and identifies and contributes to important policy issues for AI R&D, datasets, computational infrastructure, testing, standards, benchmarks, education, outreach, and related areas."
AI Interagency Working Group (IWG) of the NSTC Subcommittee on Networking and Information Technology Research and Development (NITRD) [276]	Multiple agencies; no official list	Supports activities of the SCAI and MLAI-SC and gathers information to help inform Federal strategy and investment.
NITRD Video and Analytics (VIA) Team [276]	Multiple agencies; no official list	Reports to the NITRD AI R&D IWG.

1.3.4.2. Other Interagency Coordination Mechanisms through the Executive Office of the President

Several additional efforts to coordinate Federal activities related to AI research, development, and deployment are underway in the Executive Office of the President (EOP), as listed in Table 20. In particular, the National AI Initiative Office (NAIIO), established under 15 U.S.C §9412, provides a central office for coordinating the initiative.

Table 20. Other U.S. EOP-led Entities That Participate in Coordination of AI Activities.

Activity/Entity	Participating U.S. Federal Entities	Description
National AI Initiative Office (NAIIO) [277]	EOP, NSTC agencies, U.S. Government writ large	Officially launched with the passage of the NAIIA, to oversee interagency coordination of the National Artificial Intelligence Initiative, provide support to the relevant NSTC committees, conduct public outreach, and promote access to outcomes of Initiative activities throughout the Federal Government.
EOP-OMB Office of Information and Regulatory Affairs (OIRA) [278]	EOP-OMB-OIRA and all affected agencies	In the event of development of any draft agency regulations related to AI deemed "significant" per EO 12866, OIRA will ensure that all interested or potentially impacted agencies will have an opportunity to provide input.
OMB Chief Information Officer (CIO) Council [279; 280]	OMB and 28 other executive branch agencies	A Forum of Chief Federal Information Officers focused on improving Federal IT practices. Addresses issues related to Federal IT workforce, data, cybersecurity, technology business management, and cloud services.
EOP Interagency Policy Committees (IPC) [281]	EOP and Federal departments and agencies	IPCs are the main day-to-day fora for interagency coordination of all-of-government policy and are established as needed. This mechanism can be used to coordinate on AI-related issues if needed.
NSTC Subcommittee on Open Science [282]	OSTP and Federal departments and agencies that fund R&D	Coordinates agency efforts to improve access to machine readable scholarly publications and data resulting from federally funded research.

1.3.4.3. Other Interagency Coordination Activities

Other interagency coordination efforts led by executive branch agencies are listed in Table 21. This list does not include co-funding of activities such as the National AI Research Institutes listed in

. Beyond the formal mechanisms listed here, many agencies also have a Responsible AI Official (RAIO) to manage requirements around trustworthy AI and often serve as an agency's point of contact on such issues. RAIOs regularly communicate with each other, enabling communication and planning across agencies, and serve as subject matter experts on trustworthy AI and other Federal AI initiatives.

Table 21. Other U.S. Federal Interagency Coordination Activities or Entities for AI.

Activity or Entity	Participating U.S. Federal Departments or Agencies	Description
AI Standards Coordination Working Group (AISCWG) of the Interagency Committee on Standards Policy (ICSP)	NIST, DHS, NSF (co-chairs); other ICSP agencies	Facilitates the coordination of Federal Government agency activities related to the development and use of AI standards, develops recommendations relating to AI standards to the ICSP, as appropriate, and supports NIST's role as Federal Coordinator for AI Standards [283].

Activity or Entity	Participating U.S. Federal Departments or Agencies	Description
Agency Inventories of AI Use Cases[a]	EOP-OMB, EOP-OSTP, CIO Council, Federal agencies	Coordinated across Federal agencies to publish inventories of non-classified and non-sensitive AI use-cases of the Federal Government [284].
U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools	NIST, other agencies	NIST's plan for coordinating Federal agency engagement and prioritization of AI standards development [285].
Hiring Initiative to Reimagine Equity[a]	EEOC and DOL-OFCCP	A multi-year, collaborative initiative that engages stakeholders to help reimagine hiring practices, including those that leverage AI [286].
Interagency Health AI Community[a]	VA and staff at any Federal agency	A professional interest group for any Federal staff engaged in health and medicine and AI [287].
GSA AI Center of Excellence (CoE) and Community of Practice	GSA, any Federal entity	"The Artificial Intelligence (AI) CoE incorporates machine learning, neural networks, intelligent process design and Robotic Process Automation (RPA) to develop AI solutions that address unique business challenges agency-wide. The team provides strategic tools and infrastructure support to rapidly discover use cases, identify applicable artificial intelligence methods, and deploy scalable solutions across the enterprise" [288].
GSA Robotic Process Automation Community of Practice[a]	GSA, any Federal entity	Engages Federal agencies and staff to develop effective and high-impact programs for robotic process automation and facilitates information sharing and dissemination of best practices [289].
Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning[a]	Treasury-OCC, Board of Governors of the Federal Reserve System, FDIC, BCFP, NCUA	A collaborative effort to gather stakeholder input on the use of AI/ML by financial institutions, including whether clarifications from agencies would be helpful (86 FR 16837).
All Services Personnel and Institutional Readiness Engine (ASPIRE)[b]	VA, NASA, Navy, Air Force, DOL	Cross-agency program for AI knowledge assessment as well as training/upskilling coordination and collaboration

[a] Updated December 2022.
[b] Updated February 2023.

1.3.5. Regulations, Guidelines, and Other Policies Implemented by Federal Agencies

1.3.5.1. Non-Federal Use of AI

At the national level, there is no comprehensive regulatory framework specifically for private sector use of AI technologies. The U.S. Government approach to regulation of private sector use of AI has been largely based on the OMB Memorandum (M-21-06) "Guidance for Regulation of Artificial Intelligence Applications." This memorandum provides policy context for decisions about oversight of non-Federal use of AI technologies and calls for Federal agencies to avoid "regulatory and non-regulatory actions that needlessly hamper AI innovation and growth." The FDA has been working toward a framework for regulating AI-based software as a Medical Device, as described in its 2021 Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) Action Plan, and released in September 2022 guidance documents related to regulatory requirements and oversight for certain categories of medical software and devices (see Table 22). There are currently only two sections of the Code of Federal Regulations that focus on AI explicitly,[18] though regulations that target data practices, use of information technology in general, or specific application areas or industrial sectors may be applicable to research, development, or uses of AI systems. Several agencies have released guidance indicating how AI or algorithm-based actions are covered by existing policies and regulatory frameworks.

Recent AI-specific regulatory policies, guidelines, or related activities are listed in Table 22, including for governance of AI use to protect privacy, civil rights, and civil liberties. Many of these activities were highlighted in White House fact sheets from October 2022 (at the time of the White House's release of the *Blueprint for an AI Bill of Rights)* and May 2023. For example, EEOC's Artificial Intelligence and Algorithmic Fairness Initiative has resulted in issuance of two technical assistance publications, *Assessing Adverse Impact in Software, Algorithms, and Artificial Intelligence Used in Employment Selection Procedures Under Title VII of the Civil Rights Act of 1964*, and *The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees*. Several pending agency activities, not listed in Table 22, include plans for future release of a vision for *Advancing Health Equity by Design* (HHS) and guidance related to use of algorithms for tenant screening that might violate the Fair Housing Act (HUD) [290; 24; 23].[19]

[18] 15 C.F.R. § 917.21 (2022) and 15 C.F.R. § 7.3 (2022).

[19] This section was last updated in June 2023, but is likely not to be comprehensive and might no longer be current as of the time of release of this report, given the pace of technology and policy developments in this area.

Table 22. Policies or Activities Related to Regulation of AI.

Originating Federal Entity	Title	Category	Date	Description
OSTP	Request for Information: National Priorities for Artificial Intelligence[a] [23]	Request for Information	May 2023	Requests public comments to help update U.S. national priorities and future actions on AI.
EEOC	Assessing Adverse Impact in Software, Algorithms, and Artificial Intelligence Used in Employment Selection Procedures Under Title VII of the Civil Rights Act of 1964[a] [291]	Technical Assistance Document	May 2023	Provides information to assist employers in monitoring whether algorithmic decision-making tools have adverse impacts in hiring. Includes background information, such as definitions of AI and related terms and contexts and an overview of Title VII, and questions and answers for employers. Part of EEOC's Artificial Intelligence and Algorithmic Fairness Initiative.
Department of Education	Artificial Intelligence and the Future of Teaching and Learning: Insights and Recommendations (2023)[b] [292]	Report with Insights and Recommend-ations	May 2023	Insights and recommendations related to AI policy action for teachers, educational leaders, policy makers, researchers, and educational technology innovators.
CFPB, DOJ Civil Rights Division, EEOC, FTC	Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems [293]	Joint Statement	April 2023	Joint informational statement affirming that these agencies' enforcement authorities apply to automated systems and that they will continue to monitor the development and use of automated systems and use their collective authorities to protect individuals' rights whether or not advanced technologies are involved.
EOP-OSTP	Blueprint for an AI Bill of Rights (2022)[c] [294]	Report with Principles and Framework	October 2022	Describes five principles and practices to help guide the design, use, and deployment of automated systems to help protect public civil rights, civil liberties, and privacy. These principles can provide guidance where existing law or policy guidance is absent or unclear.
DOC-BIS	Export Controls on Advanced Computing and Semiconductor Manufacturing Items to the People's Republic of China[c] [272]	Rules	October 7, 2022	Updates export control rules to restrict the People's Republic of China's ability to purchase and manufacture advanced microelectronics of use in military applications, including AI-enabled applications.
FDA	Medical Device Data Systems (MDDS), Medical Image Storage Devices, and Medical Image Communications Devices[c] [295]	Guidance Document	September 2022	Guidance for industry and FDA staff on the agency's intended approach to regulatory oversight of device- and non-device MDDS.

Originating Federal Entity	Title	Category	Date	Description
FDA	Computer Software Assurance for Production and Quality System Software[c] [296]	Draft Guidance	September 2022	Draft guidance, for public comment, on methods and testing approaches for medical device production and quality system computer software assurance that fulfill regulatory requirements.
DOC-ITA	Request for Comments on Artificial Intelligence Export Competitiveness[c] [271]	Notice on Request for Comments	August 2022	Request for public comments on questions relating to international trade, standards, export policies, and U.S. international competitiveness in AI.
VA	Final Rule: Principle-Based Ethics Framework for Access to and Use of Veteran Data[c] [297]	Final Rule	July 2022	Amends VA regulations to implement a principles-based ethics framework to be applied by anyone accessing, sharing, or using veteran data or conducting associated oversight.
HHS-CMS	Comment Solicitation on Payment Policy for SaaS Procedures (and other provisions)[c] [298]	Proposed Rule with Request for Public Comment	July 2022	Proposed rule spanning a variety of issues that includes request for public comment on how to "encourage software developers and other vendors to prevent and mitigate bias in their algorithms and predictive modeling."
HHS-CMS, HHS-OCR	Nondiscrimination in Health Programs and Activities[c] [299]	Proposed Rule	August 2022	Proposed revisions to interpretation of Section 1557 of the Affordable Care Act, including explicit prohibition of discrimination by covered entities when using clinical algorithms for decision making.
EEOC	The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employee [300]	Technical Assistance Document	May 2022	Provides background information with definitions of AI and related terms and questions and answers for employers, job applicants, and employees related to how the Americans with Disabilities Act applies in the context of algorithms. Part of EEOC's Artificial Intelligence and Algorithmic Fairness Initiative.
CFPB	Consumer Financial Protection Circular 2022-03: Adverse Action Notification Requirements in Connection with Credit Decisions Based on Complex Algorithms[c] [301]	Circular	May 2022	Clarifies that the Equal Credit Opportunity Act and Regulation B require that creditors provide written statements to applicants explaining why adverse actions were taken against them even if decisions were based on complex algorithms.
FTC	Trade Regulation Rule on Commercial Surveillance[c] [302]	Advance Notice of Proposed Rulemaking	February 2022	Advance notice of proposed rulemaking under section 18 of the FTC Act to examine whether rules addressing lax security practices, privacy abuses, and algorithmic decision making are appropriate. [302]

Originating Federal Entity	Title	Category	Date	Description
HHS-AHRQ	Impact of Healthcare Algorithms on Racial and Ethnic Disparities in Health and Healthcare[b] [303]	Research Protocol	January 2022	A research protocol for examining ways in which healthcare algorithms and algorithm-informed tools contribute to health and healthcare disparities by race or ethnicity. To be released as a report for public comment.
EEOC	Artificial Intelligence and Algorithmic Fairness Initiative [304]	Agency Initiative	October 28, 2021	An initiative to gather information and examine how technology is changing how employment decisions are made, provide technical assistance, and identify promising practices to provide guidance on ensuring that technologies are used fairly and consistently with Federal equal employment opportunity laws.
Treasury-OCC, Board of Governors of the Federal Reserve System, FDIC, BCFP, NCUA	Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning[c] [305]	Notice with Request for Information and Comment	March 31, 2021	Requests stakeholder input on the use of AI/ML by financial institutions, including whether clarifications from agencies about compliance with law and regulations would be helpful.
FDA	Artificial Intelligence/ Machine Learning-Based Software as a Medical Device Action Plan [306]	Plan	January 2021	Provides a series of actions for the FDA to advance oversight of AI/ML-based software as a medical device, including advancement of a regulatory framework.
DOC	Securing the Information and Communications Technology and Services (ICTS) Supply Chain (15 CFR §7 2022; 86 FR 4923)	Regulation	January 2021	Provides authority to the Secretary of Commerce to review and prohibit ICTS transactions for security reasons, explicitly including ICTS integral to AI (15 CFR §7.3 2022), in alignment with EO13875.

[a] Updated June 2023.

[b] Updated May 2023.

[c] Updated December 2022.

1.3.5.2. Federal Use of and Efforts in AI

The principles set out in Executive Order 13960, “Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government,” guide Federal Government uses of AI, and may affect contractors who work directly with Federal agencies. Action by the EOP and the work of individual Federal agencies will shape the use of AI for government operations, including in what ways these AI systems adhere to principles outlined in Section 3 of the Executive Order 13960. The White House has announced that OMB plans to release Draft Guidance on AI systems used by the Federal government for public comment [24].

At the agency level, there are often plans, guidelines, frameworks, or initiatives in place that address specific concerns and areas of AI implementation unique to the agency. Several Federal agencies have each published AI strategies, plans, or policies governing Federal efforts to advance or deploy AI technologies.[20] Executive Order 14091 "Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government," released on February 16, 2023, enhances requirements for Federal agencies in advancing equity, explicitly including rooting out bias in the design of artificial intelligence; designing, developing, acquiring, and using AI and automated systems, consistent with applicable law, in a manner that advances equity; ensuring that their respective civil rights offices are consulted on decisions regarding the design, development, acquisition, and use of artificial intelligence and automated systems; and protecting the public against algorithmic discrimination [307].[21] The Administrative Conference of the United States has released two recommendations and several ongoing efforts relating to use of AI systems in the Federal government [308]. A list of policies governing AI-related Federal activities is provided in Table 23.

[20] A current list of Federal agency and interagency strategic documents is maintained online at https://www.ai.gov/strategy-documents/.A fact sheet listing of recent executive branch activities related to AI governance, published at the time of release of the Blueprint for an AI Bill of Rights, is available at: https://www.whitehouse.gov/ostp/news-updates/2022/10/04/fact-sheet-biden-harris-administration-announces-key-actions-to-advance-tech-accountability-and-protect-the-rights-of-the-american-public/.

[21] Updated April, 2023.

Table 23. Current Policies Governing AI-related Federal Activities.[*]

Originating Federal Entity	Federal Entity Governed	Category	AI-relevant Policy	Description
OMB	OMB	Draft Policy Guidance	OMB Draft Guidance on AI systems used by the Federal government (anticipated Summer 2023)[a] [24]	Planned release of draft OMB policy guidance on the use of AI systems by the U.S. government. The policy will guide the development, procurement, and use of AI systems in Federal agencies and departments.
NSTC	Federal S&T agencies	Strategic Plan	The National Artificial Intelligence Research and Development Strategic Plan: 2023 Update[b] (May 2023) [309]	The 2023 update to the National Artificial Intelligence R&D Strategic Plan reaffirms eight strategies from the 2016 and 2019 plans and adds a ninth goal to establish a coordinated approach to international collaboration on AI R&D.
NIST	NIST	Resource Center	Trustworthy and Responsible Artificial Intelligence Resource Center (AIRC) (March 2023)[b] [310]	Supports the development and deployment of trustworthy and responsible AI technologies, operationalizes the NIST AI RMF and AI RMF Playbook, and provides resources related to AI.
EOP	Federal agencies	Executive Order	Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government (EO 14091) (February 2023)[c] [307]	Enhances equity-advancing requirements for agencies, including to "root out bias in the design of new technologies, such as artificial intelligence;" design, develop, acquire, and use AI and automated systems, "consistent with applicable law, in a manner that advances equity;" "ensure that their respective civil rights offices are consulted on decisions regarding the design, development, acquisition, and use of artificial intelligence and automated systems;" and "prevent and remedy discrimination, including by protecting the public from algorithmic discrimination."
U.S. Equal Employment Opportunity Commission (EEOC)	EEOC	Draft Plan	EEOC's FY2023-2027 Strategic Enforcement Plan (January 2023)[b] [311]	Released for public comment in 2023. The plan aims to eliminate barriers in recruiting and hiring related to the use of automated systems, including AI, as recruitment or screening tools that may disproportionally impact workers based on their protected status.

Originating Federal Entity	Federal Entity Governed	Category	AI-relevant Policy	Description
NIST	NIST	Conference	Trustworthy AI Conference (TRUC) (October 2022)[b] [312]	Conference to Identify risks and harms posed by AI technologies and guidance on managing those risks.
EOP-OSTP	Federal agencies	Principles/ Framework	Blueprint for an AI Bill of Rights (October 2022)[c] [294]	Describes five principles and practices to help guide the design, use, and deployment of automated systems to help protect public civil rights, civil liberties, and privacy. These principles provide guidance where existing law or policy guidance is insufficient for protections.
VA	VA	Final Rule	Final Rule: Principle-Based Ethics Framework for Access to and Use of Veteran Data (July 2022) [297]	Amends VA regulations to implement a principles-based ethics framework to be applied by anyone accessing, sharing, or using veteran data or conducting associated oversight.
DoD	DoD	Strategy and Implementation Pathway	Responsible AI (RAI) Strategy and Implementation Pathway (June 2022)[c] [313]	Provides a strategy and identifies lines of effort for DoD implementation of RAI in accordance with six tenants: (1) RAI governance, (2) Warfighter trust, (3) AI product and acquisition lifecycle, (4) Requirements validation, (5) RAI ecosystem, and (6) AI workforce.
U.S. Nuclear Regulatory Commission (NRC)	NRC	Strategic Plan	Artificial Intelligence Strategic Plan Fiscal Years 2023-2027 (June 2022)[b] [314]	A plan to help ensure NRC's readiness to review and evaluate uses of a broad spectrum of AI technologies
EEOC	Federal agencies	Technical Assistance Document	The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees [300]	Provides background information with definitions of AI and related terms and questions and answers for employers, job applications, and employees related to how the Americans with Disabilities Act applies in the context of algorithms. Part of EEOC's Artificial Intelligence and Algorithmic Fairness Initiative.
USAID	USAID	Action Plan	Artificial Intelligence Action Plan: Charting the Course for Responsible AI in USAID Programming (May 2022) [315]	Describes the agency's approach to AI, including (1) committing to responsible AI in USAID programming, (2) strengthening digital ecosystems to support responsible AI use, and (3) partnering to shape a global responsible AI agenda.

Originating Federal Entity	Federal Entity Governed	Category	AI-relevant Policy	Description
DOT	National Highway Traffic Safety Administration (NHTSA)	Final Rule	Occupant Protection for Vehicles With Automated Driving Systems (March 2022)[b] [316]	Amends the Federal Motor Vehicle Safety Standards to include protections for occupants with automated driving systems.
NGA	NGA	Strategy	NGA Data Strategy (October 2021) [317]	Sets a vision around the role of data in the NGA and provides 4 key goals: (1) manage data as a strategic asset, (2) deliver shared data services, (3) scale data and analytics capabilities, and (4) bolster data literacy in the workforce.
State	State	Strategy	Enterprise Data Strategy (September 2021) [318]	Establishes an enterprise approach to the use and application of data across the Department, along with strategic goals dealing with data analytics, management and governance.
DoD	DoD	Strategy	Department of the Navy Science & Technology Strategy for Intelligent Autonomous Systems (July 2021) [319]	Sets new goals and an execution plan around building the capabilities, processes and partnerships related to the use of intelligent autonomous systems for the Navy.
DHS	DHS	Strategic Plan	S&T Artificial Intelligence & Machine Learning Strategic Plan (July 2021) [320]	Sets the approach around the implementation of AI and ML technologies within DHS, including specific goals around building technical capabilities and developing a workforce trained in AI.
VA	VA	Strategy	U.S. Department of Veterans Affairs Artificial Intelligence (AI) Strategy (July 2021) [321]	Defines strategic goals and priorities around the use, development and deployment of AI technologies in order to improve veteran outcomes, build trust, and enhance capabilities within the VA.
DoD	DoD	Plan	Artificial Intelligence Governance Plan (June 2021) [322]	Clarifies the AI governance structures within the DoD, and demonstrates how the DoD can integrate AI in line with the National Defense Strategy and DoD Digital Modernization Strategy.
GAO	Federal agencies	Framework	An Accountability Framework for Federal	Guidance to help ensure accountability and responsible use of AI in government. Provides four complementary principles.

Originating Federal Entity	Federal Entity Governed	Category	AI-relevant Policy	Description
			Agencies and Other Entities (June 2021) [322]	
Congress	U.S. Government-wide	Initiative	National Artificial Intelligence Initiative (January 2021) [323]	Initiative to coordinate and aim Federal Government resources toward accelerating AI research, development, demonstration, and education.
HHS	HHS	Strategy	U.S. Department of Health and Human Services Artificial Intelligence (AI) Strategy (January 2021) [324]	Outlines foundational priorities, steps and goals towards advancing AI applications and governance for HHS.
Administrative Conference of the United States	Federal agencies	Statement	Agency Use of Artificial Intelligence (December 2020) [325]	Identifies issues that "agencies should consider when adopting or modifying AI systems and developing practices and procedures for their use and regular monitoring," informed by two commissioned reports and input from AI experts drawn from all sectors.
EOP	Federal agencies	Executive Order	Promoting the Use of Trustworthy AI in the Federal Government (EO 13960) (December 2020) [327]	Principles to ensure AI design, development, and use by Federal agencies is done to promote trustworthiness. Directs OMB to develop guidance for implementation.
EOP-OMB	Federal agencies	Memorandum with Guidance and Principles	Guidance for Regulation of Artificial Intelligence Applications (M-21-06, November 2020) [278]	Provides policy context and principles to Federal agencies for governance and stewardship of non-Federal uses of AI.
ODNI	IC agencies	Framework	Artificial Intelligence Ethics Framework for the Intelligence Community (June 2020) [328]	Framework to guide AI and data procurement, design, development, use, and management for the intelligence community.
NOAA	NOAA	Strategy	NOAA Artificial Intelligence Strategy (February 2020) [329]	Defines five strategic goals and detailed objectives for augmenting the development and use of AI across NOAA.
DoD	DoD	Principles	Ethical Principles for Artificial Intelligence (February 2020) [330; 331]	Defines DoD-specific principles around ethical AI, centered around five major principles for AI attributes: (1)

Originating Federal Entity	Federal Entity Governed	Category	AI-relevant Policy	Description
				Responsible, (2) Equitable, (3) Traceable, (4) Reliable, and (5) Governable.
DoD	DoD	Framework	The United States Air Force Artificial Intelligence Annex to the Department of Defense Artificial Intelligence Strategy (September 2019) [332]	Framework to describe concepts and objectives related to algorithms, data, information technology and partnerships for the Air Force.
NIST	Federal agencies	Plan	U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools (August 2019) [285]	Provides specific recommendations for Federal Government around developing AI standards, researching and incorporating trustworthiness into standards, supporting public-private partnerships, and engaging with international parties.
NSTC	Federal S&T agencies	Strategic Plan	The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update[b] (June 2019)	The 2019 update to the National Artificial Intelligence R&D Strategic Plan with eight strategies for advancing U.S. AI R&D [333].
DoD	DARPA	Investment	"AI Next" Campaign (September 2018)[b] [334]	A multi-year, $2 billion investment in over 50 new and existing AI programs within DARPA
DoD	DoD	Strategy	2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity (January 2018) [335]	Defines the strategic approach for DoD activities in AI, including both near-term priorities and broader strategic focus areas for continued efforts.

[*] A current list of Federal publications related to AI is available at: https://www.ai.gov/publications/ . [a] Updated May 2023. [b] Updated May 2023. [c] Updated December 2022.

1.3.5.3. International Coordination, Guidance, and Policies on AI

The United States engages with other nations to coordinate on research, development, deployment, principles, and standards for AI. One major channel for this coordination is through OECD, which serves as the executive secretary for the Global Partnership on AI, of which the United States is a founding member, to help advance and incorporate those shared principles for the sake of advancing AI research, trustworthiness, and responsible use, as well as the OECD Network of Experts on AI (ONE AI), an international group of experts that advises the OECD on AI policy. At the intersection of artificial intelligence and IP policy, the World Intellectual Property Organization (WIPO) has hosted a series of conversations on the impact of AI on IP policy, while the IP5 forum launched a NET/AI task force along with a roadmap for international cooperation [336; 337]. In addition, the U.S.-EU Trade and Technology Council has identified several key areas for collaboration. Additional details are provided in Table 24.

Table 24. Multi-nation Coordination Efforts for the Advancement of Responsible AI.

Coordination Effort	Lead Entity	Participating Nations	Purpose and Role
Global Partnership on Artificial Intelligence (GPAI) [60]	OECD	46 nations that support the OECD Recommendations on AI, including the U.S.	Multisector, multigovernmental, international partnership that aims to "bridge the gap between theory and practice on AI" international partners to advance (1) Responsible AI, (2) Data governance, (3) Future of work, and (4) Innovation and commercialization.
OECD Network of Experts on AI (ONE AI) [338]	OECD	30 nations	Brings together experts in AI policy, AI technology and other legal & ethical experts to provide AI policy advice for the OECD Committee on Digital Economy Policy and the OECD Policy Observatory on AI.
The WIPO Conversation on Intellectual Property and Artificial Intelligence [337]	World Intellectual Property Organization (WIPO)	Registered participants have represented 133 nations	Convenes intellectual property experts on an international level to discuss pressing issues and questions at the intersection of IP and AI.
IP5 NET/AI Task Force [336]	IP5 Forum	U.S., EU, Japan, Korea and China	Coordinates activities across the 5 nations' IP offices exploring the impact of AI on patent systems.
Quad Critical and Emerging Technologies Working Group (CETWG) [339]	Quad	U.S., Australia, India, and Japan	Since the launch of the CETWG in March 2021, U.S. has been leading the Standards Sub-group. The AI Contact Group established under the Sub-group has been coordinating with Quad partners on participation in standards-development activities across SDOs and foundational pre-standardization research.
U.S.-EU Trade and Technology Council (TTC) [340]	U.S. and EU	U.S. and EU nations	After the TTC's inaugural meeting in September 2021, the U.S. and EU issued a joint statement on AI, naming four areas for cooperation: (1) principles for trustworthy and

Coordination Effort	Lead Entity	Participating Nations	Purpose and Role
			responsible AI; (2) measurement and evaluation tools; (3) collaboration for trustworthy and responsible AI; (4) a joint study on AI and the future of work (released in January 2023).

In 2019, OECD member countries signed and agreed to adhere to the OECD AI Principles for promoting trustworthy and innovative AI that is respectful to democratic values and human rights, which provide a starting framework for countries to shape their national strategies on AI. In addition, ONE AI has published a *Framework for Classifying AI Systems* and a *Framework of Tools for Trustworthy AI*. Details of these guidance documents are provided in Table 25.

Table 25. Coordinated Intergovernmental Guidance on AI Deployment.

Entity	AI-relevant Policy	Category	Date Issued	Description
OECD ONE AI [341]	OECD Framework of Tools for Trustworthy AI	Draft Framework	June 28, 2021	This framework helps identify and analyze the potential tools for developing, issuing, and deploying trustworthy AI across many different contexts.
OECD ONE AI [342; 341]	OECD Framework for the Classification of AI Systems	Draft Framework	February 2, 2021	This framework assists policy makers, regulators and others to classify AI systems in order to compare unique opportunities and risks.
UNESCO [343]	Recommendation on Ethics	Framework	November 25, 2020	A global normative framework for AI ethics.
OECD [341; 344]	OECD AI Principles	Principles	May 22, 2019	These principles and recommendations present a framework for OECD members and other national governments to coordinate efforts towards trustworthy, transparent, and safe AI.

1.3.6. Federal Government Resources for Consumers and Small Businesses to Evaluate the Use of Artificial Intelligence

The Federal Government has provided a variety of resources that could help small businesses and consumers evaluate the use of AI, including in relation to issues such as privacy and ethical use of AI. Federal reports, frameworks, and other documents aimed at assisting non-governmental entities in evaluating or implementing AI systems are listed in Table 26.

Table 26. Federal Government Publications and Activities That Help Inform Non-Governmental Entities' Evaluation of AI Use

Originating Federal Entity	Resource Title	Resource Type	Publication or Launch Date	Description
GAO	Science & Tech Spotlight: Generative AI[a] [345]	Report	June 13, 2023	Provides an overview of technologies, opportunities, challenges, and policy context and questions associated with generative AI.
EEOC	Assessing Adverse Impact in Software, Algorithms, and Artificial Intelligence Used in Employment Selection Procedures Under Title VII of the Civil Rights Act of 1964[a] [291]	Technical Assistance Document	May 23, 2023	Provides information to assist employers in monitoring whether algorithmic decision-making tools have adverse impacts in hiring. Includes background information, such as definitions of AI and related terms and contexts and an overview of Title VII, and questions and answers for employers.
Department of Education	Artificial Intelligence and the Future of Teaching and Learning: Insights and Recommendations (2023)[b] [292]	Report	May 23, 2023	Insights and recommendations related to AI policy action for teachers, educational leaders, policy makers, researchers, and educational technology innovators.
FTC	The Luring Test: AI and the engineering of consumer trust[b]	Blog Post	May 1, 2023	Business guidance warning against the use of generative AI to manipulate consumers.
FTC	Chatbots, deepfakes, and voice clones: AI deception for sale[b]	Blog Post	March 20, 2023	Business guidance discussing the use of generative AI for fraud.
FTC	Keep your AI claims in check[b]	Blog Post	February 27, 2023	Business guidance warning marketers not to make exaggerated or unsubstantiated claims about AI products or services.
NIST	NIST AI Risk Management Framework (AI RMF 1.0)[b] [1]	Framework	January 2023	A voluntary framework for individuals and organizations to manage risk associated with AI more effectively. Includes online. companion resources: an *AI RMF Playbook*, *RMF Explainer Video*, *AI RMF Roadmap*, and an *AI RMF Crosswalk*.
NAIIO	AI Researchers Portal	Website with Links	2022	Portal providing links to resources for AI researchers including (1) Navigating Federal research funding

Originating Federal Entity	Resource Title	Resource Type	Publication or Launch Date	Description
				processes, (2) Data resources, (3) Computing resources, (4) Repository of AI research programs, and (5) Inventory of AI R&D testbeds.
FDA	Artificial Intelligence and Machine Learning (AI/ML)-Enabled Medical Devices[c] [346]	List of AI/ML-enabled Devices	October 5, 2022	Online and downloadable list of AI/ML-enabled medical devices marketed in the United States. Compiled from publicly available information as a resource for the public to be updated periodically.
EOP-OSTP	Blueprint for an AI Bill of Rights	Report with Framework and Principles	October 4, 2022	Describes five principles and practices to help guide the design, use, and deployment of automated systems to help protect public civil rights, civil liberties, and privacy. These principles provide guidance where existing law or policy guidance is insufficient for protections.
VA	AI@VA[c] [287]	Email Group		Provides a monthly newsletter with highlights of VA work and relevant Federal activities related to AI, collaboration opportunities, and invitations to informational events.
DOL	What the Blueprint for an AI Bill of Rights Means for Workers[c] [347]	Blog Post	October 4, 2022	Provides context on the implications of AI and the Blueprint for workers, and information about related DOL efforts being explored or underway.
DOE	AI Risk Management Playbook[c] [348]	Online Playbook	2022	Searchable guidance on managing different kinds of AI risks across the development lifecycle.
EOP and Federal agencies	Agency Inventories of AI Use Cases[c] [284]	Website	June 2022 (and subsequent updates)	Website linking to agency inventories of AI use cases disclosed in response to EO 13960.
FTC	Combatting Online Harms Through Innovation[c] [349]	Report	June 2022	A study directed by Congress to assess whether and how AI “may be used to identify, remove, or take any other appropriate action necessary to address” various specified “online harms.” [350]

Originating Federal Entity	Resource Title	Resource Type	Publication or Launch Date	Description
EEOC	The Americans with Disabilities Act and the Use of Software, Algorithms, and AI to Assess Job Applicants and Employees[c] [351]	Technical Assistance Document	May 12, 2022	Technical assistance that explains how employers' use of software that relies on algorithmic decisions may violate Title I of the Americans with Disabilities Act, along with promising practices for job applicants and employees.
DOJ	Algorithms, Artificial Intelligence, and Disability Discrimination in Hiring[b] [352]	Guidance Document	May 12, 2022	Guidance explaining how algorithms and AI can lead to disability discrimination in hiring.
CPSC	CPSC Artificial Intelligence and Machine Learning Test and Evaluation Forum[c] [353]	Forum	March 31, 2022	Public information- gathering forum on existing testing and evaluation capabilities for AI and ML-enabled consumer products and determining potential for risk to consumers.
NIST	Toward a Standard for Identifying and Managing Bias in Artificial Intelligence[c] [354]	Special Publication	March 15, 2022	Provides voluntary practical guidance for individuals and groups who play a role in the creation or use of AI systems, describing key aspects of potential harms or inequities due to bias in AI systems along with recommended practices.
USPTO	Artificial Intelligence Patent Dataset[c] [355]	Dataset	Updated August 2, 2021	Includes two publicly available online documents: (1) An ML-generated list of U.S. patents issued from 1976–2020 containing one or more AI technology components. (2) Patent documents on which the ML model was trained.
USPTO	AI-related Patent Resources[c] [356]	Online Resource List	March 18, 2020	Online list of USPTO AI-related patent resources, including on patent examination and legal decisions and compliance.
FTC	Aiming for truth, fairness, and equity in your company's use of AI [357]	Blog Post	April 19, 2021	A business blog post providing advice for business to consider when using AI. Provides recommendations for businesses and examples of laws that might govern business AI usage and fall under FTC jurisdiction.

Originating Federal Entity	Resource Title	Resource Type	Publication or Launch Date	Description
GAO	GAO AI Accountability Framework [322]	Report	June 1, 2020	A report outlining a framework with principles and practices for accountability in use of AI. Aimed at Federal agencies and other implementers of AI.
FTC	Using Artificial Intelligence and Algorithms [358]	Blog Post	April 1, 2020	A business blog post written by Andrew Smith, Director of the FTC Bureau of Consumer Protection. Provides advice for business to consider when using AI. Includes informal recommendations encouraging transparency and fairness.
USPTO	AI-related Patent Resources[c] [356]	Online Resource List	March 18, 2020	Online list of USPTO AI-related patent resources, including on patent examination and legal decisions and compliance.
NIST	Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management [359]	Framework	January 16, 2020	A "voluntary tool developed in collaboration with stakeholders intended to help organizations identify and manage privacy risk to build innovative products and services while protecting individuals' privacy."
FTC	Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues [360]	Report	January 1, 2016	A report on "Big Data" and AI usage in business contexts. Contains an analysis of the benefits and risks of using these technologies as well as policy and legal considerations for their use by businesses.

[a] Updated June 2023.
[b] Updated May 2023.
[c] Updated December 2022.

The government has also created and made available several technical testing and evaluation tools for developers or members of the public to characterize the performance of AI. For example, individuals with an institutional affiliation may submit facial recognition software to be evaluated via NIST's Facial Recognition Vendor Test as frequently as once every four months. NIST's Open Speech Analytic Technology Evaluation Series provides a variety of evaluation and development tools for human speech recognition and related tasks. More broadly, the Federal Government has developed or sponsored numerous (40 as of June 2023) physical and virtual testbeds—some AI-specific, others focused on a particular use-case or research domain—that "provide environments to support development of real-world applications of AI that are robust and trustworthy" [361]; a current list of these testbeds is maintained at https://www.nitrd.gov/apps/ai-rd-testbed-inventory/.

Other resources, including Federal data that might support development or TEVV of AI models, are available via the AI Researchers Portal at https://www.ai.gov/ai-researchers-portal. The NAIRR Task Force established by the National AI Initiative Act released in January 2023 a roadmap and implementation plan for a new national cyberinfrastructure to broaden access to Federal and non-Federal data, computational, and other resources in order to strengthen and democratize the U.S. AI innovation ecosystem [362]. Several other efforts to improve access to data for approved R&D purposes have been established or are underway. The COVID-19 Open Research Dataset (CORD-19) and CORD-19 Challenge, established through a public-private partnership in 2020, provided the largest collection of COVID-19-related research publications and incentivized researchers to develop AI-based tools for extracting key information to inform medical researchers and practitioners [63; 64]. In July 2022, the CHIPS Act authorized the National Secure Data Service demonstration program, a pilot for improving access to Federal data for approved research activities; these data could potentially support AI R&D. A Standard Application Process is now available for requesting access to confidential data for approved R&D purposes [363]. A full inventory of unclassified and non-sensitive Federal Government AI use cases is available at: https://www.ai.gov/ai-use-case-inventories/.[22]

Beyond these government-generated resources, the Federal Government funds a variety of third-party entities to conduct R&D or for contracting services or partnerships that may create resources of value for consumers and small businesses to evaluate the use of AI. For example, the Partnership on Employment & Accessible Technology (PEAT)—funded by DOL's Office of Disability Employment Policy—developed several resources in collaboration with DOL staff, which have been made available online. These resources include the AI & Disability Inclusion Toolkit and the Equitable AI Playbook, designed to help organizations navigate the potential risks of implementing AI technologies (specifically for people with disabilities), to outline practices for making AI implementations more equitable, and to define the business case for equitable AI to organizational leaders [364; 365]. A comprehensive list of third-party resources is outside the scope of this chapter.

1.4. Marketplace and Supply Chain

Because AI has potential applications across all industrial sectors, leadership in AI is important for innovation and national competitiveness. This section provides an overview of risks to the AI innovation ecosystem, and how exploitation of the AI supply chain and marketplace could threaten U.S. economic or national security.

1.4.1. Risks Posed to the Supply Chain and Marketplace

1.4.1.1. Supply Chain Risks

NIST defines a supply chain as the "[l]inked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the

[22] Text updated December 2022.

design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer" [366]. AI is neither a material product nor a single technology, but a category of advanced knowledge-based technologies. Here, we define an AI supply chain as inclusive of any resource—human, material, software, or informational—required to develop, deploy, and sustain an AI solution with commercial or other potential societal value. Broadly, this includes people capable of developing, supporting, and deploying AI solutions; algorithms, code, and other software elements that may be leveraged or adapted for a given application; computer hardware on which to develop or deploy AI models; and data resources with which to train or test models (especially in the case of ML, DL, and other data-intensive AI areas). Key risks associated with the AI innovation ecosystem are summarized in the following.

The U.S. AI ecosystem will not excel without a robust pool of technical talent for AI research, development, and deployment

The AI workforce spans a range of roles and functions, from entry-level engineers to experts in developing and implementing AI techniques to project managers. The AI workforce includes individuals with a range of educational experience, including different degree levels and fields. In industry, computing- and AI-related degrees (especially PhDs and master's) are highly valued. In 2019, U.S. academic institutions granted approximately 2,236 PhDs, 45,921 new master's degrees, and 89,524 bachelor's degrees in computer science and support services [367]. The 2020 CRA Taulbee survey of North American Institutions with information, computer science, and computer engineering PhD-granting departments reported that, of 2020 PhDs recipients in computing for which their specialty was known, AI/ML was the most popular area, at 19 percent [368].

There have been reports of a surge in demand for AI skills over the past 5 to 10 years, especially in the area of deep learning, data science, and other ML-related techniques [369]. These trends correlate with strong growth in wages for computer and information science researchers in recent years, and with large private sector salaries reported for individuals with AI skills [369]. Movement of AI researchers between firms could potentially be inhibited by firm non-compete agreements; FTC has sought to ban non-compete clauses in a January 2023 rulemaking [370].

More than half of the U.S. computer and mathematical sciences workers with graduate degrees were foreign born as of 2019 [371]. Estimates based on the 2021 CRA Taulbee survey suggest that approximately 64 percent of new North American AI PhDs were international students and more than 80 percent of international AI PhD graduates in 2019 remained in the United States for employment [13], suggesting that the U.S. relies heavily on foreign talent as a source of highly skilled AI workers. However, international students face hurdles in the U.S. immigration system, including long visa and green card wait times, visa restrictions, proposed changes associated with the Optional Practical Training program,[23] and the lack of an appropriate visa for individuals who wish to stay in the United States to create startup companies [373; 374]. These challenges also impact the small businesses that rely on a continuing influx of AI talent.

In academia, both difficulties in hiring qualified AI researchers and educators and a "brain drain" of AI faculty to industrial positions have been reported. The total number of North American AI

[23] The Optional Practical Training program enables F-1 visa holding students to receive up to 12 months of temporary employment authorization for work directly related to their field of study. National Institute of Standards and Technology, "AI Risk Management Framework: Second Draft - August 18, 2022" (2022), https://www.nist.gov/system/files/documents/2022/08/18/AI_RMF_2nd_draft.pdf.

faculty departures rose from 4 individuals in 2009 to 42 in 2018, dropping slightly to 33 in 2019—though the number of faculty whose research focused primarily on AI also appears to have increased over this time.[24] For these academics, the private sector can offer cutting-edge computing resources, extensive datasets, and financial support that go beyond the resources of academic institutions. Some believe that the loss of AI expert faculty from academia to industry will reduce capacity for training the next generation of AI experts, reduce the quality of training, or reduce the propensity for students to become entrepreneurs [13]. From 2010 to 2019 the share of new PhDs from AI-related fields employed by industry increased by 48 percent, while the share that entered academia fell by 44 percent [375; 13].

In one 2019 survey of AI researchers and university administrators, 89 percent of respondents reported that hiring and retaining AI experts was “difficult” or “very difficult.” Firms also report a “skills gap” and an “inability to attract specialized talent” as leading barriers to adopting new technologies (especially for emerging job roles in AI and ML) [66]. The Federal Government also faces significant challenges in attracting AI talent [66]. Efforts to map and address skills gaps within and across the Federal Government are underway, including programs such as the All Services Personnel and Institutional Readiness Engine (ASPIRE) AI Tech Sprint [57] and the AI training work required by the AI Training Act (Public Law 117-207). As with STEM fields more generally, efforts to support diversity and inclusion of underrepresented segments of the U.S. population in AI and computing could help to strengthen and broaden the U.S. AI talent pool.

A lack of diversity in the AI workforce may contribute to the incidence of discrimination, perpetuation of bias, and other harms resulting from the development and use of AI algorithms

Women and Black or African American or Hispanic workers have been historically underrepresented in the United States computing workforce. As of 2019, Women comprised only 26 percent of individuals in computer sciences and mathematics occupations, a broad category that includes AI workers [376]. As of 2017, only 13 percent of all workers in these occupations were Black, Hispanic, or American Indian or Alaska Native, with an estimated 17 percent of the college-educated workforce [377] compared to 33.2 percent of the U.S. population (18.5 percent Hispanic, 13.4 percent Black or African American, and 1.3 percent American Indian or Alaska Native) as of 2019 [378]. It has been found that a smaller share of scientists and engineers with disabilities are working in science and engineering occupations than are scientists and engineers without disabilities; however, publicly available data were not found for computer sciences and mathematics occupations or for AI occupations in particular [379].

Similar diversity trends are observed throughout higher education in computer science generally, including in AI. The Computing Research Association’s 2021 Taulbee survey results suggest that among tenured or tenure-track computer science faculty, fewer than 21 percent were female, 1 percent were Black or African American, and 2 percent were Hispanic (any race) [368]. Only 18 percent of North American PhD recipients in AI were female [13]. Of all U.S. AI Ph.D. recipients who were U.S. citizens or permanent residents, 2.4 percent were Black or African American and 3.2 percent were Hispanic—similar statistics to those for PhDs in all areas of computing [13]. According to the National Center for Science and Engineering Statistics Survey

[24] According to the 2021 AI Index Report, the number of faculty whose research focused primarily on AI increased from 105 to 167 between academic years 2016-17 and 2019-20; data are not available for earlier years.

of Earned Doctorates, approximately 6.1 percent of all computer and information science PhD recipients in 2019 reported having a disability, compared to 8.6 percent of all science and engineering PhD recipients and 10.8 percent of all non-science and engineering PhD recipients [379].

It is generally accepted that underrepresentation of demographic groups in the research, development, design, and implementation of IT can result in commercialization and deployment of IT products that do not serve all segments of a population equally well. Numerous examples exist of instances where deployed ML algorithms have discriminated against individuals based on gender, race, ethnicity, disability, or skin tone—for example, in the context of hiring decisions, healthcare recommendations, recidivism predictions or criminal sentencing, and facial recognition [380; 381].[25] There is some evidence that a lack of diversity of perspectives and experiences among AI developers has contributed to such harms, and may in general perpetuate historical inequities, bias, and discrimination [381]. Harms due to algorithmic bias and discrimination have implications for privacy, equity, civil rights, and civil liberties—and also decrease justified trust in commercially deployed AI systems, with potential ramifications for industry.

While many high technology companies have recently engaged in efforts to improve the diversity or their workforce, there is little evidence of change over the past decade or so [315]. Beyond merely increasing diversity in the AI workforce, integration of diverse voices into decision making about high technology development and deployment will be needed to improve fairness of AI systems [382]. Furthermore, there is skepticism about whether these efforts are intended to bring about real change, or simply improve these companies' images or enable them to capture a broader market share. On the other hand, relying on representatives of groups most likely to experience harm to identify and mitigate such effects is a neither fair nor complete solution—though increasing representation of these groups will have the effect of distributing the burden [381]; without building rigorous consideration of social dimensions of AI (such as fairness, accountability, and transparency) into AI education, training, and system design, these issues are likely to persist or worsen.

In addition to race, ethnicity, gender, disability, age, and life experience, disciplinary expertise is an important aspect of diversity in the AI workforce. While AI is inherently related to computing and information and communication technologies, deployed AI tools are fundamentally sociotechnical systems that interact with and affect humans and society. Public misconceptions about what AI is, how it works, and its limitations can adversely affect the ability to gain advantage from its use and related technologies. Inclusion of sociology, human factors, psychology, technology, law, and other fields into AI education and training and as a key dimension of the AI ecosystem is important for understanding the implications of technologies, optimizing their design and deployment for positive societal impact, mitigating risk, and supporting an ecosystem of more secure, trustworthy, and equitable AI systems that protect privacy, civil rights, and civil liberties.

Open source code, libraries, and other software elements support development of AI systems and wide vetting of code, but can pose risks to system security and integrity

[25] Such ML-based discrimination can occur as a result of relying on historical data that reflect systemic inequities, are not representative, or are otherwise of poor quality; bias or error in the process of labeling training data; bias in parameter optimization in the model training process itself; or biased, inappropriate, or unconsidered application of a particular model for a given use case.

Open source AI software is an integral part of AI development and implementation. Open-source software (OSS) grants users the freedom to run the software for any purpose, to modify the program, and to freely redistribute original or modified programs. In comparison with proprietary software—programs and systems that are not available for examination, modification, and redistribution—OSS provides several advantages.

AI OSS provides building blocks for development of AI systems by a wider range of users, with a lower barrier to entry, and can distribute development costs and labor across multiple individuals or organizations. The most advanced and widely used ML tools and architectures are freely available and open source. Google's TensorFlow and Facebook's PyTorch are among the most popular deep learning libraries and are both open source, as are other popular ML tools such as Scikit-learn in Python and tidymodels in R [383]. Although machine learning frameworks are often open-source, large foundation models are not. Accessing these models may be prohibitively expensive to researchers and small businesses.

Openly available source code can be examined before it is adopted or incorporated into an AI program or system. This allows users to understand how the code works, to adapt it if desired, and to inspect it to determine whether it meets their security needs. Furthermore, the openness and wide availability of OSS enables it to be evaluated by many users, creating a system of mass peer review that essentially crowdsources the efficient identification of and fixes for security or other flaws. Benefits like these have made OSS extremely popular for AI development.

However, the openness of OSS code for inspection does not necessarily guarantee a rigorous review for bugs or security vulnerabilities, or that such bugs will be corrected rather than exploited. In addition, OSS can be poorly maintained or abandoned—there is no guarantee that it will have longevity[384].[26] While proprietary software also faces these risks, the incentives for maintaining and patching proprietary software and OSS may be different. Whether the risks are greater for an instance of OSS than for similar proprietary software will vary from case to case. The availability of software elements that are well vetted, maintained, and documented for AI development will affect the shape of the AI innovation ecosystem, including who may contribute.

The United States currently has limited manufacturing capacity for microelectronics, and manufacturing capacity for leading-edge microelectronics is concentrated entirely outside of the United States

AI algorithms must be implemented on computer hardware, which is today based on semiconductor microelectronics (or, simply "semiconductor") technologies, also known as computer chips or microchips. Semiconductor production can be generally divided into two stages: device circuit design and device fabrication. These two processes can be performed by the same company—called an Integrated Device Manufacturer (IDM)—or distinct companies, in a process known as the foundry model. In the foundry model, circuits are designed by a "fabless firm" before being fabricated by a "foundry" which manufactures chips [385]. While U.S.-based companies have long led the world in semiconductor device design, over the past 30 years, the United States has ceased to be the leader in semiconductor manufacturing; as of 2021, approximately 75 percent of the world's semiconductor manufacturing capacity was located in

[26] For example, the Caffe library is still available on GitHub but it was last released in 2017.

East Asia [386]. The world's microelectronics supply chain could be disrupted by geopolitical strife or natural hazards such as seismic activity in these regions, or from shipping disruptions.

The overall success of the semiconductor industry has been grounded in the approximate doubling every 18 months of the number of transistors (microchips' fundamental electronic components) that can be economically fabricated on a chip of a given size—a phenomenon referred to as Moore's law. These regular improvements have created new applications and demand for semiconductors, from which profits are reinvested to support R&D and capital equipment required to sustain further improvements and new products in a virtuous cycle. However, in recent years, the pace of improvements has slowed while costs of improvements have increased [387].

Today, leading-edge logic microprocessors involve chip features of less than 10 or even 5 nanometers in size; the only photolithography tool capable of fabricating devices at this leading edge is made by the Dutch company ASML. ASML's extreme ultraviolet lithography (EUV) machines are so expensive—on the order of several hundred million dollars for each of the 9 to 18 machines required in a production fab—that many semiconductor manufacturing companies have abandoned leading edge fabrication resulting in industry consolidation at the leading edge. Currently, mass production of leading edge logic nodes utilizing EUV technology is occurring only at two companies: TSMC in Taiwan, and Samsung in South Korea [388].

The Creating Helpful Incentives to Produce Semiconductors (CHIPS) Act of 2022 (passed as Section A of the CHIPS and Science Act of 2022)—appropriated funds for and expanded provisions of the CHIPS for America Act (passed as part of Fiscal Year 2021 National Defense Authorization Act). This legislation included several landmark mechanisms and more than $278 billion for strengthening U.S. domestic semiconductor manufacturing and R&D capacity, securing the U.S. semiconductor supply chain, and developing the U.S. semiconductor workforce [389].[27]

Improvements in computational capacity are being outpaced by the growth rate of requirements for developing the most resource-intensive AI models

Since around 2012, the rapid rise of practically deployable AI models—especially those driven by deep neural networks—has been enabled by rapid growth in the volume of data and capacity of computational resources with which to train these models. However, over this time, computational requirements for training a leading-edge AI model, such as GPT-3 and later versions, have risen exponentially—by one estimate, doubling every 3.4 months—while the capacity of new microprocessors is no longer expected to double every 18 to 24 months [12]. While some innovative AI models require only moderate levels of computing power, training some leading-edge models can be extremely compute-intensive, and even the dominant financial cost involved in model development.

In the 2010s, GPUs—highly parallel microprocessors originally used for processing images—were widely adopted because their parallel design increased efficiency for AI tasks (for example, model training) compared to central processing units. To enable cost-effective performance and continued improvement in AI models, specialized processors whose design has been optimized for a specific AI application (rather than relying on general-purpose microprocessor designs) are increasingly employed—including those that are optimized for the efficient training or

[27] Updated in December 2022.

implementation of specific AI algorithms. Categories of AI-specific chips include specialized field-programmable gate arrays (FPGAs, typically used for inference, that is, making predictions from real-world data), and application-specific integrated circuits (ASICs, used for training or inference) implemented as systems on a chip (SoCs). Numerous chips may be leveraged in parallel or even co-located on the same, large, silicon wafer. Today, a variety of commercial processors are available that were designed for AI applications, and the leading AI chips leverage "leading node" (ASML) fabrication technologies; combining AI-specific chip designs with leading-edge fabrication techniques has enabled increased speed with efficiency improvements. In practice, numerous AI-specific processors or "accelerators" may be used for a single job, which are managed by CPUs; these can be purchased and managed by the user or "rented" via commercial cloud service providers [390].

In general, financial costs (excluding labor costs) of AI model training and deployment depend on the cost of the hardware (which increases with processing speed) and the cost of the energy required to run the associated computations—the consumption of which also has substantial environmental consequences. While smaller-feature (leading node) devices are more expensive than larger-feature (or "trailing node") devices, over time the savings due to increased efficiency outweigh the extra capital cost [388].

The market for AI chips has been projected to grow faster than the general market for microprocessors. U.S. companies generally lead the market for AI chip design and for the tools used to design AI chips, which are leveraged by companies in other nations, and hold a competitive advantage in these areas—however, the United States does not have domestic manufacturing capacity for leading-edge AI chips [388], and the supply of AI chips is limited [390]. It has been projected that the current exponential rate of growth in computational power required to train the largest AI models will not be sustainable, as the cost to train the largest model would surpass U.S. gross domestic product (GDP) within the next few years [390]. Speed and efficiency improvements can also be achieved through improvements in algorithm, software, and network design [388], or possibly as a result of breakthroughs in new hardware or computing paradigms such as neuromorphic chips or quantum computing—though the latter remains in R&D stages of maturity [390].

The high demand for and cost of computational resources for compute-intensive AI R&D limits participation among those who lack the financial resources to compete

With the rise of deep learning, participation in the AI innovation ecosystem has shifted. A recent bibliometric and text analysis-based evaluation of AI conference papers found that the greatest increases in number of publications between 2012 and 2020 were among large technology firms and elite (top-50-ranked) universities. Evidence suggests that the increases in technology firms' conference papers were due largely to a rise in firm-only research or that conducted with elite universities. The share of accepted conference papers from non-elite (below top-50-ranked) universities decreased during this window [391]. Other researchers have similarly identified a trend of concentration of leading-edge AI R&D in a few large technology firms [392]. These gaps have been attributed to a disparity in access to the resources, namely compute and data, that are available to large firms with the income (and top-tier universities with the funding, infrastructure, and experience) necessary to obtain or gain access to them [71].

This disparity is one likely reason that the share of AI PhD-holders taking jobs in industry has increased relative to the share taking jobs in academia: higher salaries and greater access to data in industry may be more attractive than academic opportunities in general. It has also been associated with challenges faced by university departments in hiring leading AI researchers to faculty positions. These disparities in access could pose a risk to the U.S. AI innovation ecosystem by putting small businesses and academic institutions at a disadvantage for both AI R&D and commercialization [391; 393]. They could also make it more difficult to nurture AI talent at a diverse range of institutions, presenting further challenges to broadening and diversifying the U.S. AI workforce. The National Artificial Intelligence Research Resource Task Force's January 2023 roadmap outlines a plan for building research cyberinfrastructure that provides U.S. researchers with access to compute, data, testing, and training resources with an explicit goal of democratizing access to AI R&D resources [394].

High quality data required for AI research and development are not equally available to all

Development of AI models requires access to data of high quality, volume, variety, and accuracy—which often require substantial labor-intensive cleaning and curation prior to use—and a talented workforce equipped to use them. Furthermore, data about individuals raise individual and collective privacy risks. Use of such data requires technical, policy, and practical controls for protecting privacy, civil rights, and civil liberties associated with data access and use, and with the use of models developed using these data across all aspects of the AI pipeline.

However, similar to computational resources, not all companies or research institutions have ready access to data sets that can be used to develop high-performing and trustworthy AI models or the capacity to manage privacy risks. Large companies whose business models generate or readily enable the collection of such data have an inherent advantage, in that their business data (e.g., on transactions or customers) can be used for AI model development. Similarly, high-profit companies may be able to afford the purchase, collection, and curation of data that can be used to train AI models. The increased reliance on ML for various business processes could mean that data-rich firms could raise the barrier to competition for less resourced firms—or potentially even yield "monopoly profits" or "data monopolies" [12]. In particular, a few companies currently control orders of magnitude more data than any other entity. This imbalance poses risks to market balance, R&D competitiveness of different types of companies and institutions, and potential concentration of talent in a small number of private sector entities as a result of seeking out leading-edge data resources [395].

1.4.1.2. Marketplace Risks

It has been estimated that AI will contribute $15.7 trillion to the global GDP by 2030 due to productivity gains from process automation and business process augmentation, and from increased consumer demand for AI-enabled products and services [267]. As indicated in Sec. 1.3 of this chapter, AI technologies have current and potential future applications across all industrial sectors. AI methods can be used to optimize processes; automate, augment, or assist otherwise human-conducted tasks; and extract new insights from data—and for predictive analytics and decision making. According to recent surveys, leading business functions that leverage AI include marketing and sales activities, security, finance, human resources and law [396], service operations such as customer care, and product service development [13]. The industry sectors within which companies were most likely to adopt AI technologies according to a 2020 survey include high-tech and telecommunications, financial services, and automotive and assembly [13].

U.S. companies have a strong position in the global AI market, but the field is highly competitive. As of 2021, the United States had the largest number of granted AI patents at 39.59 percent of the world's total, though China has had the largest share of new patent filings since 2016. The level of U.S. private sector investment in AI R&D in 2021 was estimated at $52.87 billion, compared to China's $17.21 billion and the EU's $6.42 billion [14]. In 2021, China had the largest share of peer-reviewed journal publications in AI (at 31.0 percent) followed by the EU and the United Kingdom combined (19.1 percent) and the United States (13.7 percent). Among international collaborators on AI R&D, the United States and China have the most co-publications [14].

Factors that affect the AI market include the availability and distribution of resources to support market competition (described in the preceding section), the performance and trustworthiness of deployed AI systems, public and consumer attitudes about AI, and legal and regulatory requirements. Key risks to the AI marketplace are described in the following.

Deployed AI systems may not always prove trustworthy in practice

While many forms of AI are actively deployed in industry, many AI methods face practical deployment challenges related to privacy, efficacy, reliability, safety, security, resilience, and fairness—features included in the general concept of AI trustworthiness. As noted in Sec. 1.2, AI models remain both narrow and brittle; even if a given model performs well in specific contexts, namely those for which it was specifically designed or in which it was trained, they may function other than as intended when deployed in new or real-world contexts. In addition, AI models are subject to the biases of their creators or, in the case of ML models, the data used to train them. These weaknesses present significant risks of "accident" associated with AI deployment: the potential for a model to fail at its intended task due to a lack of robustness; for the model to work "correctly" according to the system's specifications but with unintended consequences (such as perpetuation of bias, inequality, or other adverse societal conditions reflected in the model or the data used to train it); and an inability to properly monitor the system during deployment. Such failures of robustness, specification, and assurance could have adverse safety, fairness, security, privacy, confidentiality, or other societal impacts. The harms associated with such failures could be especially dire if the AI is deployed for critical functions, or if the AI elements are relied upon exclusively. Such outcomes could also reduce consumer confidence and create negative public perceptions of AI, and potentially disrupt the market for AI technologies.

Approaches to addressing these risks aim to build justified trust in AI systems by (1) developing testing, evaluation, verification, and validation methods to support rigorous model development and deployment; (2) improving AI accuracy through R&D to advance the state of the art and understanding of failure modes, along with methods for auditing and explaining such failures, preventing them, reducing their occurrence, and mitigating associated harms; and (3) establishing benchmarks and standards to provide common points of reference with which to measure different aspects of AI trustworthiness, or other technical or policy guardrails. Many of the international standards development activities, partnerships, and U.S. agency coordination, guidance, and R&D activities are working to address these risks. Efforts include developing clear definitions of different types of AI systems, developing principles and standards for trustworthy AI, and advancing R&D to improve understanding and mitigations of these risks in AI technology development and among the workforce. NIST's work in collaboration with the AI community to develop an *AI Risk Management Framework* is a start at addressing these risks. OSTP's *Blueprint for an AI Bill of Rights* establishes a set of principles for protecting the public's privacy, civil rights, and civil liberties that can inform risk management of AI across its full life cycle.

Potential public distrust in AI technologies could be a barrier to adoption

Whether or not an AI system is robust and reliable at its intended task, public perception of these technologies and the entities that deploy them will influence the ways in which they are adopted and the evolution of associated oversight regimes. Individuals may be concerned not only with the value that AI provides to the economy or the goods and services that AI can improve or make available to them, but about the implications of AI for individual privacy, autonomy, equity, civil rights, and civil liberties, as well as the intentions of those that control and profit from AI. AI can cause real harms, and any early failures to protect societal interests, democratic values, individual rights, or public safety could lead to lasting damage in the public eye, even if these failures are subsequently mitigated.

Variation in legal or regulatory regimes for data protection and use of algorithms for automated decision making create complicated compliance regimes and uncertainty for the private sector

As development and adoption of AI technologies advance, their deployment across industries and sectors enters new legal terrains where application of existing laws and regulations may not always be clear; legal protections and guidelines generally lag technological progress. As a result, companies may face uncertain current compliance regimes and legal precedents and ambiguity about their potential liability in the event of harm caused by an AI model used in their business (for example, the reconstruction/leaking of sensitive data from a deployed model, or inadvertent discrimination against a protected group in an offered service due to lack of transparency or understanding of biases present in training data).

In addition, legal requirements associated with aspects of AI deployment may vary by jurisdiction—from State to State domestically (consider the California Consumer Privacy Act (CCPA), and that the District of Columbia has recently introduced an initiative to ban algorithmic discrimination) or across non-U.S. market regions. Today, the collection and use of data on individuals or organizations in the United States by the government and the private sector are governed by wide a range of different laws, regulations, and other policies, depending on the nature of the data and the use case. Examples include the Privacy Act of 1974, the Health Insurance Portability and Accessibility Act (HIPAA), the Americans with Disabilities Act (ADA), the Rehabilitation Act, the Civil Rights Acts of 1964 and 1968, and State laws on Security Breach Notification—to name a few.

The EU General Data Protection Regulation (GDPR) was adopted in 2016 to enhance the control of individuals in the European Economic Area and the EU over their personal data. This law applies to U.S. businesses that hold data of EU persons, regardless of where the data are held. In recent years, several States have established similar laws, beginning with the California Consumer Privacy Act (CCPA), the Colorado Privacy Act of 2021, and the Virginia Consumer Data Protection Act of 2021. These State laws offer similar protections to those of the GDPR. Also of note, Illinois's Biometric Information Privacy Act sets requirements for collection, use, notification, and sale or purchase of biometric data, and limits the ability of companies to profit from such information [397].

These trends both indicate a landscape in flux and could signal a pending shift in the paradigm for data regulation. For companies operating within multiple regulatory regimes, this flux could pose compliance challenges, as could a lack of appropriate guidance or uncertainty about interpretation or application of existing laws and regulations to uses of data for AI. This uncertainty, along with uncertainty about liability for harms, could present barriers to adoption or deployment of AI in industry. [398]

Widespread AI adoption may present challenges for current antitrust enforcement; it may be possible to adapt existing law to meet those challenges

Widespread implementation of AI by companies may give rise to market dynamics that complicate antitrust analysis and enforcement. In particular, AI-driven demand for data may exacerbate antitrust issues in some markets that rely on the collection and analysis of large amounts of data. These markets are often multi-sided and provide some free services, complicating efforts to apply standard antitrust analysis, which focuses on assessment of consumer welfare measured through price or other terms and conditions that adversely affect customers [399]. Multi-sided markets provide two or more sets of services to different groups of customers. For example, ad-supported publications provide news to readers and advertising to businesses. While precedent exists, antitrust doctrine governing multi-sided markets is less established than that of single-sided markets, particularly in cases where one of the services offered is free [399]. The proliferation of this model, typified by social media companies that collect data from free users to sell targeted advertisements, has led to debate over the best way to understand and regulate non-price areas of competition, such as data privacy [400]. As AI continues to be more widely adopted, the presence of network effects in many of these sectors may further concentrate or extend the market power of firms that have access to or control large amounts of data or computational resources.

European and international organizations have also asked whether current antitrust law is equipped to handle novel forms of tacit or explicit collusion facilitated by AI—especially for ML. A recent study contemplated three scenarios of potential concern [401]. In the first, firms implement AI systems built to facilitate explicit agreements to collude, for example, by automatically setting prices at a certain level. Antitrust violations of this kind can be dealt with using traditional antitrust tools [402] and have been prosecuted under American law [403]. In the second scenario, a third party provides many firms with similar or identical AI systems, such as a pricing algorithm. These systems could appear to act in a coordinated fashion because they respond similarly to external stimuli. Depending on the circumstances, American antitrust law might prohibit this coordination as a hub-and-spoke conspiracy in which the third party intermediated an illegal agreement among the firms [404; 405]. In a third scenario, the interaction of many different AI pricing systems could give rise to emergent strategies that resemble tacit or explicit coordination. It has been suggested that EU antitrust law is likely flexible enough to accommodate the current effects of AI, but may need to be updated as systems advance [399; 401], and that legislative changes may be necessary to account for new forms of tacit collusion made possible by AI [402]. The same is likely true for American law, which currently may have to address such advanced forms of AI collusion through civil remedies focused on the net anticompetitive effect of the use of such AI or merger control that prevents the market concentration necessary for the collusion to be successful.

Use of AI to automate trading may lead to increased volatility and instability in markets

Algorithmic trading has been increasingly used in financial and currency markets [406] and it is not unreasonable to expect other markets to become more automated. The speed at which automated algorithms can pursue trades forces markets to fluctuate faster and increases their volatility. In addition, it is unknown if the different AI driving these trades will counteract or align with one another, and whether the end result will be stability or instability. Since the AI systems are effectively black boxes, there is additional systematic risk for which it is difficult to account [407].

AI-induced market instability is a concrete example of the general concern that reliance on AI may risk diminished economic or societal resilience [392]. If AI systems operating in markets were as well understood as human traders, there would be less risk.

1.4.2. Risks to the American Public's Privacy, Civil Rights, and Civil Liberties

While AI presents great potential for economic and societal benefit, research, design, development, deployment, and governance of AI technologies also pose risks to privacy, safety, confidentiality, fairness, civil rights, and civil liberties—with the nature of potential harms dependent on context and use. For example, AI systems used to inform healthcare decisions could lead to adverse health outcomes if they do not work as intended, or to inequitable health outcomes if they do not work well for everyone. AI algorithms used to make decisions about home loans or hiring could unfairly discriminate against individuals on the basis of race, color, gender, religion, disability status, age, or other protected classes if the model is biased or used in a biased manner. Data used to power AI could be collected about individuals without their knowledge and enable surveillance of individual digital or real-world activities or otherwise compromise their privacy. AI can be used to profile and target individuals (as in advertising) or predict future behavior to inform decision making (as with predicting recidivism rates in parole decisions), potentially without their knowledge or consent or in violation of their civil rights or civil liberties. Finally, increasing reliance on automated systems presents a risk that individuals have no choice but to use AI-based systems for critical services without alternatives, or could lack recourse in the event of adverse impacts. Numerous studies have explored bias in AI and identified past or potential harms associated with the development and use of AI systems (see, for example, [408; 409; 380; 410; 411; 392; 412–414]).

While Federal agencies have begun to clarify how some existing laws and regulations apply to AI systems and uses (see Table 22 and Table 23), it is likely that not all of these risks are appropriately addressed through current regulatory frameworks, and additional guardrails could be needed. In October 2022, OSTP released a *Blueprint for an AI Bill of Rights*, which provided nonbinding principles and practices that can be applied in the event of gaps in current policies for the design, use, and deployment of automated systems that have the potential to meaningfully affect civil rights, civil liberties, privacy, and equal opportunities and access to critical resources or services. Namely, it identifies five core protections to which everyone in America should be entitled: (1) Safe and effective automated systems, (2) Protection against algorithmic discrimination, (3) Data privacy, (4) Notice and explanation, and (5) Human alternatives, consideration, and fallback [294].[28]

[28] Updated December 2022.

Many of the risks to privacy, civil rights, and civil liberties are associated with data collection and use. The financial value of AI incentivizes the collection, aggregation, and repurposing of data to power it—including data about individuals. Such data may be collected from public records or in the course of day-to-day activities, such as routine transactions and social activity, mediated by the integration of digital technologies into nearly every aspect of daily life. The widespread collection of data on individuals, and its use in AI models, poses ethical and legal concerns. For example, individuals may be unaware of the extent of data collection, the range of possible uses of data or the potential for data to be used for purposes other than the original purpose of collection, or how the data will ultimately be used; even when notice-and-consent banners are used, the information provided may be too lengthy and complicated—or else too oversimplified—for informed decisions to be made. In some cases, the use of particular digital services may be so integral to daily life that the choice to opt out of using them in order to avoid associated data collection may not be a practical option.

Even seemingly harmless data can yield sensitive information about individuals or groups when aggregated with data from other sources. In general, data-intensive technologies require both technical and policy controls to protect against breach of privacy or confidentiality and other harms. In the case of AI, models trained on potentially sensitive information can in some cases be reverse-engineered or caused to "leak" aspects of the data on which they were trained. Furthermore, AI systems trained using sensitive data could become capable of inferring sensitive information from non-sensitive data, facilitating the identification, profiling, or targeting of individuals based on protected features or in an otherwise discriminatory or even predatory manner [415; 416]. The potential for harm associated with the use of data for AI and deployment of AI across a variety of use cases could also present financial, liability, and reputational risks to entities developing or commercially deploying it [380], and could also have market ramifications for companies or for the industry writ large.

There are several ways in which data can result in model bias and associated harms. First, the data themselves may be biased, for example by being non-representative of an actual population, potentially due to data availability and accessibility issues. For example, a face recognition model—or some other model that considers physical attributes such as hair texture—trained on a collection of images that includes only light-skinned people may not perform well for images of individuals with darker skin. Even if a data set is demographically representative, it could be "sparse"—that is, there could be too few examples of minority groups, or of a characteristic of interest within a minority group, for the model to be properly trained. Second, even if a data set is accurate and representative, it may reflect historical societal biases, including discrimination and inequities, and could project them into current decision making. Third, the knowledge, experience, and views of the individuals that curate and label data used to develop AI (as well as those that develop the AI models themselves) can influence their work and the way in which data shape an AI model. The associated risks are perhaps most acute in the case of supervised machine learning, which requires human-labeled data as inputs; inaccurate labels, or those that reflect prejudice, will affect model performance.

All of these potential vectors for bias present risks to the trustworthiness of AI systems.[29] Failure to recognize and mitigate this bias poses the potential for AI-based products to propagate societal

[29] "Trustworthy" AI is defined as AI that reflects "characteristics such as accuracy, explainability and interpretability, privacy, reliability, robustness, safety, and security or resilience to attacks," mitigates bias, and appropriately considers fairness and transparency National Artificial Intelligence Initiative, "Advancing Trustworthy AI," NAII, accessed May 9, 2022, https://www.ai.gov/strategic-pillars/advancing-trustworthy-ai/.

harms, including potential violations of privacy, civil rights, or civil liberties. These risks underscore that AI is inherently sociotechnical, and that expertise in a range of disciplines is necessary for developing trustworthy AI. NIST is currently in the process of developing formal guidance for assessing and managing risks of bias in AI. The March 2022 NIST publication, *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence*, describes categories of bias, what is at stake, and approaches to mitigating bias in AI. It also provides preliminary guidance for addressing these challenges as they relate to datasets, model testing and evaluation, and human factors [354].[30]

NIST's *Privacy Framework* and associated resources provide voluntary guidance for identifying and managing privacy risks in the development of products and services [359]. In March 2022, NIST released an initial draft *AI Risk Management Framework* describing technical and sociotechnical AI risks, and key functions necessary for identifying and managing these risks for multiple AI stakeholders. In January 2023, NIST released the final version of the NIST *AI Risk Management Framework*, along with an *AI RMF Playbook*, *RMF Explainer Video*, *AI RMF Roadmap*, and an *AI RMF Crosswalk* [418; 419; 372]. DOE has released an online AI Risk Management Playbook to support responsible and trustworthy AI use and development, including methodologies incorporating ethical and equity governance and suggested practices for AI [348].

AI systems can be opaque—that is, they may lack transparency about how they were developed and how exactly they work. Outputs of AI systems, DL systems in particular, are also often not easily explainable. This poses complications for justified trust in AI systems and can make oversight challenging. Reliance on AI systems—especially for critical resources or services—can conflict with principles of individual agency and cause harms when proper validation, monitoring, oversight, or alternatives are lacking. AI models are also vulnerable to discordant or malicious inputs and other manipulation—either intentional or inadvertent—whose outputs could lead to harms. Additional relevant Federal government policies and resources for ethical and trustworthy AI can be found in Table 19–Table 26.

1.4.3. Risks to the National Security, Including Economic Security, of the United States

Due to its broad utility across a variety of applications, AI has direct implications for U.S. national security, including economic security. AI can enable increases in productivity across industrial sectors and lead to new products, processes, and services. AI can also be employed in critical infrastructure or in support of national security and defense, with the potential to alter the cost-benefit ratio for cyber and kinetic conflict and to increase the volume of information and the speed with which security decisions are made. In addition, the use of AI by foreign governments or third parties, and potential for such entities to influence or exploit any aspect of the AI innovation ecosystem, poses additional national security, including economic security, risks. Key examples of these risks are highlighted in the following.

AI-specific security vulnerabilities can be exploited by adversaries

[30] "Trustworthy" AI is defined as AI that reflects "characteristics such as accuracy, explainability and interpretability, privacy, reliability, robustness, safety, and security or resilience to attacks," mitigates bias, and appropriately considers fairness and transparency National Artificial Intelligence Initiative, "Advancing Trustworthy AI".

AI, especially ML, is susceptible to several well-known exploits that risk making AI not useful or not trustable. As AI becomes increasingly integral to the economy, these risks and the threat of these risks also become more important to the national security of the United States. If a nuclear power plant or the electric grid depends on AI for monitoring and adjusting the system, then incorrect inferences can have catastrophic effects. These effects will occur at speeds that are beyond human ability to detect and correct in real time. Even systems such as food distribution and package delivery are becoming dependent on AI [420].

If the adversary understands an AI system well enough, it is possible for them to construct noise-like data that can be added to the operational data to push the AI into making incorrect inferences [421]. This noise can be at a low enough level to be undetectable by humans, but sufficient to convince the AI to make high-confidence classifications that are incorrect. Similarly, researchers have been able to add visual content to a real-world scene (in the form of a sticker designed to trick an ML algorithm) to force high-confidence, incorrect classification by an ML system [422]. As with other cybersecurity risks, attribution of such attacks may be challenging. In addition, AI introduces complexity into systems that can sometimes make it difficult to diagnose and mitigate attacks and failures.

If the adversary has or obtains access to a system's training data, it would be theoretically possible for the adversary to alter them in such a way that models trained using them are effectively useless. Other so-called "data poisoning" attacks can have more subtle effects—such as only yielding incorrect outputs in specific contexts—that are harder to recognize and can be inflicted on a pre-trained system by a sufficiently knowledgeable adversary with sufficient access to the model and training data.

As such, it is necessary for all entities developing and deploying sensitive AI systems to protect their AI model and training data from exfiltration and exploitation—though a balance may be needed here, as open access to data and code allows market-enabling reuse and auditing of resources. When U.S.-based companies have leading-edge AI systems, there is an additional risk that a potential adversary could steal IP for the purpose of their own use. This could dilute or eliminate any competitive advantage that the United States has in AI.

Limited availability of secure, cutting-edge, or mission-critical AI tools can constrain national security, including economic security

AI is becoming increasingly critical to the national security, including economic security, of the United States. Countries such as China and Russia have publicly declared that AI is a national strategic technology and have made large investments in AI and AI research [423; 424]. The increasing international competition in AI leads to several risks to the United States:

- Non-U.S. entities may be unwilling to share cutting edge AI or AI tools, putting United States entities at a technological disadvantage;
- Foreign governments may ration critical hardware, for which the U.S. has limited manufacturing capacity, to prioritize their own needs or strategically to keep the United States disadvantaged; and
- Foreign governments or third parties could build "back doors" or other vulnerabilities into AI systems at any point of the value chain to leverage subsequently for cyber exploitation of the entities that deploy them; such risks could limit the AI tools that are appropriate for sensitive applications.

Several recent Federal policies have implications for computer hardware important for AI. CHIPS Act provisions aim to enhance U.S. access to and manufacturing capacity for advanced semiconductor technologies [389]. In October 2022, the Department of Commerce's Bureau of Industry and Security announced new rules for export controls on advanced computing and semiconductor manufacturing items designed to restrict the ability of the People's Republic of China to purchase or manufacture certain high-end microprocessors of use in military applications, including AI-enabled applications [425; 426; 327].[31]

In addition to international competition around AI tools and components, domestic providers of AI systems may not be willing to make their cutting-edge data, software, and hardware available to the U.S. Government for defense purposes [427; 428]. In some cases, this has to do with trade secrets and data rights, and in others it has been due to disagreements over the morality of how the technology may be used. In addition, many companies at the leading edge of AI research are multi-national corporations that must consider the ramifications of their decisions in a global marketplace. Even if the corporation is headquartered in the United States, it may choose to act in a way that does not support U.S. national security objectives.

Reluctance or insufficient supply of AI talent to work for the U.S. Government may negatively affect national security

The lack of sufficient AI talent in the United States, described in Sec 1.4, has particular national security implications in that it is difficult for the U.S. Government to hire workers with relevant expertise. Because AI skills and knowledge can garner high salaries in the private sector, government jobs with limited salary potential may be less appealing to top AI talent [429]. Furthermore, many of the top AI researchers and graduate students are foreign citizens and not qualified to work on sensitive government projects, or to work for the U.S. Government at all. Federal agencies often need special hiring authorities to bring in needed AI talent [430]. Finally, perceived moral and ethical issues associated with some defense and national security work [431] may further reduce the AI talent pool willing to work for the government.

AI surveillance capabilities can be used to facilitate state repression of human rights and strengthen authoritarian regimes in opposition to democratic principles

As AI becomes increasingly available, advanced, and prevalent in institutions and everyday life, it is likely that some foreign governments will use AI to push back against U.S. notions of human rights, societal norms, and democratic principles in their country and across the world. The prevailing international AI standards and practices will have a strong influence on what AI systems and AI uses will be considered acceptable across the world, with potential implications for human rights, societal norms, and democratic principles around the world.

There has been much reporting on biases that can exist in AI systems in a variety of disciplines [432; 433; 392] and how these can lead to discrimination. Potential solutions include further clarifying how existing laws prohibit such discrimination, establishing non-discrimination laws for AI systems [434; 432; 433; 392], or banning certain uses of AI through national law or international treaty.

As an example, there have been public reports of foreign governments using AI for widespread surveillance of their population. Also, there have been public reports of AI being used to detect ethnic minorities so that they can be discriminated against. Whether such uses of AI fit into the

[31] Updated December 2022.

prevailing international standards and practices will have great human rights implications—a major security interest for the United States.

This example should be sharply contrasted from other widely reported cases [435] where AI systems *mis*identified people in a discriminatory way due to biases in the training data. These failures are unintended consequences and could be remedied by better testing, evaluation, verification, and validation. Diversification of the AI talent pool may also help avoid or at least detect these types of issues early in the process or AI development.

AI-driven technologies can be used to promote misinformation and advance disinformation campaigns

Propaganda campaigns using mis-, dis- and mal-information (errors, lies and innuendo) are long established techniques dating back at least to World War II [436]. Digital and AI-driven technologies have made these campaigns easier, quicker, and less costly to implement, have more extensive coverage and give propagators the ability to quickly pivot to align with current thinking[32] [437; 438]. If the aim of the campaign is to disrupt the economy, they do not even need to have a clear, unified message. Instead, sowing confusion and lack of trust can be enough to reduce the efficiency of the U.S. markets and economy and cause significant disruptions [439].

1.4.4. Emerging Risks and Long-Term Trends in the Marketplace and Supply Chain

AI presents additional economic and societal risks beyond those described in the National Security context in section 1.4.3 that continue to evolve over time. The AI innovation ecosystem is developing rapidly, with new advances, societal implications, and policy[33] questions emerging at a rapid cadence—and the boundaries of what is considered "AI" may change over time. In addition to the issues raised in previous sections, this section describes other emerging risks and long-term trends.

Safety, security, and societal risks of AI will expand as AI becomes more complex and is increasingly adopted for critical functions

It is expected that AI will continue to present important opportunities to address challenges whose solutions yield substantial economic and societal benefit. It is unclear whether or on what timeline artificial general intelligence might be achieved, but would bring with it additional ethics, safety, and governance concerns, including potential for misalignment with human priorities or values. While the long-term future of AI cannot be predicted, the current technology landscape and the history of AI and information technology writ large can help to inform an understanding of emerging risks and long-term trends. Increasing reliance on AI over time without redundancy or a non-AI alternative, the increasing complexity of AI systems, and the acceleration of the pace and adoption of AI-supported decision making could all increase the stakes of an AI system failure or exploit, including with real harms for human health, safety, privacy, civil rights, and civil liberties.

[32] In military terms, a "force multiplier."

[33] Intellectual property-related issues are also important and evolving, and are thus not addressed in detail in this report. See section 1.3.1.2 for a description of recent USPTO activities related to AI and IP and the discussion of generative AI in this section for additional context.

Focusing on near-term benefits of AI without planning for longer-term needs could limit future benefits or lead to widespread harm

Recent applications of AI have led to great enthusiasm for the potential of AI and ML to solve pressing real-world problems, improve business processes, provide desirable consumer products and services, and yield economic benefits. However, a rush to adopt AI to realize enhanced profits and other benefits rather than deliberate planning for longer-term adoption could result in otherwise foreseeable societal harms—for example, if there is a failure to plan for system resilience to protect against catastrophic failures or misalignment with societal priorities, or if insufficient attention is given to protecting the public's safety, security, privacy, civil rights, or civil liberties. Such harms could also cause backlash that might have market ramifications, or potentially indicate that AI market norms conflict with democratic principles.

Similarly, a failure of current technologies to live up to near-term expectations could reduce support for deployment of AI systems. This could result in a decrease in research or venture capital funding for AI technologies—as has happened in the past in the so-called "AI winters" that occurred in the 1970s and around the turn of the millennium [4]. Long-term benefits for any technology are generally underpinned by near-term R&D. Enthusiasm for near-term benefits of AI and currently dominant areas, such as large, DL models, could draw focus from other areas of AI that are less mature or prominent, but that could lead to important benefits in the longer term [440].

New models and implementations for computation are being pursued to sustain advances in AI

Because current computer hardware implementations are approaching scaling limits, new approaches to computing are being pursued to enable further advances in computational capacity and capabilities and to address the energy efficiency of computing. These include new architectures, hardware implementations, and fabrication methods, as well as new models for computing—such as neuromorphic computing or quantum computing, which could potentially offer advantages for certain types of computations, though it is not yet clear how.

Adoption of AI will continue to contribute to labor market shifts, with the potential to make work more precarious, cause unemployment, or increase inequality

While AI technologies present potential economic benefits, the precise nature of their implications for the U.S. and global labor force are not fully clear, nor is their time frame for impact—and this is likely to vary across industrial sectors and occupational fields. Technological change has historically led to shifts in the nature of work, including instances of technological unemployment. While automation technologies have historically displaced routine or low-skill tasks, it is becoming increasingly feasible for AI to automate nonroutine, cognitive tasks [441]. Concurrently with the surge in AI development and deployment in recent years, concerns have risen about the potential for AI to lead to widespread technological unemployment, exacerbate inequality, or result in privacy, civil rights or civil liberties violations—for example, as a result of worker or workplace surveillance.

It is generally expected that AI will further affect the labor market in at least three ways that can have positive or negative ramifications:

1. AI will automate some work tasks currently conducted by humans, reducing the need for labor or shifting the nature of tasks conducted by workers in certain occupational fields;

2. AI will be used to augment human functions or assist or monitor human workers in carrying out work tasks to enhance performance, productivity, or worker safety or accessibility; and
3. Deployment of AI technologies will lead to new products, services, or industries, creating new types of jobs with different skills requirements, benefits, and rights—for example, demand for AI developers or data curators.

A key example of AI-driven shifts in the labor market is the growth in AI development jobs in the private sector. There have also been rises in “gig” work—service activities scheduled or otherwise facilitated by AI systems—and “ghost work”—the labor-intensive human-conducted tasks necessary to develop and sustain AI systems, such as data labeling or sorting or content moderation. This work often offers the ability to work on-demand or remotely (for digital tasks), but is often overlooked or invisible, low-wage, and menial [442]. Recent advances in cutting-edge natural language and image generation models suggest that some AI systems could rival humans in text-based and visual content generation. These capabilities could have significant implications for the nature or availability of work in associated occupational fields [443].

While the nature of work is continuously shifting, abrupt changes can have substantial societal impacts in the absence of mitigating policies. In December, 2022, the U.S.-EU Trade and Technology Council released a study on The Impact of Artificial Intelligence on the Future of Workforces in the European Union and The United States of America [444]. The study provides an overview of AI and its current state of adoption, highlights themes related to impact of AI on work, including intellectual work, and provides case studies on the use of AI in human resources and hiring and in warehousing operations. In addition, as required by the National AI Initiative Act of 2020, NSF has commissioned a study from the National Academies of Sciences, Engineering, and Medicine (NASEM) on implications of AI for the workforce, to be delivered to Congress by January of 2023 in the form of an update to a 2017 NASEM report [445].

Market adoption of AI has continued to further incentivize the collection and commodification of personal data

Private sector collection of data created by anyone with a digital presence is heavily incentivized for targeted advertising and for use (or sale) to power data-intensive AI. This commodification of data has allowed private sector companies to benefit economically from information about an individual’s experience without their explicit knowledge or consent, counter to globally recognized Fair Information Practice Principles [446]. These data can be used for targeted advertising (by the private sector) or messaging (by any number of actors) to influence an individual’s subsequent actions. This ongoing and long-term trend raises issues of privacy, fairness, and individual autonomy that could harm individuals or society or damage public trust (e.g., in companies or technologies) and may persist without deliberate policy action [447] or advancing rights-preserving technologies.

The societal and geopolitical importance of AI is likely to increase

As AI tools and systems become more powerful and widely adopted, their capacity to influence individuals, society, and institutions will likely increase, with potential geopolitical ramifications. Depending on how AI governance evolves worldwide, the risk that AI could be used to undermine democratic principles could expand. In addition, leveraging AI for cybersecurity applications could lead to a security dilemma. Namely, while the use of certain

ML-based methods could advance cyber defenses, successful defenses against the vulnerabilities introduced by ML could require increased knowledge of an adversary's system, blurring boundaries between cyber offense and defense and presenting a risk of conflict escalation [448; 449].

Recent advances in generative AI point to emerging opportunities, challenges, and risks

Recent advances in generative AI have become highly visible due to availability of user interfaces for generation of natural language, image, and computer code content in response to user inputs. These models have been trained on very large amounts of data using substantial computational resources, meaning that only well-resourced companies have the capability of competing in development of foundational models for generative AI, and the details of the models themselves and how the model inputs from the public are used are generally not visible to the public. These advances and their social and policy implications are unfolding rapidly, and have already raised several key risks in the public domain.

While generative AI tools may have significant benefits, they can also be a low-cost means to create large quantities of text, images, and video that often seem very realistic and believable, with substantial potential for deliberate or inadvertent misuse. For example, realistic videos could be used to portray events that never occurred and propagate disinformation used to harm reputations, create political unrest, or challenge shared notions of reality. Reliance on a generative model's outputs in a search engine presents risk of biased[34] or inaccurate results being interpreted as correct or complete truths, and improperly informing members of the public. The potential for students to use generative AI models to generate content such as essays or computer code for their assignments instead of completing original work has been frequently highlighted. These concerns have spurred calls to provide notice when AI is used to generate content. They have also stimulated research into methods for detection of AI-generated content and approaches for verifying original content—for example, through built-in "watermarking" (cryptographic signing) of images generated by an actual camera (potentially itself enabled by AI) [450] or of images created by a generative AI model.

Generative AI outputs may exacerbate or present new risks to equity, civil rights, and equal opportunity. These systems compound already well-documented patterns of algorithmic bias and do so seemingly more authoritatively, more quickly, and while being made available for more people to use. With generative AI, these impacts could be subtler and more difficult for human cognition to detect. Generative AI engines have been manipulated to produce unusual, abusive, or offensive outputs, even when technical controls to protect against such outputs have been implemented—and, in some instances, entered regimes where they have performed in an unusual manner (e.g., producing inaccurate, offensive, or otherwise problematic outputs) in the absence of deliberate manipulation [451]. Generative AI tools also may replace workers[35] in creative jobs (for example, artists or writers) that have been considered safe from automation—and their works may have been used to train the model that replaced them, without consent and remuneration. Open questions remain about how copyright, authorship, and fair use policies will apply to content created by or used to train generative AI models [345]. The scale and speed with which content can be created—and the great reduction in the level of human effort required to yield new content—could magnify the potential for adverse impacts.[36] The Department of

[34] See section 1.4.2 for additional discussion.

[35] As discussed earlier in this section.

[36] This section was updated in June 2023.

Commerce announced in June 2023 plans for a Public Working Group on Generative AI to address opportunities and challenges associated with these technologies, including to inform guidance on how to manage risks [25].

1.5. Recommendations

Through the course of preparing this chapter, many sources—academic articles, market reviews, government-sponsored studies, blog posts, and conversations with Federal subject matter experts—revealed various challenges facing the AI industry in the United States. The pace of progress in AI R&D and deployment is rapid, and a large number of Federal efforts are underway to address evolving needs. The following recommendations for congressional, executive branch, or nationwide actions address additional opportunities to help:

- Grow the U.S. economy through the secure and responsible advancement of AI;
- Strengthen the United States' global position in the adoption of trustworthy and rights-respecting AI;
- Mitigate current and emerging risks to a competitive AI marketplace and supply chain for AI;
- Mitigate current and emerging risks to the American public's privacy, civil rights and civil liberties, and other potential harms of AI; and
- Advance societal priorities and address societal concerns associated with the expeditious adoption of AI.

Each recommendation below responds to a challenge identified in the development of this chapter. Recommendations have been intentionally kept at a high level, without specifying how they should be undertaken or by whom.

Challenge 1: AI systems present risks to privacy, civil rights, and civil liberties that can be introduced at any stage of development or the AI supply chain.

Recommendation 1: Congress should take action to establish or strengthen data privacy and protection laws that safeguard privacy, civil rights, and civil liberties; support a competitive AI innovation ecosystem; and help advance the responsible adoption of trustworthy and rights-preserving AI technologies.

Recommendation 2: The U.S. Government should invest in education and research to support the development of sociotechnical researchers and practitioners necessary to design and deploy AI systems for positive societal impact, mitigate residual risks to safety, security, civil rights and civil liberties, and support trustworthy and equitable AI ecosystems across all sectors of the economy.

Challenge 2: There is some concern about whether Federal coordination of national strategy on AI—including the foundation of the AI R&D innovation ecosystem—is sufficiently robust to meet opportunities for and mitigate risks associated with AI.

Recommendation 3: Congress should reauthorize the National AI Initiative Act of 2020 (NAIIA), 15 U.S.C. §§9401 *et seq*., regularly in order to enable the United States to meet changing needs across sectors as the landscape of AI evolves, and expand it to include emphasis on the need to protect the American public's civil rights, civil liberties, privacy, and safety.

Recommendation 4: Congress should empower the NAIIO to provide strong Federal coordination and leadership for AI activities in partnership with associated agencies across the executive branch, such as NIST in its Federal AI standards coordination role.

Challenge 3: The extent to which the AI standards, policies, or regulations emerging across the globe uphold democratic values and support the ability of U.S. companies to compete will depend upon the nature of U.S. international engagement in their development.

Recommendation 5: The U.S. Government should establish a formal public-private forum to support R&D and TEVV coordination across agencies with input from the private sector and enable U.S. leadership in trustworthy and responsible AI research, development, and standards.

Recommendation 6: The United States should lead global efforts to develop technically sound AI standards to enable continued innovation, ensure that global markets are open and fair, and promote AI development and use in a way that protects privacy, civil rights, civil liberties, and human rights. These efforts should consider gaps in and the most effective incentives for participation among U.S. companies and institutions, as well as R&D aligned to trustworthy AI standards development and principles.

Challenge 4: AI R&D and deployment is concentrated in large, well-resourced companies and institutions such that smaller organizations face difficulty competing in the marketplace and injecting new ideas into the AI innovation ecosystem.

Recommendation 7: The U.S. Government should support more equitable, secure, and privacy-enhanced access to research data sets—consistent with the original purpose of collection and while safeguarding privacy, civil rights, and civil liberties in their use—and computational resources to support AI innovation by research institutions, small- and medium-sized companies, and the general public. Examples include implementing the recommendations of the NAIRR Task Force.

Recommendation 8: Any efforts of Congress to modernize copyright, patent subject matter eligibility, or tech-transfer laws should take into consideration how such adjustments would best support the commercialization of innovative AI breakthroughs and a competitive AI innovation ecosystem while protecting the American public’s privacy, civil rights, and civil liberties.

Challenge 5: There is concern that the United States is not drawing on the full range and diversity of available talent required to sustain long-term advances and competitiveness in AI.

Recommendation 9: The United States should expand AI-related upskilling, cross-training and certification programs, and other programs designed to help individuals apply AI to expand their capabilities and productivity across all education and experience levels, for example through public-private partnerships and developing new interagency AI training programs.

Recommendation 10: The United States should expand and ensure accessibility of AI R&D and education activities across all relevant academic disciplines at Minority-Serving Institutions including but not limited to at Historically Black Colleges and Universities, Hispanic Serving Institutions, Women’s colleges, and community colleges to help ensure a diverse future AI workforce positioned to meet industry, government, academic, and societal needs.

Recommendation 11: The United States should reform immigration law to make it easier for non-U.S. citizen AI graduate students and researchers to study and remain and work in the United States in order to retain the best and most diverse talent, with appropriate safeguards for security.

Challenge 6: Insufficient or inconsistent effort or availability of resources for AI R&D, deployment, and safeguards could stifle the ability of the U.S. AI marketplace to thrive.

Recommendation 12: Fully fund the President's budget to support AI activities and programs, such as for interagency coordination; protecting the American public and consumers against potential AI-related harms; AI R&D and standards development; R&D for next-generation computer hardware; increasing availability of AI testing, evaluation, verification, and validation resources; developing and operationalizing AI models as mandated in government; and strengthening U.S.-based manufacturing of leading-edge microprocessors, including graphics processing units (GPUs), which are an essential part of the AI infrastructure. This investment would serve as a critical component to develop safeguards and guardrails to mitigate risks in the AI ecosystem more broadly. Such guardrails should be embedded in each individual major AI initiative that the U.S. Government undertakes or funds (such as a specific section in each solicitation for funding opportunities for a major AI initiative that requires that developers of AI tools test for adverse impacts and other concepts related to trustworthy and responsible AI). This will ensure that consideration of trustworthy and responsible AI is a part of the development process for all major initiatives, rather than an afterthought.

References

[1] NIST. “AI Risk Management Framework.” https://www.nist.gov/itl/ai-risk-management-framework.

[2] Organisation of Economic Co-operation and Development. “OECD AI Recommendations 2021.” Organisation of Economic Co-operation and Development (OECD), 2021. https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449.

[3] Roberts, Jacob. “Thinking Machines: The Search for Artificial Intelligence.” Accessed December 10, 2021. https://www.sciencehistory.org/distillations/thinking-machines-the-search-for-artificial-intelligence.

[4] Mitchell, Melanie. “Why AI Is Harder Than We Think.” April 26, 2021. http://arxiv.org/pdf/2104.12871v2.

[5] Schuchmann, Sebastian. “History of the First AI Winter - Towards Data Science.” Accessed December 10, 2021. https://towardsdatascience.com/history-of-the-first-ai-winter-6f8c2186f80b.

[6] World Intellectual Property Organization. *WIPO Technology Trends 2019: Artificial Intelligence*. Geneva: World Intellectual Property Organization, 2019. Accessed December 20, 2021. https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf.

[7] Russell, Stuart J., and Peter Norvig. *Artificial Intelligence: A Modern Approach*. With the assistance of Ming-wei Chang et al. 4th ed. Pearson Series in Artificial Intelligence. Hoboken: Pearson, 2021. Accessed December 4, 2021.

[8] Brown, Tom B., Benjamin Mann, Nick Ryder, Melanie Subbiah, Jared Kaplan, Prafulla Dhariwal, and Arvind Neelakantan et al. “Language Models Are Few-Shot Learners.” May 28, 2020. https://arxiv.org/pdf/2005.14165.

[9] Ribeiro, John. “AlphaGo’s Unusual Moves Prove Its AI Prowess, Experts Say.” Accessed December 10, 2021. https://www.pcworld.com/article/420054/alphagos-unusual-moves-prove-its-ai-prowess-experts-say.html.

[10] Markoff, John. “On ‘Jeopardy!’ Watson Win Is All but Trivial.” Accessed December 10, 2021. https://www.nytimes.com/2011/02/17/science/17jeopardy-watson.html.

[11] LeCun, Yann, Yoshua Bengio, and Geoffrey Hinton. “Deep Learning.” *Nature* 521, no. 7553 (2015): 436–44. https://doi.org/10.1038/nature14539. https://www.nature.com/articles/nature14539.

[12] Littman, Michael L., and et al. “Gathering Strength, Gathering Storms: The One Hundred Year Study of Artificial Intelligence (AI100) 2021 Study Panel Report.” Stanford University, Stanford, CA, 9/2021. http://ai100.stanford.edu/2021-report.

[13] Zhang, Daniel, and et al. “The AI Index 2021 Annual Report.” AI Index Steering Committee, Human-Centered AI Institution, Stanford University, March 2021. https://aiindex.stanford.edu/wp-content/uploads/2021/11/2021-AI-Index-Report_Master.pdf.

[14] Zhang, Daniel, and et al. “The AI Index 2022 Annual Report.” AI Index Steering Committee, Human-Centered AI Institution, Stanford University, March 2022. https://aiindex.stanford.edu/wp-content/uploads/2022/03/2022-AI-Index-Report_Master.pdf.

[15] Toole, Andrew A., Nicholas A. Pairolero, Alexander V. Giczy, James Q. Forman, Christyann Pulliam, Matthew Such, and Kakali Chaki et al. “Inventing AI: Tracing the Diffusion of Artificial Intelligence with U.S. Patents.” IP Data Highlights 5, U.S. Patent

and Trademark Office Office of the Chief Economist, October 2020. https://www.uspto.gov/sites/default/files/documents/OCE-DH-AI.pdf.

[16] Hodge, Graeme A., and Carsten Greve. "Public-Private Partnerships: An International Performance Review." *Public Administration Review* 67, no. 3 (2007): 545–58. https://doi.org/10.1111/j.1540-6210.2007.00736.x.

[17] Select Committee on Artificial Intelligence of the National Science & Technology Council. "The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update." June 2019. https://www.nitrd.gov/pubs/National-AI-RD-Strategy-2019.pdf.

[18] "Director's Blog: The Latest from USPTO Leadership." Accessed December 19, 2022. https://www.uspto.gov/blog/director/entry/incentivizing-and-protecting-innovation-in.

[19] U.S. Patent and Trademark Office. "Artificial Intelligence." Accessed December 19, 2022. https://www.uspto.gov/initiatives/artificial-intelligence.

[20] United States Patent and Trademark Office. "AI and Emerging Technology Partnership Engagement and Events." Accessed August 10, 2022. https://www.uspto.gov/initiatives/artificial-intelligence/ai-and-emerging-technology-partnership-engagement-and-events.

[21] U.S. Patent and Trademark Office. "Public Views on Artificial Intelligence and Intellectual Property Policy." U.S. Patent and Trademark Office (USPTO), October 2020. https://www.uspto.gov/sites/default/files/documents/USPTO_AI-Report_2020-10-07.pdf.

[22] U.S. Patent and Trademark Office. "Patent Eligible Subject Matter: Public View on the Current Jurisprudence in the United States." 2022. https://www.uspto.gov/sites/default/files/documents/USPTO-SubjectMatterEligibility-PublicViews.pdf.

[23] The White House. "FACT SHEET: Biden-Harris Administration Takes New Steps to Advance Responsible Artificial Intelligence Research, Development, and Deployment." *The White House*, May 23, 2023. Accessed June 27, 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/23/fact-sheet-biden-harris-administration-takes-new-steps-to-advance-responsible-artificial-intelligence-research-development-and-deployment/.

[24] The White House. "FACT SHEET: Biden-Harris Administration Announces New Actions to Promote Responsible AI Innovation That Protects Americans' Rights and Safety." *The White House*, May 4, 2023. Accessed May 19, 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/04/fact-sheet-biden-harris-administration-announces-new-actions-to-promote-responsible-ai-innovation-that-protects-americans-rights-and-safety/.

[25] U.S. Department of Commerce. "Biden-Harris Administration Announces New NIST Public Working Group on AI." Accessed July 5, 2023. https://www.commerce.gov/news/press-releases/2023/06/biden-harris-administration-announces-new-nist-public-working-group-ai.

[26] National Science Foundation. "Award # 2229885 - Institute for Trustworthy AI in Law and Society (TRAILS)." Accessed May 18, 2023. https://www.nsf.gov/awardsearch/showAward?AWD_ID=2229885&HistoricalAwards=false.

[27] National Science Foundation. “Award # 2229876 - AI Institute for Agent-Based Cyber Threat Intelligence and Operation.” Accessed May 19, 2023. https://www.nsf.gov/awardsearch/showAward?AWD_ID=2229876&HistoricalAwards=false.

[28] UC Santa Barbara. “Announcing the NSF AI Institute for Agent-Based Cyber Threat Intelligence and OperatioN (ACTION) | the ACTION Institute.” Accessed May 19, 2023. https://action.ucsb.edu/news/announcing-nsf-ai-institute-agent-based-cyber-threat-intelligence-and-operation-action.

[29] United States Department of Agriculture. “AI-CLIMATE (AI Institute for Climate-Land Interactions, Mitigation, Adaptation, Tradeoffs and Economy) - UNIVERSITY of MINNESOTA.” Accessed May 19, 2023. https://portal.nifa.usda.gov/web/crisprojectpages/1030594-ai-climate-ai-institute-for-climate-land-interactions-mitigation-adaptation-tradeoffs-and-economy.html.

[30] University of Minnesota. “U of M to Lead New AI Institute Focusing on Climate-Smart Agriculture and Forestry.” *University of Minnesota*, May 4, 2023. Accessed May 19, 2023. https://twin-cities.umn.edu/news-events/u-m-lead-new-ai-institute-focusing-climate-smart-agriculture-and-forestry.

[31] National Science Foundation. “Award # 2229929 - AI Institute for Artificial and Natural Intelligence.” Accessed May 19, 2023. https://www.nsf.gov/awardsearch/showAward?AWD_ID=2229929&HistoricalAwards=false.

[32] National Science Foundation. “NSF Award Search: Award # 2229881 - AI Institute for Societal Decision Making (AI-SDM).” Accessed May 19, 2023. https://www.nsf.gov/awardsearch/showAward?AWD_ID=2229881&HistoricalAwards=false.

[33] Carnegie Mellon University. “Carnegie Mellon Leads NSF AI Institute for Societal Decision Making.” Accessed May 19, 2023. https://www.cmu.edu/news/stories/archives/2023/may/carnegie-mellon-leads-nsf-ai-institute-for-societal-decision-making.

[34] National Science Foundation. “Award # 2229612 - AI Institute for Inclusive Intelligent Technologies for Education (INVITE).” Accessed May 19, 2023. https://www.nsf.gov/awardsearch/showAward?AWD_ID=2229612&HistoricalAwards=false.

[35] INVITE Institute. “About - INVITE Institute.” Accessed May 19, 2023. https://invite.illinois.edu/about/.

[36] National Science Foundation. “Award # 2229873 - AI Institute for Transforming Education for Children with Speech and Language Processing Challenges.” Accessed May 19, 2023. https://www.nsf.gov/awardsearch/showAward?AWD_ID=2229873&HistoricalAwards=false.

[37] University at Buffalo. “NSF AI Institute for Transforming Education for Children with Speech and Language Processing Challenges.” Accessed May 19, 2023. https://www.buffalo.edu/ai4exceptionaled.html.

[38] National Science Foundation. “NSF Award Search.” Accessed December 17, 2021. https://www.nsf.gov/awardsearch/advancedSearchResult?ProgEleCode=132Y&BooleanElement=Any&BooleanRef=Any&ActiveAwards=true#results.

[39] The Ohio State University. "ICICLE: Intelligent CI with Computational Learning in the Environment: Partner Institutions." Accessed December 19, 2021. https://icicle.osu.edu/who-we-are/partner-institutions.

[40] University of California San Diego. "TILOS: Industry." Accessed December 19, 2021. https://tilos.ucsd.edu/industry-collaboration/.

[41] National AI Institute for Adult Learning and Online Education. "Who We Are." Accessed December 19, 2021. https://aialoe.org/.

[42] Duke University. "Athena: Who We Are." NSF NAI for Edge Computing Leveraging Next Generation Networks. Accessed December 19, 2021. https://athena.duke.edu/who-we-are.

[43] The Ohio State University. "NSF AI Institute for Future Edge Networks and Distributed Intelligence." Accessed December 19, 2021. https://aiedge.osu.edu/.

[44] National Science Foundation AI Institute for Engaged Learning. "The National Science Foundation AI Institute for Engaged Learning." Accessed December 19, 2021. https://www.aiengage.org/.

[45] National Science Foundation AI Institute for Collaborative Assistance and Responsive Interaction for Networked Groups. "NSF AI Institute for Collaborative Assistance and Responsive Interaction for Networked Groups (AI-CARING)." Accessed December 19, 2021. http://ai-caring.org/.

[46] AI Institute for Advances in Optimization. "Artificial Intelligence Institute for Advances in Optimization." Accessed December 19, 2021. https://www.ai4opt.org/.

[47] National Science Foundation AI Institute in Dynamic Systems. "AI Institute in Dynamic Systems." Accessed December 19, 2021. http://dynamicsai.org/.

[48] Iowa State University. "AIIRA AI Institute for Resilient Agriculture: Institutions and Organizations." Accessed December 19, 2021. https://aiira.iastate.edu/about-us/institutions-and-organizations/.

[49] AgAID Institute. "Partners: Agricultural AI for Transforming Workforce and Decision Support." Accessed December 19, 2021. https://agaid.org/partners/.

[50] National Artificial Intelligence Initiative Office. "The Networking & Information Technology R&D Program and the National Artificial Intelligence Initiative Office Supplement to the President's FY2022 Budget." https://arxiv.org/pdf/2111.02374.pdf.

[51] AI Institute for Food Systems. "Partners." Accessed August 10, 2022. https://aifs.ucdavis.edu/.

[52] Institute for Foundations of Machine Learning. "Team Members." Accessed December 19, 2021. https://www.ifml.institute/team.

[53] University of Colorado Boulder. "NSF National AI Institute for Student-AI Teaming: Our Team." Accessed December 19, 2021. https://www.colorado.edu/research/ai-institute/who-we-are/our-team.

[54] National Science Foundation AI Institute for Research on Trustworthy AI in Weather, Climate, and Coastal Oceanography. "Partners." Accessed December 19, 2021. https://www.ai2es.org/partners/.

[55] U.S. Department of Agriculture. "USDA-NIFA and NSF Establish Nationwide Network of Artificial Intelligence Research Institutes." Accessed December 20, 2021. https://nifa.usda.gov/press-release/artificial-intelligence-research.

[56] University of Illinois. "AI Farms: Collaborating Institutions and Partners." Accessed December 19, 2021. https://aifarms.illinois.edu/about-us/collabs-partners/.

[57] Department of Veterans Affairs, Veterans Health Administration Office of Chief Research and Development Officer. “NAII AI Tech Sprints.” Accessed December 12, 2022. https://www.research.va.gov/naii/tech-sprints.cfm.

[58] National Institute of Standards and Technology. “Applied AI.” Accessed March 30, 2022. https://www.nist.gov/applied-ai.

[59] U.S. Department of Energy. “Department of Energy Announces the First Five Consortium: Artificial Intelligence Tools to Help First Responders Save Lives, Property.” Accessed December 19, 2021. https://www.energy.gov/articles/department-energy-announces-first-five-consortium.

[60] Global Partnership on Artificial Intelligence. “About - GPAI.” Accessed December 9, 2021. https://gpai.ai/about/.

[61] National Cybersecurity Center of Excellence. “Frequently Asked Questions.” Accessed February 1, 2022. https://csrc.nist.rip/nccoe/The-Center/FAQ/FAQ.html.

[62] National Institute of Standards and Technology. “NIST Establishes National Cybersecurity Center of Excellence: State of Maryland and Montgomery County Join Partnership.” Accessed February 1, 2022. https://www.nist.gov/news-events/news/2012/02/nist-establishes-national-cybersecurity-center-excellence.

[63] Allen Institute for AI. “COVID-19 Open Research Dataset Challenge (CORD-19): An AI Challenge with AI2, CZI, MSR, Georgetown, NIH & the White House.” Accessed December 28, 2022. https://www.kaggle.com/datasets/allen-institute-for-ai/CORD-19-research-challenge.

[64] Wang, Lucy Lu, Kyle Lo, Yoganand Chandrasekhar, Russell Reas, Jiangjiang Yang, Douglas Burdick, and Darrin Eide et al. “CORD-19: The Covid-19 Open Research Dataset.” *ArXiv*, 2020; Version 4. Accessed December 28, 2022. https://www.ncbi.nlm.nih.gov/pmc/articles/pmc7251955/.

[65] Partnership on Employment and Accessible Technology. “About the Partnership on Employment & Accessible Technology (PEAT) - Peatworks.” Accessed December 28, 2022. https://www.peatworks.org/about/.

[66] Harris, Laurie A. “Artificial Intelligence: Background, Selected Issues, and Policy Considerations.” Congressional Research Service In Focus, Congressional Research Service, May 19, 2021. https://crsreports.congress.gov/product/pdf/R/R46795.

[67] Cihon, Peter. “Standards for AI Governance: International Standards to Enable Global Coordination in AI Research & Development.” University of Oxford; Future of Humanity Institute, April 2019. https://www.fhi.ox.ac.uk/wp-content/uploads/Standards_-FHI-Technical-Report.pdf.

[68] International Organization for Standardization. “Using and Referencing IEC and ISO Standards to Support Public Policy.” International Organization for Standardization (ISO), Geneva, 2015. https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100358.pdf.

[69] International Organization for Standardization. “Members - ANSI - United States.” Accessed February 13, 2022. https://www.iso.org/member/2188.html.

[70] ISO. “ISO - Get Involved.” Accessed March 28, 2022. https://www.iso.org/get-involved.html.

[71] National Security Commission on AI. “Final Report: National Security Commission on Artificial Intelligence.” 2021. https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

[72] International Organization for Standardization. “About Us - Members.” Accessed February 13, 2022. https://www.iso.org/members.html.

[73] International Electrotechnical Commission. “Frequently Asked Questions | IEC.” Accessed December 19, 2021. https://www.iec.ch/faq.

[74] International Electrotechnical Commission, International Organization for Standardization, and International Telecommunication Union. “International Standards & Trade Agreements.” Accessed March 28, 2022. https://www.iso.org/files/live/sites/isoorg/files/standards/benefits_of_international_standards/WSC_International_Standards_%26_trade_agreements_2018.pdf.

[75] International Organization for Standardization. “ISO/IEC JTC 1/SC 42 - Artificial Intelligence.” Accessed December 4, 2021. https://www.iso.org/committee/6794475.html.

[76] International Organization for Standardization. “ISO/IEC JTC 1/SC 27.” Accessed February 8, 2022. https://www.iso.org/committee/45306.html.

[77] International Organization for Standardization. “ISO/IEC JTC 1/SC 32.” Accessed February 8, 2022. https://www.iso.org/committee/45342.html.

[78] International Organization for Standardization. “ISO/IEC JTC 1/SC 37.” Accessed February 8, 2022. https://www.iso.org/committee/313770.html.

[79] International Organization for Standardization. “ISO/IEC JTC 1/SC 38.” Accessed February 8, 2022. https://www.iso.org/committee/601355.html.

[80] Institute of Electrical and Electronics Engineers. “History of IEEE.” Accessed February 13, 2022. https://www.ieee.org//about/ieee-history.html#the-societies-converge-and-merge.

[81] Institute of Electrical and Electronics Engineers. “IEEE at a Glance.” Accessed February 13, 2022. https://www.ieee.org/about/at-a-glance.html.

[82] Institute of Electrical and Electronics Engineers Standards Association. “Welcome to IEEE P2247.4 - Adaptive Instructional Systems (C/LT/AIS) P2247.4.” Accessed December 9, 2021. https://sagroups.ieee.org/2247-4/.

[83] Institute of Electrical and Electronics Engineers Standards Association. “P2817 Guide for Verification of Autonomous Systems.” Accessed February 9, 2022. https://standards.ieee.org/project/2817.html.

[84] Institute of Electrical and Electronics Engineers Standards Association. “IEEE P2830 Working Group.” Accessed February 9, 2022. https://sagroups.ieee.org/2830/.

[85] Institute of Electrical and Electronics Engineers Standards Association. “IEEE P2840 Working Group.” Accessed February 9, 2022. https://sagroups.ieee.org/2840/.

[86] Institute of Electrical and Electronics Engineers Standards Association. “IEEE P2841 Deep Learning Working Group.” Accessed February 9, 2022. https://sagroups.ieee.org/2841/.

[87] Institute of Electrical and Electronics Engineers Standards Association. “IEEE P2850 ICOS Working Group.” Accessed February 9, 2022. https://sagroups.ieee.org/2850/.

[88] Institute of Electrical and Electronics Engineers Standards Association. “IEEE P2863 Organizational Governance of Artificial Intelligence Working Group.” Accessed December 4, 2021. https://sagroups.ieee.org/2863/.

[89] Institute of Electrical and Electronics Engineers Standards Association. “IEEE P2894 Working Group.” Accessed February 9, 2022. https://sagroups.ieee.org/2894/.

[90] Institute of Electrical and Electronics Engineers Standards Association. “IEEE P2895 Working Group.” Accessed February 9, 2022. https://sagroups.ieee.org/2895/.

[91] Institute of Electrical and Electronics Engineers Standards Association. “P2937 Standard for Performance Benchmarking for AI Server Systems.” Accessed February 9, 2022. https://standards.ieee.org/project/2937.html.

[92] Institute of Electrical and Electronics Engineers Standards Association. “P2945 Standard for Technical Requirements for Face Recognition Systems.” Accessed February 9, 2022. https://standards.ieee.org/project/2945.html.

[93] Institute of Electrical and Electronics Engineers Standards Association. “IEEE P2961 Working Group.” Accessed February 9, 2022. https://sagroups.ieee.org/2961/.

[94] Institute of Electrical and Electronics Engineers Standards Association. “IEEE P2986 Working Group.” Accessed February 9, 2022. https://sagroups.ieee.org/2986/.

[95] Institute of Electrical and Electronics Engineers Standards Association. “IEEE P3652.1 Federated Machine Learning Working Group.” Accessed February 9, 2022. https://sagroups.ieee.org/3652-1/.

[96] Institute of Electrical and Electronics Engineers Standards Association. “IEEE - 1.3.1 EMELC-WG - Engineering Methodologies for Ethical Life-Cycle Concerns Working Group | StandICT.Eu 2023.” Accessed December 9, 2021. https://www.standict.eu/standards-repository/working-group/ieee-131-emelc-wg-engineering-methodologies-ethical-life-cycle.

[97] Institute of Electrical and Electronics Engineers Standards Association. “IEEE P7006 Working Group.” Accessed February 9, 2022. https://sagroups.ieee.org/7006/#:~:text=Scope%3A%20This%20standard%20describes%20the,and%20values%20controlled%20by%20individuals.

[98] Institute of Electrical and Electronics Engineers Standards Association. “IEEE P7007 - Ontological Standard for Ethically Driven Robotics and Automation Systems.” Accessed February 9, 2022. https://site.ieee.org/sagroups-7007/.

[99] Institute of Electrical and Electronics Engineers Standards Association. “IEEE P7008 - Ethically Driven Nudging for Robotic, Intelligent and Autonomous Systems.” Accessed February 9, 2022. https://sagroups.ieee.org/7008/.

[100] International Telecommunication Union. “About ITU.” Accessed December 19, 2021. https://www.itu.int/en/about/Pages/default.aspx.

[101] International Telecommunication Union. “Artificial Intelligence.” Accessed December 19, 2021. https://www.itu.int/en/ITU-T/AI/Pages/default.aspx.

[102] International Telecommunication Union. “Focus Group on AI for Autonomous and Assisted Driving (FG-AI4AD).” Accessed December 22, 2021. https://www.itu.int/en/ITU-T/focusgroups/AI4AD/Pages/default.aspx.

[103] International Telecommunication Union. “Focus Group on Environmental Efficiency for Artificial Intelligence and Other Emerging Technologies (FG-AI4EE).” Accessed December 22, 2021. https://www.itu.int/en/ITU-T/focusgroups/AI4EE/Pages/default.aspx.

[104] Wiegand, Thomas, Naomi Lee, Sameer Pujari, Manjula Singh, Shan Xu, Monique Kuglitsch, and Marc Lecoultre et al. “Whitepaper for the ITU/WHO Focus Group on Artificial Intelligence for Health.” International Telecommunication Union (ITU); World Health Organization, 2020. https://www.itu.int/en/ITU-T/focusgroups/ai4h/Pages/default.aspx.

[105] International Telecommunication Union. "Focus Group on AI for Natural Disaster Management (FG-AI4NDM)." Accessed December 22, 2021. https://www.itu.int/en/ITU-T/focusgroups/ai4ndm/Pages/default.aspx.

[106] International Telecommunication Union. "ITU Focus Group on Autonomous Networks (FG-an)." Accessed December 22, 2021. https://www.itu.int/en/ITU-T/focusgroups/AN/Pages/default.aspx.

[107] International Telecommunication Union. "Focus Group on Machine Learning for Future Networks Including 5G." Accessed February 9, 2022. https://www.itu.int/en/ITU-T/focusgroups/ml5g/Pages/default.aspx.

[108] International Telecommunication Union. "Study Group 11 at a Glance." Accessed December 21, 2021. https://www.itu.int/en/ITU-T/about/groups/Pages/sg11.aspx.

[109] International Telecommunication Union. "Study Group 12 at a Glance." Accessed December 21, 2021. https://www.itu.int/en/ITU-T/about/groups/Pages/sg12.aspx.

[110] International Telecommunication Union. "Study Group 13 at a Glance." Accessed December 21, 2021. https://www.itu.int/en/ITU-T/about/groups/Pages/sg13.aspx.

[111] International Telecommunication Union. "Study Group 16 at a Glance." Accessed December 21, 2021. https://www.itu.int/en/ITU-T/about/groups/Pages/sg16.aspx.

[112] International Telecommunication Union. "Study Group 17 at a Glance." Accessed December 21, 2021. https://www.itu.int/en/ITU-T/about/groups/Pages/sg17.aspx.

[113] International Telecommunication Union. "Study Group 2 at a Glance." Accessed December 21, 2021. https://www.itu.int/en/ITU-T/about/groups/Pages/sg02.aspx.

[114] International Telecommunication Union. "Study Group 20 at a Glance." Accessed December 21, 2021. https://www.itu.int/en/ITU-T/about/groups/Pages/sg20.aspx.

[115] International Telecommunication Union. "Study Group 9 at a Glance." Accessed December 21, 2021. https://www.itu.int/en/ITU-T/about/groups/Pages/sg09.aspx.

[116] International Telecommunication Union. "Study Group 3 at a Glance." Accessed February 9, 2022. https://www.itu.int/en/ITU-T/about/groups/Pages/sg03.aspx.

[117] American National Standards Institute. "U.S. TAGs to ISO Committees: ANSI-Accredited U.S. Technical Advisory Groups (TAGS) To ISO." Accessed December 19, 2021. https://www.ansi.org/iso/ansi-activities/us-tags.

[118] European Telecommunications Standards Institute. "About ETSI." Accessed February 13, 2022. https://www.etsi.org/about.

[119] European Telecommunications Standards Institute. "ETSI - Committees for ICT Standardization Work." Accessed December 4, 2021. https://www.etsi.org/committees.

[120] 3rd Generation Partnership Project. "About 3GPP Home." Accessed March 4, 2022. https://www.3gpp.org/about-3gpp/about-3gpp.

[121] European Telecommunications Standards Institute. "CIM: Industry Specification Group (ISG) Cross Cutting Context Information Management (CIM)." Accessed December 21, 2021. https://www.etsi.org/committee/cim.

[122] European Telecommunications Standards Institute. "EHEALTH." Accessed December 21, 2021. https://www.etsi.org/technologies/ehealth.

[123] European Telecommunications Standards Institute. "INT: Technical Committee (TC) Core Network and Interoperability Testing (INT)." Accessed December 21, 2021. https://www.etsi.org/committee/int.

[124] European Telecommunications Standards Institute. "NFV: Industry Specification Group (ISG) Network Functions Virtualisation (NFV)." Accessed December 21, 2021. https://www.etsi.org/committee/nfv.

[125] European Telecommunications Standards Institute. "PDL: Industry Specification Group (ISG) Permissioned Distributed Ledger (PDL)." Accessed December 21, 2021. https://www.etsi.org/committee/1467-pdl.

[126] European Telecommunications Standards Institute. "SmartM2M: Technical Committee (TC) Smart Machine-to-Machine Communications (SmartM2M)." Accessed December 21, 2021. https://www.etsi.org/committee/smartm2m.

[127] European Telecommunications Standards Institute. "ARF: Industry Specification Group (ISG) Augmented Reality Framework (ARF)." Accessed December 21, 2021. https://www.etsi.org/committee/1420-arf.

[128] European Telecommunications Standards Institute. "ETSI Cyber Security Standardisation Overview." Accessed December 21, 2021. https://portal.etsi.org/Portals/0/TBpages/CYBER/2020-10-CYBER-presentation-website.pdf.

[129] European Telecommunications Standards Institute. "Experiential Networked Intelligence (ENI)." Accessed December 21, 2021. https://www.etsi.org/technologies/experiential-networked-intelligence.

[130] European Telecommunications Standards Institute. "Multi-Access Edge Computing (MEC)." Accessed December 21, 2021. https://www.etsi.org/technologies/multi-access-edge-computing.

[131] European Telecommunications Standards Institute. "One Machine-to-Machine Partnership Project (ONEM2M)." Accessed December 21, 2021. https://www.etsi.org/committee/1419-onem2m.

[132] European Telecommunications Standards Institute. "Securing Artificial Intelligence (SAI)." Accessed December 21, 2021. https://www.etsi.org/technologies/securing-artificial-intelligence.

[133] European Telecommunications Standards Institute. "Zero Touch Network & Service Management (ZSM)." Accessed December 21, 2021. https://www.etsi.org/technologies/zero-touch-network-service-management.

[134] Object Management Group. "OMG Specifications Are ISO Standards | Object Management Group." Accessed December 19, 2021. https://www.omg.org/iso/index.htm.

[135] Object Management Group. "Application Programming Interfaces for Knowledge Platforms (API4KP), V1.0 - Beta 1." April 2021. https://www.omg.org/spec/API4KP/1.0/Beta1/PDF.

[136] Object Management Group. "AI Platform Task Force | Object Management Group." Accessed December 9, 2021. https://www.omg.org/ai/.

[137] Responsible AI Institute. "Responsible Artificial Intelligence (RAI) Certification Beta." Responsible AI Institute (RAI), April 2021. https://assets.ctfassets.net/rz1q59puyoaw/1myaH22mA16Y0eIXQND3qv/7974df6bd0973e65f100d327b93129a2/Whitepaper.pdf.

[138] Responsible AI Institute. "RAI | Programs & Tools." Accessed December 19, 2021. https://www.responsible.ai.

[139] Consumer Technology Association. “CTA Committees, Subcommittees and Working Groups.” Accessed December 4, 2021. https://standards.cta.tech/kwspub/home/Committees/.

[140] Consumer Technology Association. “Consumer Technology Association's Active Committees, Subcommittees and Working Groups.” Accessed February 13, 2022. https://standards.cta.tech/kwspub/home/Committees/.

[141] SAE International. “The Mission of SAE International Is to Advance Mobility Knowledge and Solutions.” Accessed May 23, 2023. https://www.sae.org/.

[142] “SAE Levels of Driving Automation™ Refined for Clarity and International Audience.” Accessed May 23, 2023. https://www.sae.org/blog/sae-j3016-update.

[143] Duke Institute for Health Innovation. “Health AI Partnership: An Innovation and Learning Network for Health AI Software.” Accessed December 20, 2022. https://dihi.org/health-ai-partnership-an-innovation-and-learning-network-to-facilitate-the-safe-effective-and-responsible-diffusion-of-health-ai-software-applied-to-health-care-delivery-settings/.

[144] Turpin, Rob, Emily Hoefer, Joe Lewelling, and Pat Baird. “Machine Learning AI in Medical Devices: Adapting Regulatory Frameworks and Standards to Ensure Safety and Performance.” AAAMI; BSI, 2020. https://www.medical-device-regulation.eu/wp-content/uploads/2020/09/machine_learning_ai_in_medical_devices.pdf.

[145] International Medical Device Regulators Forum. “About IMDRF.” Accessed March 28, 2022. https://www.imdrf.org/about.

[146] International Medical Device Regulators Forum. “Working Groups: Participation on Working Groups.” Accessed March 28, 2022. https://www.imdrf.org/about/working-groups.

[147] International Medical Device Regulators Forum. “Artificial Intelligence Medical Devices.” Accessed March 28, 2022. https://www.imdrf.org/working-groups/artificial-intelligence-medical-devices.

[148] The White House. “Listening to the American People - OSTP - the White House.” Accessed May 1, 2023. https://www.whitehouse.gov/ostp/ai-bill-of-rights/listening-to-the-american-people/.

[149] National Artificial Intelligence Initiative. “PUBLIC INPUT on a NATIONAL AI RESEARCH RESOURCE IMPLEMENTATION PLAN.” Accessed May 2, 2023. https://www.ai.gov/nairrtf/86-fr-39081-responses/.

[150] EU Observatory for ICT Standardisation. “The European Observatory for ICT Standardisation.” Accessed March 23, 2022. https://2023.standict.eu/euos.

[151] International Organization for Standardization. “Voting and Membership in ISO.” Accessed December 19, 2021. https://www.iso.org/sites/ConsumersStandards/voting_iso.html.

[152] International Organization for Standardization. “ISO/IEC CD 22123-2.4.” Accessed February 11, 2022. https://www.iso.org/standard/80351.html.

[153] Nativi, Stefano, and Sarah de Nigris. *AI Watch: AI Standardisation Landscape State of Play and Link to the EC Proposal for an AI Regulatory Framework.* EUR 30772. Luxembourg: Publications Office of the European Union, 2021. Accessed December 4, 2021. https://doi.org/10.2760/376602. https://www.standict.eu/sites/default/files/2021-07/jrc125952_ai_watch_task_9_standardization_activity_mapping_v5.1%281%29.pdf.

[154] International Organization for Standardization. "ISO/IEC WD 27046.4." Accessed February 11, 2022. https://www.iso.org/standard/78572.html.

[155] International Organization for Standardization. "ISO/IEC CD 5140." Accessed February 11, 2022. https://www.iso.org/standard/80910.html.

[156] International Organization for Standardization. "ISO/IEC AWI 5339." Accessed December 4, 2021. https://www.iso.org/standard/81120.html.

[157] International Organization for Standardization. "ISO/IEC AWI 5392." Accessed December 4, 2021. https://www.iso.org/standard/81228.html.

[158] International Organization for Standardization. "ISO/IEC AWI TS 5471." Accessed December 4, 2021. https://www.iso.org/standard/82570.html.

[159] International Organization for Standardization. "ISO/IEC AWI TS 5928." Accessed February 11, 2022. https://www.iso.org/standard/81848.html?browse=tc.

[160] International Organization for Standardization. "ISO/IEC AWI TS 6254." Accessed December 9, 2021. https://www.iso.org/standard/82148.html.

[161] International Organization for Standardization. "ISO/IEC AWI TS 8200." Accessed December 4, 2021. https://www.iso.org/standard/83012.html.

[162] International Standards Organization. "ISO/IEC 24668:2022." Accessed December 19, 2022. https://www.iso.org/standard/78368.html.

[163] International Organization for Standardization. "ISO/IEC DIS 27559." Accessed February 11, 2022. https://www.iso.org/standard/71677.html.

[164] International Standards Organization. "ISO/IEC TS 4213:2022." Accessed December 19, 2022. https://www.iso.org/standard/79799.html.

[165] International Organization for Standardization. "ISO/IEC DIS 27556." Accessed February 11, 2022. https://www.iso.org/standard/71674.html.

[166] International Standards Organization. "ISO/IEC TR 24368:2022." Accessed December 19, 2022. https://www.iso.org/standard/78507.html.

[167] International Organization for Standardization. "ISO/IEC DIS 22989." Accessed December 4, 2021. https://www.iso.org/standard/74296.html.

[168] International Organization for Standardization. "ISO/IEC DIS 23053." Accessed December 4, 2021. https://www.iso.org/standard/74438.html.

[169] International Organization for Standardization. "ISO/IEC TR 3445." Accessed February 11, 2022. https://www.iso.org/standard/79582.html.

[170] International Standards Organization. "ISO/IEC 38507:2022." Accessed December 19, 2022. https://www.eeoc.gov/laws/guidance/americans-disabilities-act-and-use-software-algorithms-and-artificial-intelligence.

[171] International Organization for Standardization. "ISO/IEC PRF 19944-2." Accessed February 10, 2022. https://www.iso.org/standard/79574.html.

[172] International Organization for Standardization. "ISO/IEC 23751." Accessed February 11, 2022. https://www.iso.org/standard/76834.html.

[173] International Organization for Standardization. "ISO/IEC 24745:2022." Accessed February 11, 2022. https://www.iso.org/standard/75302.html.

[174] International Organization for Standardization. "ISO/IEC TR 24372:2021." Accessed February 11, 2022. https://www.iso.org/standard/78508.html.

[175] International Organization for Standardization. "ISO/IEC 21838-2:2021." Accessed February 11, 2022. https://www.iso.org/standard/74572.html.

[176] International Organization for Standardization. “ISO/IEC TR 24030:2021.” Accessed December 9, 2021. https://www.iso.org/standard/77610.html.

[177] International Organization for Standardization. “ISO/IEC 22123-1:2021.” Accessed February 11, 2022. https://www.iso.org/standard/80350.html.

[178] International Organization for Standardization. “ISO/IEC TS 27570:2021.” Accessed February 11, 2022. https://www.iso.org/standard/71678.html.

[179] International Organization for Standardization. “ISO/IEC 19944-1:2020.” Accessed February 11, 2022. https://www.iso.org/standard/79573.html.

[180] International Organization for Standardization. “ISO/IEC 20547-4:2020.” Accessed December 9, 2021. https://www.iso.org/standard/71278.html.

[181] International Organization for Standardization. “ISO/IEC TR 20547-1:2020.” Accessed December 9, 2021. https://www.iso.org/standard/71275.html.

[182] International Organization for Standardization. “ISO/IEC 20547-3:2020.” Accessed December 9, 2021. https://www.iso.org/standard/71277.html.

[183] International Organization for Standardization. “ISO/IEC TS 23167:2020.” Accessed February 11, 2022. https://www.iso.org/standard/74805.html.

[184] International Organization for Standardization. “ISO/IEC 20546:2019.” Accessed December 9, 2021. https://www.iso.org/standard/68305.html.

[185] International Organization for Standardization. “ISO/IEC TR 22678:2019.” Accessed February 11, 2022. https://www.iso.org/standard/73642.html.

[186] International Organization for Standardization. “ISO/IEC 20889:2018.” Accessed February 11, 2022. https://www.iso.org/standard/69373.html.

[187] International Organization for Standardization. “ISO/IEC TR 20547-5:2018.” Accessed December 9, 2021. https://www.iso.org/standard/72826.html.

[188] International Organization for Standardization. “ISO/IEC TR 20547-2:2018.” Accessed December 9, 2021. https://www.iso.org/standard/71276.html.

[189] International Organization for Standardization. “ISO/IEC 29134:2017.” Accessed February 11, 2022. https://www.iso.org/standard/62289.html.

[190] International Organization for Standardization. “ISO/IEC 29190:2015.” Accessed February 11, 2022. https://www.iso.org/standard/45269.html.

[191] Institute of Electrical and Electronics Engineers Standards Association. “Developing Standards: The Standards Development Lifecycle.” Accessed December 19, 2021. https://standards.ieee.org/develop/index.html.

[192] Institute of Electrical and Electronics Engineers Standards Association. “PARs, PAR Forms & Continuous Processing.” Accessed December 19, 2021. https://standards.ieee.org/faqs/pars.html.

[193] Institute of Electrical and Electronics Engineers Standards Association. “P2049.1 Standard for Human Augmentation: Taxonomy and Definitions.” Accessed February 10, 2022. https://standards.ieee.org/project/2049_1.html.

[194] Institute of Electrical and Electronics Engineers Standards Association. “P2049.2 Standard for Human Augmentation: Privacy and Security.” Accessed February 10, 2022. https://standards.ieee.org/project/2049_2.html.

[195] Institute of Electrical and Electronics Engineers Standards Association. “P2049.3 Standard for Human Augmentation: Identity.” Accessed February 10, 2022. https://standards.ieee.org/project/2049_3.html.

[196] Institute of Electrical and Electronics Engineers Standards Association. “P2049.4 Standard for Human Augmentation: Methodologies and Processes for Ethical Considerations.” Accessed February 10, 2022. https://standards.ieee.org/project/2049_4.html.

[197] Institute of Electrical and Electronics Engineers Standards Association. “P2247.1 Draft Standard for the Classification of Adaptive Instructional Systems.” Accessed February 10, 2022. https://sagroups.ieee.org/2247-1/.

[198] Institute of Electrical and Electronics Engineers Standards Association. “P2247.2 - Interoperability Standards for Adaptive Instructional Systems (AISs).” Accessed December 4, 2021. https://standards.ieee.org/project/2247_2.html.

[199] Institute of Electrical and Electronics Engineers Standards Association. “P2247.3 - Recommended Practices for Evaluation of Adaptive Instructional Systems.” Accessed December 4, 2021. https://standards.ieee.org/project/2247_3.html.

[200] Institute of Electrical and Electronics Engineers Standards Association. “P2247.4 - Recommended Practice for Ethically Aligned Design of Artificial Intelligence (AI) In Adaptive Instructional Systems.” Accessed December 4, 2021. https://standards.ieee.org/ieee/2247.4/10368/.

[201] Institute of Electrical and Electronics Engineers Standards Association. “IEEE P2671 IEEE Draft Standard for General Requirements of Online Detection Based on Machine Vision in Intelligent Manufacturing.” Accessed May 5, 2022. https://standards.ieee.org/ieee/2671/7176/.

[202] Institute of Electrical and Electronics Engineers Standards Association. “P2672 Guide for General Requirements of Mass Customization.” Accessed February 10, 2022. https://standards.ieee.org/project/2672.html.

[203] Institute of Electrical and Electronics Engineers Standards Association. “P2751 3D Map Data Representation for Robotics and Automation.” Accessed February 10, 2022. https://standards.ieee.org/project/2751.html.

[204] Institute of Electrical and Electronics Engineers Standards Association. “P2802 Standard for the Performance and Safety Evaluation of Artificial Intelligence Based Medical Device: Terminology.” Accessed February 10, 2022. https://standards.ieee.org/project/2802.html.

[205] Institute of Electrical and Electronics Engineers Standards Association. “P2807 Framework of Knowledge Graphs.” Accessed February 10, 2022. https://standards.ieee.org/project/2807.html.

[206] Institute of Electrical and Electronics Engineers Standards Association. “P2807.1 Standard for Technical Requirements and Evaluation of Knowledge Graphs.” Accessed February 10, 2022. https://standards.ieee.org/project/2807_1.html.

[207] Institute of Electrical and Electronics Engineers Standards Association. “P2807.2 Guide for Application of Knowledge Graphs for Financial Services.” Accessed February 10, 2022. https://standards.ieee.org/project/2807_2.html.

[208] Institute of Electrical and Electronics Engineers Standards Association. “P2807.4 Guide for Scientific Knowledge Graphs.” Accessed February 10, 2022. https://standards.ieee.org/project/2807_4.html.

[209] Institute of Electrical and Electronics Engineers Standards Association. “P2817 Guide for Verification of Autonomous Systems.” Accessed February 10, 2022. https://standards.ieee.org/ieee/2817/7644/.

[210] Institute of Electrical and Electronics Engineers Standards Association. “P2840 Standard for Responsible AI Licensing.” Accessed February 10, 2022. https://standards.ieee.org/project/2840.html.

[211] Institute of Electrical and Electronics Engineers Standards Association. “P2841 Framework and Process for Deep Learning Evaluation.” Accessed February 10, 2022. https://standards.ieee.org/project/2841.html.

[212] Institute of Electrical and Electronics Engineers Standards Association. “P2850 Standard for an Architectural Framework for Intelligent Cities Operation System.” Accessed February 10, 2022. https://standards.ieee.org/project/2850.html.

[213] Institute of Electrical and Electronics Engineers Standards Association. “P2874 Standard for Spatial Web Protocol, Architecture and Governance.” Accessed February 10, 2022. https://standards.ieee.org/project/2874.html.

[214] Institute of Electrical and Electronics Engineers Standards Association. “P2888.6 Standard for Holographic Visualization for Interfacing Cyber and Physical Worlds.” Accessed May 5, 2022. https://standards.ieee.org/ieee/2888.6/10788/.

[215] Institute of Electrical and Electronics Engineers Standards Association. “P2894 Guide for an Architectural Framework for Explainable Artificial Intelligence.” Accessed February 10, 2022. https://standards.ieee.org/project/2894.html.

[216] Institute of Electrical and Electronics Engineers Standards Association. “P2895 Standard Taxonomy for Responsible Trading of Human-Generated Data.” Accessed February 10, 2022. https://standards.ieee.org/project/2895.html.

[217] Institute of Electrical and Electronics Engineers Standards Association. “2941-2021 IEEE Approved Draft Standard for Artificial Intelligence (AI) Model Representation, Compression, Distribution and Management.” Accessed February 10, 2022. https://standards.ieee.org/project/2941.html.

[218] Institute of Electrical and Electronics Engineers Standards Association. “P2961 Guide for an Architectural Framework and Application for Collaborative Edge Computing.” Accessed February 10, 2022. https://standards.ieee.org/project/2961.html.

[219] Institute of Electrical and Electronics Engineers Standards Association. “P2975 Standard for Industrial Artificial Intelligence (AI) Data Attributes.” Accessed February 10, 2022. https://standards.ieee.org/project/2975.html.

[220] Institute of Electrical and Electronics Engineers Standards Association. “P2986 Recommended Practice for Privacy and Security for Federated Machine Learning.” Accessed February 10, 2022. https://standards.ieee.org/project/2986.html.

[221] Institute of Electrical and Electronics Engineers Standards Association. “IEEE P2995 Trial-Use Standard for a Quantum Algorithm Design and Development.” Accessed May 5, 2022. https://standards.ieee.org/ieee/2995/10633/.

[222] Institute of Electrical and Electronics Engineers Standards Association. “P3110 Standard for Computer Vision (CV) - Algorithms, Application Programming Interfaces (API), and Technical Requirements for Deep Learning Framework.” Accessed May 5, 2022. https://standards.ieee.org/ieee/3110/10687/.

[223] Institute of Electrical and Electronics Engineers Standards Association. “P3119 Standard for the Procurement of Artificial Intelligence and Automated Decision Systems.” Accessed May 5, 2022. https://standards.ieee.org/ieee/3119/10729/.

[224] Institute of Electrical and Electronics Engineers Standards Association. “P3135 Standard for Specifying Requirements for Neurofeedback Systems Design.” Accessed May 5, 2022. https://standards.ieee.org/ieee/3135/10790/.

[225] Institute of Electrical and Electronics Engineers Standards Association. “P3141 Standard for 3D Body Processing.” Accessed May 5, 2022. https://standards.ieee.org/ieee/3141/10825/.

[226] Institute of Electrical and Electronics Engineers Standards Association. “P7003 Algorithmic Bias Considerations.” Accessed February 10, 2022. https://standards.ieee.org/project/7003.html.

[227] Institute of Electrical and Electronics Engineers Standards Association. “P7004 Standard for Child and Student Data Governance.” Accessed February 10, 2022. https://standards.ieee.org/project/7004.html.

[228] Institute of Electrical and Electronics Engineers Standards Association. “P7004.1 Recommended Practices for Virtual Classroom Security, Privacy and Data Governance.” Accessed May 5, 2022. https://standards.ieee.org/ieee/7004.1/10285/.

[229] Institute of Electrical and Electronics Engineers Standards Association. “P7008 Standard for Ethically Driven Nudging for Robotic, Intelligent and Autonomous Systems.” Accessed February 10, 2022. https://standards.ieee.org/project/7008.html.

[230] Institute of Electrical and Electronics Engineers Standards Association. “P7009 Standard for Fail-Safe Design of Autonomous and Semi-Autonomous Systems.” Accessed February 10, 2022. https://standards.ieee.org/project/7009.html.

[231] Institute of Electrical and Electronics Engineers Standards Association. “P7010.1 Recommended Practice for Environmental Social Governance (ESG) And Social Development Goal (SDG) Action Implementation and Advancing Corporate Social Responsibility.” Accessed May 5, 2022. https://standards.ieee.org/ieee/7010.1/10756/.

[232] Institute of Electrical and Electronics Engineers Standards Association. “P7011 Standard for the Process of Identifying and Rating the Trustworthiness of News Sources.” Accessed February 10, 2022. https://standards.ieee.org/project/7011.html.

[233] Institute of Electrical and Electronics Engineers Standards Association. “P7012 Standard for Machine Readable Personal Privacy Terms.” Accessed February 10, 2022. https://standards.ieee.org/project/7012.html.

[234] Institute of Electrical and Electronics Engineers Standards Association. “P7014 Standard for Ethical Considerations in Emulated Empathy in Autonomous and Intelligent Systems.” Accessed February 10, 2022. https://standards.ieee.org/project/7014.html.

[235] Institute of Electrical and Electronics Engineers Standards Association. “P7015 Standard for Data and Artificial Intelligence (AI) Literacy, Skills, and Readiness.” Accessed May 5, 2022. https://standards.ieee.org/ieee/7015/10688/.

[236] Institute of Electrical and Electronics Engineers Standards Association. “P7030 Recommended Practice for Ethical Assessment of Extended Reality (XR) Technologies.” Accessed May 5, 2022. https://standards.ieee.org/ieee/7030/10799/.

[237] Institute of Electrical and Electronics Engineers Standards Association. “P7130 Standard for Quantum Technologies Definitions.” Accessed May 5, 2022. https://standards.ieee.org/ieee/7130/10680/.

[238] Institute of Electrical and Electronics Engineers Standards Association. “P2801 IEEE Draft Recommended Practice for the Quality Management of Datasets for Medical

Artificial Intelligence.” Accessed February 10, 2022. https://standards.ieee.org/project/2801.html.

[239] Institute of Electrical and Electronics Engineers Standards Association. “P3333.1.3 Draft Standard for the Deep Learning Based Assessment of Visual Experience Based on Human Factors.” Accessed February 10, 2022. https://standards.ieee.org/project/3333_1_3.html.

[240] Institute of Electrical and Electronics Engineers Standards Association. “P1872.2-2021 Draft Standard for Autonomous Robotics (AuR) Ontology.” Accessed February 10, 2022. https://standards.ieee.org/standard/1872_2-2021.html.

[241] Institute of Electrical and Electronics Engineers Standards Association. “IEEE 7001-2021 IEEE Approved Draft Standard for Transparency of Autonomous Systems.” Accessed February 10, 2022. https://standards.ieee.org/project/7001.html.

[242] Institute of Electrical and Electronics Engineers Standards Association. “P7002 IEEE Draft Standard for Data Privacy Process.” Accessed February 10, 2022. https://standards.ieee.org/project/7002.html.

[243] Institute of Electrical and Electronics Engineers Standards Association. “2089-2021 IEEE Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children.” Accessed February 10, 2022. https://standards.ieee.org/standard/2089-2021.html.

[244] Institute of Electrical and Electronics Engineers Standards Association. “7005-2021 IEEE Standard for Transparent Employer Data Governance.” Accessed February 10, 2022. https://standards.ieee.org/standard/7005-2021.html.

[245] Institute of Electrical and Electronics Engineers Standards Association. “7007-2021 IEEE Ontological Standard for Ethically Driven Robotics and Automation Systems.” Accessed February 10, 2022. https://standards.ieee.org/standard/7007-2021.html.

[246] Institute of Electrical and Electronics Engineers Standards Association. “2842-2021 IEEE Recommended Practice for Secure Multi-Party Computation.” Accessed February 10, 2022. https://standards.ieee.org/standard/2842-2021.html.

[247] Institute of Electrical and Electronics Engineers Standards Association. “2830-2021 IEEE Standard for Technical Framework and Requirements of Trusted Execution Environment Based Shared Machine Learning.” Accessed February 10, 2022. https://standards.ieee.org/standard/2830-2021.html.

[248] Institute of Electrical and Electronics Engineers Standards Association. “IEEE 7000-2021 - IEEE Standard Model Process for Addressing Ethical Concerns During System Design.” Accessed December 9, 2021. https://standards.ieee.org/standard/7000-2021.html.

[249] Institute of Electrical and Electronics Engineers Standards Association. “3652.1-2020 IEEE Guide for Architectural Framework and Application of Federated Machine Learning.” Accessed February 10, 2022. https://standards.ieee.org/standard/3652_1-2020.html.

[250] Institute of Electrical and Electronics Engineers Standards Association. “IEEE 2660.1-2020 IEEE Recommended Practice for Industrial Agents: Integration of Software Agents and Low-Level Automation Functions.” Accessed May 5, 2022. https://standards.ieee.org/ieee/2660.1/6264/.

[251] Institute of Electrical and Electronics Engineers Standards Association. “7010-2020 IEEE Recommended Practice for Assessing the Impact of Autonomous and Intelligent

Systems on Human Well-Being." Accessed February 10, 2022. https://standards.ieee.org/standard/7010-2020.html.

[252] Institute of Electrical and Electronics Engineers Standards Association. "1855-2016 IEEE Standard for Fuzzy Markup Language." Accessed February 10, 2022. https://standards.ieee.org/standard/1855-2016.html.

[253] Institute of Electrical and Electronics Engineers Standards Association. "1873-2015 IEEE Standard for Robot Map Data Representation." Accessed February 10, 2022. https://ieeexplore.ieee.org/document/7300355.

[254] Institute of Electrical and Electronics Engineers Standards Association. "IEEE 1232.3-2014 - IEEE Guide for the Use of Artificial Intelligence Exchange and Service Tie to All Test Environments (AI-ESTATE)." Accessed December 4, 2021. https://standards.ieee.org/standard/1232_3-2014.html.

[255] Consumer Technology Association. "R13 - CTA-2096-Guidelines for Developing Trustworthy Artificial Intelligence Systems." Accessed December 4, 2021. https://standards.cta.tech/apps/group_public/project/details.php?project_id=637.

[256] Consumer Technology Association. "R13WG1-CTA-2090, the Use of Artificial Intelligence in Health Care: Trustworthiness." Accessed February 11, 2022. https://standards.cta.tech/apps/group_public/project/details.php?project_id=609.

[257] American National Standards Institute. "ANSI/CTA-2089.1-2020 - Definitions/Characteristics of Artificial Intelligence in Health Care." Accessed December 4, 2021. https://webstore.ansi.org/standards/ansi/ansicta20892020.

[258] National Institute of Standards and Technology. "NIST Special Publication 500-290 Edition 3 (2015): Information Technology: American National Standard for Information Systems." Accessed February 11, 2022. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-290e3.pdf.

[259] Object Management Group. "Decision Model and Notation™ (DMN™) | Object Management Group." Accessed December 9, 2021. https://www.omg.org/dmn/.

[260] Object Management Group. "About the Semantics of Business Vocabulary and Business Rules Specification Version 1.5." Accessed December 9, 2021. https://www.omg.org/spec/SBVR/1.5/About-SBVR/.

[261] Object Management Group. "About the Distributed Ontology, Model, and Specification Language Specification Version 1.0." Accessed December 9, 2021. https://www.omg.org/spec/DOL/1.0/About-DOL/.

[262] Object Management Group. "Robotic Interaction Service Framework (RoIS)." Object Management Group (OMG), 2016. https://www.omg.org/spec/RoIS/1.2/PDF/changebar.

[263] Object Management Group. "About the Finite State Machine Component for RTC Specification Version 1.0." Accessed December 9, 2021. https://www.omg.org/spec/FSM4RTC/1.0/About-FSM4RTC/.

[264] Object Management Group. "Ontology Definition Metamodel™ (ODM™) | Object Management Group." Accessed December 4, 2021. https://www.omg.org/odm/.

[265] Object Management Group. "About the Robotic Technology Component Specification Version 1.1." Accessed December 9, 2021. https://www.omg.org/spec/RTC/About-RTC/.

[266] Harris, Laurie A. “Overview of Artificial Intelligence.” Congressional Research Service In Focus, Congressional Research Service, 2017. https://crsreports.congress.gov/product/pdf/IF/IF10608.

[267] PricewaterhouseCoopers. “Sizing the Prize: What’s the Real Value of AI for Your Business and How Can You Capitalise?,” 2017. https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf.

[268] Arnold, Zachary, Ilya Rahkovsky, and Tina Huang. “Tracking AI Investment: Initial Findings from the Private Markets.” Center for Security and Emerging Technology, September 2020. https://cset.georgetown.edu/publication/tracking-ai-investment/.

[269] Lubongo, Cesar, and Paschalis Alexandridis. “Assessment of Performance and Challenges in Use of Commercial Automated Sorting Technology for Plastic Waste.” *Recycling* 7, no. 2 (2022): 11. https://doi.org/10.3390/recycling7020011.

[270] Srivastava, Swapnil. “10 Ways AI Is Transforming the Restaurant Industry.” Accessed December 29, 2022. https://www.forbes.com/sites/forbestechcouncil/2022/09/22/10-ways-ai-is-transforming-the-restaurant-industry/?sh=350668916ec8.

[271] Federal Register. “Request for Comments on Artificial Intelligence Export Competitiveness.” Accessed December 20, 2022. https://www.federalregister.gov/documents/2022/08/16/2022-17576/request-for-comments-on-artificial-intelligence-export-competitiveness.

[272] Department of Commerce. “Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items; Supercomputer and Semiconductor End Use; Entity List Modification.” *Federal Register* 87, no. 197 (2022): 62186–215. Accessed December 20, 2022. https://www.govinfo.gov/content/pkg/FR-2022-10-13/pdf/2022-21658.pdf.

[273] National Science and Technology Council. “SC-AI Charter.” 2016. Accessed March 30, 2022. https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/NSTC/ai_charter_-_signed_final.pdf.

[274] The White House. “Select Committee on Artificial Intelligence | the White House.” Accessed December 4, 2021. https://www.whitehouse.gov/ostp/nstc/select-committee-on-artificial-intelligence/.

[275] National Artificial Intelligence Initiative. “MLAI-SC - Machine Learning and AI Subcommittee.” Accessed December 9, 2021. https://www.ai.gov/about/#MLAI-SC-MACHINE-LEARNING-AND-AI-SUBCOMMITTEE.

[276] National Artificial Intelligence Initiative. “AI R&D IWG - NITRD AI R&D Interagency Working Group.” Accessed December 20, 2021. https://www.ai.gov/about/#AI-IWG-NITRD-AI-INTERAGENCY-WORKING-GROUP.

[277] National Artificial Intelligence Initiative. “SCAI - Select Committee on AI.” Accessed December 4, 2021. https://www.ai.gov/about/#SCAI-SELECT-COMMITTEE-ON-AI.

[278] Vought, Russell T. “M-21-06: Guidance for Regulation of Artificial Intelligence Applications.” Accessed December 19, 2021. https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-06.pdf.

[279] Chief Information Officers Council. “Home: Welcome to CIO.Gov!.” Accessed December 20, 2021. https://www.cio.gov/.

[280] Chief Information Officers Council. "Members and Leadership: Who We Are." Accessed December 20, 2021. https://www.cio.gov/about/members-and-leadership/#council-committees.

[281] Memorandum on Renewing the National Security Council System. National Security Memorandum/NSM-2. Executive Office of the President. February 4, 2021. Accessed December 20, 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/02/04/memorandum-renewing-the-national-security-council-system/.

[282] The White House. "Charter of the Subcommittee on Open Science." 2022. Accessed December 19, 2022. https://www.whitehouse.gov/wp-content/uploads/2022/08/08-2022-SOS-NSTC-CHARTER.pdf.

[283] National Institute of Standards and Technology. "AI Standards: Federal Engagement." Accessed December 9, 2021. https://www.nist.gov/artificial-intelligence/ai-standards-federal-engagement.

[284] National Artificial Intelligence Initiative Office. "Agency Inventories of AI Use Cases." Accessed December 30, 2022. https://www.ai.gov/ai-use-case-inventories/.

[285] National Institute of Standards and Technology. "U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools." 2019. https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf.

[286] Office of Federal Contract Compliance Programs. "HIRE Fact Sheet." Accessed December 29, 2022. https://www.dol.gov/sites/dolgov/files/OFCCP/pdf/HIREInitiativeFactSheet-508c.pdf.

[287] Department of Veterans Affairs, Veterans Health Administration Office of Chief Research and Development Officer. "Join Our AI Communities!." Accessed December 29, 2022. https://www.research.va.gov/naii/join.cfm#signup.

[288] General Services Administration. "Artificial Intelligence | GSA - IT Modernization Centers of Excellence: Accelerate Adoption of Artificial Intelligence to Discover Insights at Machine Speed." Accessed December 4, 2021. https://coe.gsa.gov/coe/artificial-intelligence.html.

[289] General Services Administration. "Federal Robotic Process Automation Community of Practice." Accessed January 2, 2023. https://www.gsa.gov/technology/government-it-initiatives/federal-robotic-process-automation-community-of-practice.

[290] The White House. "Fact Sheet: Biden-Harris Administration Announces Key Actions to Advance Tech Accountability and Protect the Rights of the American Public." Accessed December 29, 2022. https://www.whitehouse.gov/ostp/news-updates/2022/10/04/fact-sheet-biden-harris-administration-announces-key-actions-to-advance-tech-accountability-and-protect-the-rights-of-the-american-public/.

[291] US EEOC. "Select Issues: Assessing Adverse Impact in Software, Algorithms, and Artificial Intelligence Used in Employment Selection Procedures Under Title VII of the Civil Rights Act of 1964." Accessed June 26, 2023. https://www.eeoc.gov/select-issues-assessing-adverse-impact-software-algorithms-and-artificial-intelligence-used.

[292] U.S. Department of Education. "Artificial Intelligence and the Future of Teaching and Learning (PDF)." May 2023. Accessed May 23, 2023. https://www2.ed.gov/documents/ai-report/ai-report.pdf.

[293] EEOC. “Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems.” Accessed June 22, 2023. https://www.eeoc.gov/joint-statement-enforcement-efforts-against-discrimination-and-bias-automated-systems.

[294] The White House. “Blueprint for an AI Bill of Rights | OSTP | the White House.” Accessed December 28, 2022. https://www.whitehouse.gov/ostp/ai-bill-of-rights/.

[295] U.S. Food and Drug Administration. “Medical Device Data Systems, Medical Image Storage Devices, and Medical Image Communications Devices: Guidance for Industry and Food and Drug Administration Staff.” FDA, September 28, 2022. https://www.fda.gov/media/88572/download#page=6&zoom=100,144,158.

[296] U.S. Food and Drug Administration. “Computer Software Assurance for Production and Quality System Software: Draft Guidance for Industry and Food and Drug Administration Staff.” U.S. Food and Drug Administration (FDA), September 2022. https://www.fda.gov/media/161521/download.

[297] Department of Veterans Affairs. “AR52-Final Rule-Principle-Based Ethics Framework for Access to and Use of Veteran Data.” Accessed December 29, 2022. https://www.regulations.gov/document/VA-2022-OTHER-0017-0001.

[298] Federal Register. “Medicare Program: Hospital Outpatient Prospective Payment and Ambulatory Surgical Center Payment Systems and Quality Reporting Programs; Organ Acquisition; Rural Emergency Hospitals: Payment Policies, Conditions of Participation, Provider Enrollment, Physician Self-Referral; New Service Category for Hospital Outpatient Department Prior Authorization Process; Overall Hospital Quality Star Rating; COVID-19.” Accessed January 3, 2023. https://www.federalregister.gov/documents/2022/11/23/2022-23918/medicare-program-hospital-outpatient-prospective-payment-and-ambulatory-surgical-center-payment.

[299] Federal Register. “Nondiscrimination in Health Programs and Activities.” Accessed December 29, 2022. https://www.federalregister.gov/documents/2022/08/04/2022-16217/nondiscrimination-in-health-programs-and-activities.

[300] US EEOC. “The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees.” Accessed June 26, 2023. https://www.eeoc.gov/laws/guidance/americans-disabilities-act-and-use-software-algorithms-and-artificial-intelligence.

[301] Consumer Financial Protection Bureau. “Consumer Financial Protection Circular 2022-03: Adverse Action Notification Requirements in Connection with Credit Decisions Based on Complex Algorithms.” | Consumer Financial Protection Bureau. Accessed December 29, 2022. https://www.consumerfinance.gov/compliance/circulars/circular-2022-03-adverse-action-notification-requirements-in-connection-with-credit-decisions-based-on-complex-algorithms/.

[302] Office of Information and Regulatory Affairs. “View Rule.” Trade Regulation Rule on Commercial Surveillance. Accessed December 29, 2022. https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202110&RIN=3084-AB69.

[303] Agency for Healthcare Research and Quality. “Impact of Healthcare Algorithms on Racial and Ethnic Disparities in Health and Healthcare: Research Protocol.” Accessed December 29, 2022.

[304] EEOC. “EEOC Launches Initiative on Artificial Intelligence and Algorithmic Fairness.” Accessed May 23, 2023. https://www.eeoc.gov/newsroom/eeoc-launches-initiative-artificial-intelligence-and-algorithmic-fairness.

[305] Federal Register. “Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning.” Accessed December 30, 2022. https://www.federalregister.gov/documents/2021/03/31/2021-06607/request-for-information-and-comment-on-financial-institutions-use-of-artificial-intelligence.

[306] U.S. Food and Drug Administration. “Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) Action Plan.” January 2021. https://www.fda.gov/media/145022/download.

[307] Executive Order on Further Advancing Racial Equity and Support for Underserved Communities Through The Federal Government. EO 14091. Executive Office of the President. February 16, 2023. Accessed April 21, 2023. https://www.whitehouse.gov/briefing-room/presidential-actions/2023/02/16/executive-order-on-further-advancing-racial-equity-and-support-for-underserved-communities-through-the-federal-government/.

[308] Administrative Conference of the United States. “Artificial Intelligence | Administrative Conference of the United States.” Accessed May 1, 2023. https://www.acus.gov/ai.

[309] National Science and Technology Council. “National Artificial Intelligence Research and Development Strategic Plan 2023 Update.” May 2023. Accessed May 23, 2023. https://www.whitehouse.gov/wp-content/uploads/2023/05/National-Artificial-Intelligence-Research-and-Development-Strategic-Plan-2023-Update.pdf.

[310] National Institute of Standards and Technology. “Trustworthy & Responsible Artificial Intelligence Resource Center (AIRC).” Accessed May 19, 2023. https://airc.nist.gov/Home.

[311] Federal Register. “Draft Strategic Enforcement Plan.” Accessed May 19, 2023. https://www.federalregister.gov/documents/2023/01/10/2023-00283/draft-strategic-enforcement-plan.

[312] National Institute of Standards and Technology. “Trustworthy AI Conference (TRUC).” 2022. https://www.nist.gov/news-events/events/2022/10/trustworthy-ai-conference-truc-2022.

[313] Department of Defense. “Responsible Artificial Intelligence Strategy and Implementation Pathway.” Department of Defense (DOD), June 2022. https://www.ai.mil/docs/RAI_Strategy_and_Implementation_Pathway_6-21-22.pdf.

[314] U.S. Nuclear Regulatory Commission. “Artificial Intelligence Strategic Plan.” 2022. Accessed May 19, 2023. https://www.nrc.gov/docs/ML2217/ML22175A206.pdf.

[315] USAID. “Artificial Intelligence Action Plan: Charting the Course for Responsible AI in USAID Programming.” USAID, May 2022. https://www.usaid.gov/sites/default/files/2022-05/USAID_Artificial_Intelligence_Action_Plan.pdf.

[316] Federal Register. “Occupant Protection for Vehicles with Automated Driving Systems.” Accessed May 19, 2023. https://www.federalregister.gov/documents/2022/03/30/2022-05426/occupant-protection-for-vehicles-with-automated-driving-systems.

[317] National Geospatial-Intelligence Agency. “NGA Data Strategy.” Accessed February 13, 2022. https://www.nga.mil/assets/files/RCD_U_2021-00986_210205-006_NGA_Data_Strategy_Digital__APPROVED_21-873_093021_v6.pdf.

[318] U.S. Department of State. “Enterprise Data Strategy: Empowering Data Informed Diplomacy.” Accessed February 13, 2022. https://www.state.gov/wp-content/uploads/2021/09/Reference-EDS-Accessible.pdf.

[319] U.S. Department of the Navy. “Department of the Navy Science & Technology Strategy for Intelligent Autonomous Systems.” Accessed February 13, 2021. https://www.onr.navy.mil/Media-Center/Press-Releases/2021/ONR-IAS-Strategy-Release.

[320] U.S. Department of Homeland Security. “S&T Artificial Intelligence & Machine Learning Strategic Plan.” Accessed February 13, 2022. https://www.dhs.gov/sites/default/files/publications/21_0730_st_ai_ml_strategic_plan_2021.pdf.

[321] U.S. Department of Veterans Affairs. “Artificial Intelligence (AI) Strategy: U.S. Department of Veterans Affairs.” Accessed February 13, 2022. https://www.research.va.gov/naii/VA_AI%20Strategy_V2-508.pdf.

[322] U.S. Government Accountability Office. “Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entitites.” GAO-21-519SP, June 2021. https://www.gao.gov/assets/gao-21-519sp.pdf.

[323] National Artificial Intelligence Initiative. “NAIIO - National Artificial Intelligence Initiative Office.” Accessed December 20, 2021. https://www.ai.gov/about/#NAIIO_National_Artificial_Intelligence_Initiative_Office.

[324] U.S. Department of Health and Human Services. “Artificial Intelligence (AI) Strategy: U.S. Department of Health and Human Services.” Accessed February 13, 2022. https://www.hhs.gov/sites/default/files/final-hhs-ai-strategy.pdf.

[325] Agency Use of Artificial Intelligence. Administrative Conference of the United States. 86 Federal Register 6616. December 16, 2020.

[326] *Federal Register*.

[327] “Executive Order on Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government: EO 13960.” In, *Federal Register*, 78939–43.

[328] Office of the Director of National Intelligence. “Artificial Intelligence Ethics Framework for the Intelligence Community.” June 2020. https://www.intelligence.gov/images/AI/AI_Ethics_Framework_for_the_Intelligence_Community_1.0.pdf.

[329] National Oceanic and Atmospheric Administration. “NOAA Artificial Intelligence Strategy: Analytics for Next-Generation Earth Science.” Accessed February 13, 2022. https://sciencecouncil.noaa.gov/Portals/0/2020%20AI%20Strategy.pdf.

[330] Defense Innovation Board. “AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense.” Defense Innovation Board, 2019. https://media.defense.gov/2019/Oct/31/2002204458/-1/-1/0/DIB_AI_PRINCIPLES_PRIMARY_DOCUMENT.PDF.

[331] U.S. Department of Defense. “DOD Adopts Ethical Principles for Artificial Intelligence.” Accessed December 19, 2021. https://www.defense.gov/News/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/.

[332] U.S. Department of the Air Force. “The United States Air Force Artificial Intelligence Annex to the Department of Defense Artificial Intelligence Strategy.” Accessed February 13, 2022. https://media.defense.gov/2019/Sep/12/2002182176/-1/-

1/1/US%20AIR%20FORCE%20AI%20ANNEX%20TO%20DOD%20AI%20STRATEGY.PDF.

[333] Federal Register. “Request for Information to the Update of the National Artificial Intelligence Research and Development Strategic Plan.” Accessed December 20, 2022. https://www.federalregister.gov/documents/2022/02/02/2022-02161/request-for-information-to-the-update-of-the-national-artificial-intelligence-research-and.

[334] Defense Advanced Research Projects Agency. “AI Next Campaign.” Accessed May 19, 2023. https://www.darpa.mil/work-with-us/ai-next-campaign.

[335] U.S. Department of Defense. “Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity.” February 12, 2019. https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF.

[336] United States Patent and Trademark Office, European Patent Office, Japan Patent Office, Korean Intellectual Property Office, and National Intellectual Property Administration. “New Emerging Technologies and Artificial Intelligence (NET/AI) | FiveIPoffices.” Accessed August 10, 2022. https://www.fiveipoffices.org/activities/NET_AI.

[337] World Intellectual Property Organization. “Artificial Intelligence and Intellectual Property Policy.” Accessed August 10, 2022. https://www.wipo.int/about-ip/en/artificial_intelligence/conversation.html.

[338] Organisation for Economic Co-operation and Development. “OECD Network of Experts on AI (ONE AI).” Accessed February 13, 2022. https://oecd.ai/en/network-of-experts.

[339] *The White House*. “Fact Sheet: Quad Summit.” March 12, 2021. Accessed August 19, 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2021/03/12/fact-sheet-quad-summit/.

[340] *The White House*. “U.S.-EU Trade and Technology Council Inaugural Joint Statement.” September 29, 2021. Accessed December 20, 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/29/u-s-eu-trade-and-technology-council-inaugural-joint-statement/.

[341] Organisation for Economic Co-operation and Development. “Tools for Trustworthy AI: A Framework to Compare Implementation Tools for Trustworthy AI Systems.” 312 (2021): 24. Accessed December 4, 2021. https://doi.org/10.1787/008232ec-en.

[342] Organisation for Economic Co-operation and Development. “Public Consultation on the OECD Framework for Classifying AI Systems.” Accessed December 22, 2021. https://oecd.ai/en/wonk/classification.

[343] Environment News Service. “Artificial Intelligence Ethics Approved by 193 Countries.” *Environment News Service*, December 1, 2021. Accessed December 21, 2021. https://ens-newswire.com/artificial-intelligence-ethics-approved-by-193-countries/.

[344] Organisation for Economic Co-operation and Development. “OECD Legal Instruments.” Accessed December 4, 2021. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

[345] U.S. Government Accountability Office. “Science & Tech Spotlight: GENERATIVE AI.” GAO-23-106782, Government Accountability Office (GAO), June 13, 2023. https://www.gao.gov/assets/gao-23-106782.pdf.

[346] U.S. Food and Drug Administration. “Artificial Intelligence and Machine Learning (AI/ML)-Enabled Medical Devices.” Accessed December 28, 2022. https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-aiml-enabled-medical-devices.

[347] Department of Labor. “What the Blueprint for an AI Bill of Rights Means for Workers.” U.S. Department of Labor Blog. Accessed December 29, 2022. https://blog.dol.gov/2022/10/04/what-the-blueprint-for-an-ai-bill-of-rights-means-for-workers.

[348] Department of Energy. “DOE AI Risk Management Playbook (AIRMP).” Accessed December 29, 2022. https://www.energy.gov/ai/doe-ai-risk-management-playbook-airmp.

[349] Federal Trade Commission. “Combatting Online Harms Through Innovation; Federal Trade Commission Report to Congress.” Accessed August 10, 2022. https://www.ftc.gov/system/files/ftc_gov/pdf/Combatting%20Online%20Harms%20Through%20Innovation%3B%20Federal%20Trade%20Commission%20Report%20to%20Congress.pdf.

[350] Consolidated Appropriations Act, 2021. Public Law 116-260. U.S. Congress. June 8, 2022. Accessed June 8, 2022. https://www.congress.gov/bill/116th-congress/house-bill/133/text.

[351] United States Equal Employment Opportunity Commission. “The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees.” Accessed December 20, 2022. https://www.eeoc.gov/laws/guidance/americans-disabilities-act-and-use-software-algorithms-and-artificial-intelligence.

[352] U.S. Department of Justice. “Algorithms, Artificial Intelligence, and Disability Discrimination in Hiring.” Accessed December 20, 2022. https://www.ada.gov/resources/ai-guidance/.

[353] Consumer Product Safety Commission. “Consumer Product Safety Commission: A Notice by the Consumer Product Safety Commission on 01/28/2022.” Accessed March 28, 2022. https://www.federalregister.gov/documents/2022/01/28/2022-01721/cpsc-artificial-intelligence-and-machine-learning-test-and-evaluation-forum.

[354] Schwartz, Reva, Apostol Vassilev, Kristen Greene, Lori Perine, Andrew Burt, and Patrick Hall. “Towards a Standard for Identifying and Managing Bias in Artificial Intelligence.” 2022. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1270.pdf.

[355] U.S. Patent and Trademark Office. “Artificial Intelligence Patent Dataset.” Accessed December 28, 2022. https://www.uspto.gov/ip-policy/economic-research/research-datasets/artificial-intelligence-patent-dataset.

[356] U.S. Patent and Trademark Office. “AI-Related Patent Resources.” Accessed January 3, 2023. https://www.uspto.gov/initiatives/artificial-intelligence/artificial-intelligence-resources.

[357] Federal Trade Commission. “Aiming for Truth, Fairness, and Equity in Your Company’s Use of AI.” Accessed December 4, 2021. https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai.

[358] Federal Trade Commission. “Using Artificial Intelligence and Algorithms.” Accessed December 4, 2021. https://www.ftc.gov/news-events/blogs/business-blog/2020/04/using-artificial-intelligence-algorithms.

[359] National Institute of Standards and Technology. “Privacy Framework.” Accessed December 9, 2021. https://www.nist.gov/privacy-framework/privacy-framework.

[360] Federal Trade Commission. “Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues.” FTC Report, 2016. https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.

[361] Networking and Information Technology Research and Development Program. “AI R&D Testbed Inventory.” Accessed December 20, 2021. https://www.nitrd.gov/apps/ai-rd-testbed-inventory/.

[362] NAIRR Task Force. “Strengthening and Democratizing the U.S. Artificial Intelligence Innovation Ecosystem: An Implementation Plan for a National Artificial Intelligence Research Resource.” January 2023. https://www.ai.gov/wp-content/uploads/2023/01/NAIRR-TF-Final-Report-2023.pdf.

[363] National Center for Science and Engineering Statistics. “Standard Application Process | NSF - National Science Foundation.” Accessed December 30, 2022. https://ncses.nsf.gov/about/standard-application-process.

[364] PEAT. “AI & Disability Inclusion Toolkit: Implementing Equitable AI in the Workplace.” Accessed December 20, 2022. https://www.peatworks.org/ai-disability-inclusion-toolkit/.

[365] PEAT. “The Equitable AI Playbook - Peatworks: How to Use Artificial Intelligence While Fostering Workplace Inclusion.” Accessed December 20, 2022. https://www.peatworks.org/ai-disability-inclusion-toolkit/the-equitable-ai-playbook/.

[366] NIST. “Supply Chain - Glossary | CSRC.” Accessed December 19, 2022. https://csrc.nist.gov/glossary/term/supply_chain.

[367] National Center for Educational Statistics. “Integrated Postsecondary Educational Data System Completions Survey Data.” Accessed 2021. https://ncsesdata.nsf.gov/explorer/surveys?superTopic=Students%20and%20Education&survey=IPEDS_C&page=1.

[368] Zweben, Stuart, and Betsy Bizot. “2020 Taulbee Survey.” Bachelor’s and Doctoral Degree Production Growth Continues but New Student Enrollment Shows Declines. Accessed December 20, 2021. https://cra.org/wp-content/uploads/2021/05/2020-CRA-Taulbee-Survey.pdf.

[369] Zwetsloot, Remco, Roxanne Heston, and Zachary Arnold. “Strengthening the U.S. AI Workforce: A Policy and Research Agenda.” September 2019. https://cset.georgetown.edu/wp-content/uploads/CSET_US_AI_Workforce.pdf.

[370] Federal Trade Commission. “Non-Compete Clause Rulemaking.” Accessed July 19, 2023. https://www.ftc.gov/legal-library/browse/federal-register-notices/non-compete-clause-rulemaking.

[371] Burke, Amy, Abigail Okrent, and Katherine Hale. “The State of U.S. Science and Engineering 2022 | NSF - National Science Foundation.” Accessed January 6, 2023. https://ncses.nsf.gov/pubs/nsb20221/u-s-and-global-stem-education-and-labor-force.

[372] National Institute of Standards and Technology. “AI Risk Management Framework: Second Draft - August 18, 2022.” August 2022. https://www.nist.gov/system/files/documents/2022/08/18/AI_RMF_2nd_draft.pdf.

[373] United States Citizenship and Immigration Services. “Optional Practical Training (OPT) For F-1 Students.” Accessed August 10, 2022. https://www.uscis.gov/working-in-the-united-states/students-and-exchange-visitors/optional-practical-training-opt-for-f-1-students.

[374] Zwetsloot, Remco, James Dunham, Zachary Arnold, and Tina Huang. “Keeping Top AI Talent in the United States.” 2019. https://cset.georgetown.edu/wp-content/uploads/Keeping-Top-AI-Talent-in-the-United-States.pdf.

[375] Gehlhaus, Diana, and Ilya Rahkovsky. “U.S. AI Workforce: Labor Market Dynamics.” CSET Issue Brief, Center for Security and Emerging Technology, 2021.

[376] Abigail Okrent and Amy Burke. “The STEM Labor Force of Today: Scientists, Engineers, and Skilled Technical Workers | NSF - National Science Foundation.” Accessed January 6, 2023. https://ncses.nsf.gov/pubs/nsb20212/participation-of-demographic-groups-in-stem.

[377] Khan, Beethika, Carol Robbins, and Abigail Okrent. “The State of U.S. Science and Engineering 2020 | NSF - National Science Foundation.” Accessed December 16, 2021. https://ncses.nsf.gov/pubs/nsb20201/u-s-s-e-workforce.

[378] U.S. Census Bureau. “U.S. Census Bureau QuickFacts: United States.” Accessed December 21, 2021. https://www.census.gov/quickfacts/fact/table/US/PST045219.

[379] NCSES. “Women, Minorities, and Persons with Disabilities in Science and Engineering: 2021 | NSF - National Science Foundation.” Accessed December 20, 2022. https://ncses.nsf.gov/pubs/nsf21321/report/persons-with-disability.

[380] Crawford, Kate, and Ryan Calo. “There Is a Blind Spot in AI Research.” *Nature* 538 (2016): 311–13. https://doi.org/10.1038/538311a.

[381] Kuhlman, Caitlin, Latifa Jackson, and Rumi Chunara. “No Computation Without Representation: Avoiding Data and Algorithm Biases Through Diversity.” February 26, 2020. http://arxiv.org/pdf/2002.11836v1.

[382] Bogost, Ian. “The Problem with Diversity in Computing.” *The Atlantic*, June 25, 2019. Accessed December 16, 2021. https://www.theatlantic.com/technology/archive/2019/06/tech-computers-are-bigger-problem-diversity/592456/.

[383] Engler, Alex C. “How Open-Source Software Shapes AI Policy.” The Brookings Institution; Center for Technology Innovation, August 10, 2021. https://www.brookings.edu/research/how-open-source-software-shapes-ai-policy/.

[384] Jia, Yangqing. “Caffe | Deep Learning Framework.” Accessed August 12, 2022. https://caffe.berkeleyvision.org/.

[385] Liu, Mark. “Taiwan and the Foundry Model.” *Nature Electronics* 4, no. 5 (2021): 318–20. https://doi.org/10.1038/s41928-021-00576-y.

[386] Varas, Antonio, Raj Varadarajan, Jimmy Goodrich, and Falan Yinug. “Strengthening the Global Semiconductor Supply Chain in an Uncertain Era.” Boston Consulting Group and Semiconductor Industry Association, April 2021. https://www.semiconductors.org/wp-content/uploads/2021/05/BCG-x-SIA-Strengthening-the-Global-Semiconductor-Value-Chain-April-2021_1.pdf.

[387] Platzer, Michaela D., John F. Sargent, JR., and Karen M. Sutter. "Semiconductors: U.S. Industry, Global Competition, and Federal Policy." Congressional Research Service, October 26, 2020. https://crsreports.congress.gov/product/pdf/R/R46581.

[388] Khan, Saif M., and Alexander Mann. "AI Chips: What They Are and Why They Matter: An AI Chips Reference." April 2020. https://cset.georgetown.edu/wp-content/uploads/AI-Chips%E2%80%94What-They-Are-and-Why-They-Matter.pdf.

[389] The White House. "Fact Sheet: CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China." Accessed December 19, 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/.

[390] Lohn, Andrew J., and Micah Musser. "AI and Compute: How Much Longer Can Computing Power Drive Artificial Intelligence Progress?," CSET, January 2022. https://cset.georgetown.edu/wp-content/uploads/AI-and-Compute-How-Much-Longer-Can-Computing-Power-Drive-Artificial-Intelligence-Progress.pdf.

[391] Ahmed, Nur, and Muntasir Wahed. "The De-Democratization of AI: Deep Learning and the Compute Divide in Artificial Intelligence Research." Accessed December 16, 2021. https://arxiv.org/ftp/arxiv/papers/2010/2010.15581.pdf.

[392] Osoba, Osonde A., and William Welser, IV. "The Risks of Artificial Intelligence to Security and the Future of Work." RAND, 2017. https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE237/RAND_PE237.pdf.

[393] Ho, Daniel E., Jennifer King, Russell C. Wald, and Christopher Wan. "Building a National AI Research Resource:: A Blueprint for the National Research Cloud." White Paper, Stanford University; Stanford Law School; Stanford University Human-Centered Artificial Intelligence, 2021. https://hai.stanford.edu/sites/default/files/2021-10/HAI_NRCR_2021_0.pdf.

[394] National Artificial Intelligence Initiative. "The National Artificial Intelligence Research Resource Task Force (NAIRRTF)." Accessed December 22, 2021. https://www.ai.gov/nairrtf/.

[395] Calo, Ryan. "Artificial Intelligence Policy: A Primer and Roadmap." *SSRN Electronic Journal*, 2017. Accessed December 16, 2021. https://doi.org/10.2139/ssrn.3015350. https://doi.org/10.2139/ssrn.3015350.

[396] Markets and Markets. "Artificial Intelligence Market: Global Forecast to 2026." Markets and Markets, 2021.

[397] Illinois Compiled Statutes. 740 ILCS 14/ Biometric Information Privacy Act. Illinois General Assembly. Accessed December 22, 2021. https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

[398] "Next-Wave-Artificial-Intelligence_-Robust-Explainable-Adaptable-Ethical-and-Accountable.."

[399] ABA Antitrust Law Section, Big Data Task Force. "Artificial Intelligence & Machine Learning: Emerging Legal and Self-Regulatory Considerations: Part Two: Competition Implications of Big Data and Artificial Intelligence/Machine Learning." American Bar Association, February 2021. https://www.americanbar.org/content/dam/aba/administrative/antitrust_law/comments/feb-21/aba-big-data-task-force-white-paper-part-two-final-215.pdf.

[400] Crémer, Jacques, Yves-Alexandre de Montjoye, and Heike Schweitzer. "Competition Policy for the Digital Era." European Commission, Luxembourg, 2019. https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf.

[401] Autorité de la Concurrence, and Bundeskartellamt. "Algorithms and Competition." Autorité de la Concurrence; Bundeskartellamt, November 2019. https://www.autoritedelaconcurrence.fr/sites/default/files/algorithms-and-competition.pdf.

[402] Organisation for Economic Co-operation and Development. "Algorithms and Collusion: Competition Policy in the Digital Age." 2017. http://www.oecd.org/competition/algorithms-collusion-competition-policy-in-the-digital-age.htm.

[403] Department of Justice. "U.S. V. Daniel William Aston and Trod Limited." Accessed May 23, 2023. https://www.justice.gov/atr/case/us-v-daniel-william-aston-and-trod-limited.

[404] "Algorithms and Collusion: Competition Policy in the Digital Age." Accessed May 1, 2023. https://www.oecd.org/daf/competition/Algorithms-and-colllusion-competition-policy-in-the-digital-age.pdf.

[405] "Hub-and-Spoke Arrangements – Note by the United States." https://www.justice.gov/atr/page/file/1313546/download.

[406] Nanalyze. "Machine Learning for Stock Trading Strategies." Accessed December 9, 2021. https://www.nanalyze.com/2020/05/machine-learning-for-stock-trading-strategies/.

[407] Cheatham, Benjamin, Kia Javanmardian, and Hamid Samandari. "Confronting the Risks of Artificial Intelligence." McKinsey, April 2019. https://www.cognitivescale.com/wp-content/uploads/2019/06/Confronting_AI_risks_-_McKinsey.pdf.

[408] AI Now Institute. "The AI Now Report: The Social and Economic Implications of Artificial Intelligence Technologies in the Near-Term." A summary of the AI Now public symposium, hosted by the White House and, AI Now Institute, September 22, 2016. https://ainowinstitute.org/AI_Now_2016_Report.pdf.

[409] Buolamwini, Joy, and Timnit Gebru. "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification." *Conference on fairness, accountability and transparency*, 2018, 77–91. https://proceedings.mlr.press/v81/buolamwini18a.html.

[410] Eubanks, Virginia. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York, NY, USA: St. Martin's Press, 2018.

[411] Noble, Safiya Umoja. *Algorithms of Oppression*. New York, NY, USA: New York University Press, 2018.

[412] Su Lin Blodgett, Solon Barocas, Hal Daumé III, and Hanna Wallach. "Language (Technology) Is Power: A Critical Survey of "Bias" in NLP." *arXiv preprint*, 2020. https://arxiv.org/abs/2005.14050.

[413] West, Sarah Myers, Meredith Whittaker, and Kate Crawford. "Discriminating Systems: Gender, Race, and Power in AI." April 2019. https://ainowinstitute.org/discriminatingsystems.pdf.

[414] Whittaker, Meredith, Meryl Alper, Cynthia L. Bennett, Sara Hendren, Liz Kaziunas, Mara Mills, Meredith Ringel Morris, Joy Rankin, Emily Rogers, Marcel Salas, Sarah

Myers West. “Disability, Bias, and AI.” AI Now Institute, November 2019. https://ainowinstitute.org/disabilitybiasai-2019.pdf.

[415] Dataversity. “Is Your AI Model Leaking Intellectual Property? - Dataversity.” Accessed August 18, 2022. https://www.dataversity.net/is-your-ai-model-leaking-intellectual-property/.

[416] Rocher, Luc, Julien M. Hendrickx, and Yves-Alexandre de Montjoye. “Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models.” *Nature Communications* 10, no. 1 (2019): 3069. https://doi.org/10.1038/s41467-019-10933-3. https://www.nature.com/articles/s41467-019-10933-3/.

[417] National Artificial Intelligence Initiative. “Advancing Trustworthy AI.” Accessed May 9, 2022. https://www.ai.gov/strategic-pillars/advancing-trustworthy-ai/.

[418] National Institute of Standards and Technology. “AI Risk Management Framework.” Accessed December 30, 2022. https://www.nist.gov/itl/ai-risk-management-framework.

[419] National Institute of Standards and Technology. “AI RMF Playbook.” Accessed January 5, 2023. https://pages.nist.gov/AIRMF/.

[420] Marr, Bernard. “The Brilliant Ways UPS Uses Artificial Intelligence, Machine Learning and Big Data.” Accessed December 10, 2021. https://www.forbes.com/sites/bernardmarr/2018/06/15/the-brilliant-ways-ups-uses-artificial-intelligence-machine-learning-and-big-data/?sh=2b02b8c45e6d.

[421] Goodfellow, Ian J., Jonathon Shlens, and Christian Szegedy. “Explaining and Harnessing Adversarial Examples.” Google Inc, December 19, 2014. https://arxiv.org/pdf/1412.6572.

[422] Eykholt, Kevin, Ivan Evtimov, Earlence Fernandes, Bo Li, Amir Rahmati, Chaowei Xiao, Atul Prakash, Tadayoshi Kohno, and Dawn Song. “Robust Physical-World Attacks on Deep Learning Models.” July 27, 2017. https://arxiv.org/pdf/1707.08945.

[423] Konaev, Margarita. “Thoughts on Russia’s AI Strategy.” Accessed December 10, 2021. https://cset.georgetown.edu/article/thoughts-on-russias-ai-strategy/.

[424] Reuters Media. “China Has Won AI Battle with U.S., Pentagon's Ex-Software Chief Says.” Accessed December 10, 2021. https://www.reuters.com/technology/united-states-has-lost-ai-battle-china-pentagons-ex-software-chief-says-2021-10-11/.

[425] Department of Commerce Bureau of Industry and Security. “Commerce Implements New Export Controls on Advanced Computing and Semiconductor Manufacturing Items to the People’s Republic of China (PRC).” Department of Commerce Bureau of Industry and Security, October 7, 2022. https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3158-2022-10-07-bis-press-release-advanced-computing-and-semiconductor-manufacturing-controls-final/file.

[426] “Executive Order on Maintaining American Leadership in Artificial Intelligence: EO 13859.” In, *Federal Register*, 3967–72.

[427] U.S. Government Accountability Office. “Military Acquisitions: DOD Is Taking Steps to Address Challenges Faced by Certain Companies.” GAO-17-644, U.S. Government Accountability Office (GAO), July 2017. https://www.gao.gov/assets/gao-17-644.pdf.

[428] Wakabayashi, Daisuke, and Scott Shane. “Google Will Not Renew Pentagon Contract That Upset Employees.” Accessed December 10, 2021. https://www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html.

[429] GSA. “Recruiting AI Talent | GSA - IT Modernization Centers of Excellence.” Accessed December 30, 2022. https://coe.gsa.gov/coe/ai-guide-for-government/recruiting-ai-talent/index.html.

[430] The Center for Digital Talent. “List of Department of Defense Hiring Authorities and Mechanisms — A Playbook for the Department of Defense.” Accessed December 30, 2022. https://www.techtalentfordefense.org/resources/list-of-dod-hiring-authorities-and-mechanisms.

[431] Shane, Scott, Cade Metz, and Daisuke Wakabayashi. “How a Pentagon Contract Became an Identity Crisis for Google.” Accessed June 2, 2022. https://www.nytimes.com/2018/05/30/technology/google-project-maven-pentagon.html.

[432] Benjamin, Ruha. “Assessing Risk, Automating Racism.” *Science (New York, N.Y.)* 366, no. 6464 (2019): 421–22. Accessed December 19, 2021. https://doi.org/10.1126/science.aaz3873.

[433] Obermeyer, Ziad, Brian Powers, Christine Vogel, and Sendhil Mullainathan. “Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations.” *Science (New York, N.Y.)* 366, no. 6464 (2019): 447–53. Accessed December 13, 2021. https://doi.org/10.1126/science.aax2342. https://www.science.org/doi/pdf/10.1126/science.aax2342.

[434] Austermuhle, Martin. “D.C. Attorney General Introduces Bill to Ban ‘Algorithmic Discrimination’ – DCist.” Accessed December 10, 2021. https://dcist.com/story/21/12/09/dc-attorney-general-introduces-bill-to-ban-algorithmic-discrimination/.

[435] Mac, Ryan. “Facebook Apologizes After A.I. Puts ‘Primates’ Label on Video of Black Men.” Accessed December 10, 2021. https://www.nytimes.com/2021/09/03/technology/facebook-ai-race-primates.html.

[436] National Army Museum. “'You Americans Are Sooo Different.': Online Collection | National Army Museum, London.” Accessed December 10, 2021. https://collection.nam.ac.uk/detail.php?acc=2002-02-916-1.

[437] National Academies of Sciences, Engineering, and Medicine. *A Decadal Survey of the Social and Behavioral Sciences: A Research Agenda for Advancing Intelligence Analysis*. Washington, D.C.: National Academies Press, 2019. Accessed December 4, 2021. https://doi.org/10.17226/25335. https://nap.nationalacademies.org/catalog/25335/a-decadal-survey-of-the-social-and-behavioral-sciences-a.

[438] Theohary, Catherine A. “Defense Primer: Information Operations.” IF10771, Congressional Research Service, December 1, 2021. https://crsreports.congress.gov/product/pdf/IF/IF10771.

[439] Petratos, Pythagoras N. “Misinformation, Disinformation, and Fake News: Cyber Risks to Business.” *Business Horizons* 64, no. 6 (2021): 763–74. https://doi.org/10.1016/j.bushor.2021.07.012.

[440] Klinger, Joel, Juan Mateos-Garcia, and Konstantinos Stathoulopoulos. “A Narrowing of AI Research?,” September 22, 2020. https://arxiv.org/pdf/2009.10385.pdf.

[441] Aghion, Phillippe, Benjamin F. Jones, and Charles I. Jones. *Artificial Intelligence and Economic Growth: The Economics of Artificial Intelligence*. With the assistance of Ajay Agrawal, Joshua Gans, and Avi Goldfarb. Cambridge, MA: University of Chicago Press, 2019. Chapter 9. Accessed December 19, 2021.

[442] Gray, Mary L., and Siddharth Suri. *Ghost Work: How to Stop Silicon Valley from Building a New Global Underclass*. Boston: Houghton Mifflin Harcourt, 2019.

[443] Davenport, Thomas H., and Nitin Mittal. “How Generative AI Is Changing Creative Work.” Accessed December 28, 2022. https://hbr.org/2022/11/how-generative-ai-is-changing-creative-work.

[444] “The Impact of Artificial Intelligence on the Future of Workforces in the European Union and the United States of America: An Economic Study Prepared in Response to the US-EU Trade and Technology Council Inaugural Joint Statement.” 2022. https://www.whitehouse.gov/wp-content/uploads/2022/12/TTC-EC-CEA-AI-Report-12052022-1.pdf.

[445] National Academies of Sciences, Engineering, and Medicine. “Automation and the US Workforce: An Update | National Academies.” National Academies of Sciences, Engineering, and Medicine (NASEM), 2017. https://www.nationalacademies.org/our-work/automation-and-the-us-workforce-an-update.

[446] OECD. “OECD Legal Instruments: Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.” Accessed April 21, 2023. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188.

[447] Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York, NY, USA: PublicAffairs, 2019. Accessed December 4, 2021.

[448] Hoffman, Wyatt. “AI and the Future of Cyber Competition.” CSET, January 2021. https://cset.georgetown.edu/wp-content/uploads/CSET-AI-and-the-Future-of-Cyber-Competition-4.pdf.

[449] National Academies of Sciences, Engineering, and Medicine. “Implications of Artificial Intelligence for Cybersecurity: Proceedings of a Workshop.” National Academies of Sciences, Engineering, and Medicine (U.S.), Washington DC, 2019. https://nap.nationalacademies.org/read/25488.

[450] Farid, Hany. “Watermarking ChatGPT, DALL-E and Other Generative AIs Could Help Protect Against Fraud and Misinformation.” Accessed May 1, 2023. https://theconversation.com/watermarking-chatgpt-dall-e-and-other-generative-ais-could-help-protect-against-fraud-and-misinformation-202293.

[451] Metz, Cade. “What Makes Chatbots ‘Hallucinate’ or Say the Wrong Thing?” *The New York Times*, March 29, 2023. Accessed May 1, 2023. https://www.nytimes.com/2023/03/29/technology/ai-chatbots-hallucinations.html.

Appendix A. Abbreviations

AHCRQ	Agency for Healthcare Research and Quality
CFPB	Consumer Financial Protection Bureau
CFTC	Commodity Futures Trading Commission
CISO Council	Chief Information Security Officer Council
CPSC	Consumer Product Safety Commission
DHS	Department of Homeland Security
DOC	Department of Commerce
DOC-BIS	Bureau of Industry and Security
DOC-NIST	National Institute of Standards and Technology
DOC-NOAA	National Oceanic and Atmospheric Administration
DOC-USPTO	U.S. Patent and Trademark Office
DoD-DARPA	Defense Advanced Research Projects Agency
DoD	Department of Defense
DOE	Department of Energy
DOI	Department of the Interior
DOJ-ATF	Bureau of Alcohol, Tobacco, and Firearms
DOL	Department of Labor
DOL-ODEP	Office of Disability Employment Policy
DOL-OFCCP	Office of Federal Contract Compliance Programs
DOT	Department of Transportation
ED	Department of Education
EEOC	Equal Employment Opportunity Commission
EOP	Executive Office of the President
EOP-CEA	Council of Economic Advisors
EOP-NEC	National Economic Council
EOP-NSC	National Security Council
EOP-NSTC	National Science and Technology Council
EOP-OMB	Office of Management and Budget
EOP-OMB-OIRA	Office of Information and Regulatory Affairs
EOP-OSTP	Office of Science and Technology Policy
EPA	Environmental Protection Agency
FCC	Federal Communication Commission
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FRB	Federal Reserve Board
FTC	Federal Trade Commission
GSA	General Services Administration
HHS	Department of Health and Human Services
HHS-CMS	Centers for Medicare and Medicaid Services
HHS-FDA	Food and Drug Administration
HHS-NIH	National Institutes of Health
HHS-OCR	HHS Office for Civil Rights
IC	Intelligence Community
NASA	National Aeronautics and Space Administration
NSF	National Science Foundation

ODNI-IARPA	Intelligence Advanced Research Projects Activity
OPM	Office of Personnel Management
SEC	Securities and Exchange Commission
State Dept.	State Department
Treasury-OCC	Office of the Comptroller of the Currency
Treasury-OFAC	Office of Foreign Assets Control
Treasury-OIS	Office of Intelligence Support
Treasury	Treasury Department
USAID	U.S. Agency for International Development
USDA	U.S. Department of Agriculture
USDA-NIFA	National Institute of Food and Agriculture
VA	U.S. Department of Veterans Affairs

Appendix B. ACA Specifications for This Study

STUDY TO ADVANCE ARTIFICIAL INTELLIGENCE.—

(1) IN GENERAL.—

(A) STUDY REQUIRED.—Not later than 1 year after the date of enactment of this Act, the Secretary of Commerce and the Federal Trade Commission shall complete a study on the state of the artificial intelligence industry and the impact of such industry on the United States economy.

(B) REQUIREMENTS FOR STUDY.—In conducting the study, the Secretary and the Commission shall—

(i) develop and conduct a survey of the artificial intelligence industry through outreach to participating entities as appropriate to—

(I) establish a list of industry sectors that implement and promote the use of artificial intelligence;

(II) establish a list of public-private partnerships focused on promoting the adoption and use of artificial intelligence, as well as industry-based bodies, including international bodies, which have developed, or are developing, mandatory or voluntary standards for artificial intelligence;

(III) the status of such industry-based mandatory or voluntary standards; and

(IV) provide a description of the ways entities or industry sectors implement and promote the use of artificial intelligence;

(ii) develop a comprehensive list of Federal agencies with jurisdiction over the entities and industry sectors identified under clause (i);

(iii) identify which Federal agency or agencies listed under clause (ii) each entity or industry sector interacts with;

(iv) identify all interagency activities that are taking place among the Federal agencies listed under clause (ii), such as working groups or other coordinated efforts;

(v) develop a brief description of the jurisdiction and expertise of the Federal agencies listed under clause (ii) with regard to such entities and industry sectors;

(vi) identify all regulations, guidelines, mandatory standards, voluntary standards, and other policies implemented by each of the Federal agencies identified under clause (ii), as well as all guidelines, mandatory standards, voluntary standards, and other policies implemented by industry-based bodies;

(vii) identify Federal Government resources that exist for consumers and small businesses to evaluate the use of artificial intelligence; and

(viii) consult with the Office of Science and Technology Policy and interagency efforts on artificial intelligence to minimize duplication of activities among the Federal agencies identified under clause (ii).

(2) MARKETPLACE AND SUPPLY CHAIN SURVEY.—The Secretary and Commission shall conduct a survey of the marketplace and supply chain of artificial intelligence to—

(A) identify and assess risks posed to such marketplace and supply chain;

(B) review the ability of foreign governments or third parties to exploit the supply chain in a manner that raises risks to the economic and national security of the United States; and

(C) identify emerging risks and long-term trends in such marketplace and supply chain.

(3) REPORT TO CONGRESS.—Not later than 6 months after the completion of the study required under paragraph (1), the Secretary and the Commission shall submit to the Committee on Energy and Commerce and the Committee on Science, Space, and Technology of the House of Representatives, and the Committee on Commerce, Science, and Transportation of the Senate, and make publicly available on their respective websites, a report that contains—

(A) the results of the study conducted pursuant to paragraph (1) and the survey conducted pursuant to paragraph (2); and

(B) recommendations to—

(i) grow the United States economy through the secure advancement of artificial intelligence;

(ii) develop a national strategy to advance the United States business sectors' position in the world on the adoption of artificial intelligence;

(iii) develop strategies to mitigate current and emerging risks to the marketplace and supply chain of artificial intelligence; and

(iv) develop legislation that—

(I) advances the expeditious adoption of artificial intelligence applications in interstate commerce that takes into account findings from available Federal advisory committees that produce recommendations on artificial intelligence to the extent possible; and

(II) addresses societal priorities related to the expeditious adoption of artificial intelligence applications in interstate commerce, including but not limited to maintaining ethics, reducing bias, and protecting privacy and security.

Appendix C. North American Industrial Classification Systems (NAICS) Sectors

NAICS Code	Sector	Description
11	Agriculture, Forestry, Fishing and Hunting	Activities of this sector are growing crops, raising animals, harvesting timber, and harvesting fish and other animals from farms, ranches, or the animals' natural habitats.
21	Mining, Quarrying, and Oil and Gas Extraction	Activities of this sector are extracting naturally occurring mineral solids, such as coal and ore; liquid minerals, such as crude petroleum; and gases, such as natural gas; and beneficiating (e.g., crushing, screening, washing, and flotation) and other preparation at the mine site, or as part of mining activity.
22	Utilities	Activities of this sector are generating, transmitting, and/or distributing electricity, gas, steam, and water and removing sewage through a permanent infrastructure of lines, mains, and pipe.
23	Construction	Activities of this sector are erecting buildings and other structures (including additions); heavy construction other than buildings; and alterations, reconstruction, installation, and maintenance and repairs.
31–33	Manufacturing	Activities of this sector are the mechanical, physical, or chemical transformation of materials, substances, or components into new products.
42	Wholesale Trade	Activities of this sector are selling or arranging for the purchase or sale of goods for resale; capital or durable non-consumer goods; and raw and intermediate materials and supplies used in production, and providing services incidental to the sale of the merchandise.
44–45	Retail Trade	Activities of this sector are retailing merchandise generally in small quantities to the general public and providing services incidental to the sale of the merchandise.
48–49	Transportation and Warehousing	Activities of this sector are providing transportation of passengers and cargo, warehousing and storing goods, scenic and sightseeing transportation, and supporting these activities.
51	Information	Activities of this sector are distributing information and cultural products, providing the means to transmit or distribute these products as data or communications, and processing data.
52	Finance and Insurance	Activities of this sector involve the creation, liquidation, or change in ownership of financial assets (financial transactions) and/or facilitating financial transactions.
53	Real Estate and Rental and Leasing	Activities of this sector are renting, leasing, or otherwise allowing the use of tangible or intangible assets (except copyrighted works), and providing related services.
54	Professional, Scientific, and Technical Services	Activities of this sector are performing professional, scientific, and technical services for the operations of other organizations.
55	Management of Companies and Enterprises	Activities of this sector are the holding of securities of companies and enterprises, for the purpose of owning controlling interest or influencing their management decisions, or administering, overseeing, and managing other establishments of the same company or enterprise and normally undertaking the strategic or organizational planning and decision-making role of the company or enterprise.
56	Administrative and Support and Waste	Activities of this sector are performing routine support activities for the day-to-day operations of other organizations.

NAICS Code	Sector	Description
	Management and Remediation Services	
61	Educational Services	Activities of this sector are providing instruction and training in a wide variety of subjects.
62	Health Care and Social Assistance	Activities of this sector are providing health care and social assistance for individuals.
71	Arts, Entertainment, and Recreation	Activities of this sector are operating or providing services to meet varied cultural, entertainment, and recreational interests of their patrons.
72	Accommodation and Food Services	Activities of this sector are providing customers with lodging and/or preparing meals, snacks, and beverages for immediate consumption.
81	Other Services (except Public Administration)	Activities of this sector are providing services not elsewhere specified, including repairs, religious activities, grantmaking, advocacy, laundry, personal care, death care, and other personal services.
92	Public Administration	Activities of this sector are administration, management, and oversight of public programs by Federal, State, and local governments.

Internet of Things

Chapter Contents

List of Tables

List of Figures

2. Internet of Things

Summary

In the Consolidated Appropriations Act of 2021 (Public Law 116-260, Division FF, Title XV, §1501), Congress tasked the National Institute of Standards and Technology (NIST) to prepare a series of reports on critical and emerging technologies and their impact on the U.S. economy. This chapter focuses on the Internet of Things (IoT) and IoT in manufacturing as one of its sectors, and addresses the following topics:

- industry sectors that develop and promote IoT,
- public-private partnerships (PPPs) and interagency activities related to IoT,
- industry bodies that develop IoT standards,
- Federal agencies with IoT jurisdiction,
- laws and regulations developed by the Federal Government,
- Federal resources for consumers,
- market trends for IoT in manufacturing,
- risks to supply chains and marketplace,
- IoT-related risks to the national security, including economic security,[37] of the United States, and
- recommendations for the safe and effective use of IoT.

Recommendations

IoT offers potentially large benefits to society, such as higher productivity, reduced costs, and improved customer experience. However, the rapid expansion of these technologies also poses significant risks to cybersecurity, privacy and personal freedom, and national security, including economic security. The Federal Government can play an important role in promoting the development and uptake of IoT, while mitigating these serious risks. Indeed, the Federal Government only acquires IoT devices that comply with NIST guidelines for IoT. Based on the results of the study, the following actions are proposed:

Recommendation 1: The Federal Government should encourage manufacturers and service providers to anticipate and address potential risks to safety and rights of users during early stages of product development, rather than as add-ons or modifications to a near-final product or as post-market fixes.

[37] The Consolidated Appropriations Act of 2021 refers to "economic and national security," and economic security is understood to be part of national security for the purposes of authorities such as the Consolidated Appropriations Act of 2021 and Section 232 of the Trade Expansion Act of 1962 (Public Law 87-794).

Recommendation 2: The Federal Government should continue to play a role in educating consumers and businesses about the risks and benefits of IoT; how to safely use IoT devices; and what choices customers have in accepting or rejecting IoT technologies and services.

Recommendation 3: The Federal Government should promote the development of technologies and other innovations that would enable customers to easily and effectively control collection, use, access, transfer, and deletion of their data.

Recommendation 4: The Federal Government should continue to develop and disseminate flexible frameworks and guidance, so that manufacturers can implement protections for safety and rights that are commensurate with risks posed by their products or services.

Recommendation 5: The Federal Government should continue to encourage the transition to smart manufacturing and other IoT systems in areas that have no ownership, are too risky for commercial investment, have been resistant to solutions, or require coordination across multiple stakeholders.

Recommendation 6: The Federal Government should continue to engage with industry consortia, non-profit organizations, and academic institutions to obtain input on its standards development activities and promote awareness among stakeholders.

Recommendation 7: The Federal Government should continue to advance work to develop international standards on IoT.

Recommendation 8: The Federal Government should support IoT research and development projects, innovation hubs, centers of excellence, and testing facilities to ensure that the United States maintains intellectual leadership in this space.

Recommendation 9: The Federal Government should analyze potential impacts of incentives, such as tax credits, to help small- and medium-sized manufacturers invest in secure but potentially costly IoT technologies.

Recommendation 10: The Federal Government should collaborate with industry to define required skills and sponsor programs to help businesses train and retrain workers.

2.1. Overview

2.1.1. Definition of the "Internet of Things"

The internet of things (IoT) is a technology that adds a device to an inert object (for example: vehicles, plant electronic systems, roofs, lighting, etc.) that can measure environmental parameters, generate associated data and transmit them through a communications network. As noted by NIST and other sources, one of the challenges of IoT is the lack of a consistent and agreed-upon definition. NIST highlights two "essential concepts" of IoT: "the capacity to support … networked relationships between components" and "the presence of sensors and/or actuators that allow the components to interact with the physical world." [1]. For purposes of this chapter, the IoT is "the network of physical objects – 'Things' – that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet" [2]. This is just one of many definitions of the term: a recent study by the National Institute of Standards and

Technology (NIST) listed 30 options [3]. Various definitions are largely in agreement about several key properties of IoT, which include identifiable Things; connection of these Things to the internet and each other; ubiquity of Things; sensing and interoperable communication capabilities; embedded intelligence; self-configurability; and programmability [3].

In the past 10 years, IoT has penetrated all market sectors, from healthcare to agriculture to energy. IoT in manufacturing, also referred to in the literature as *Industrial IoT (IIoT), Industry 4.0*, *smart factories*, and *smart manufacturing*, is an emerging form of production that integrates manufacturing assets with sensors, computing platforms, communication technology, simulation, data intensive modeling, and predictive engineering. While the concept of IoT in manufacturing has been increasingly embraced by businesses, this market sector also lacks an agreed-upon definition of the term. One of the frequently cited descriptions was suggested by NIST as a "fully integrated, collaborative manufacturing system that responds in real time to meet changing demands and conditions in the factory, in the supply networks, and in customer needs" [4].

2.1.2. IoT and IoT in Manufacturing

IoT in manufacturing is one of the market sectors in the sprawling landscape of devices, systems, and applications under the broad umbrella of IoT. To the extent possible, this chapter highlights the regulatory landscape, industry and Federal activities, partnerships, risks, and market conditions in manufacturing and industrial IoT. However, for some of these topics it is impossible to isolate manufacturing from other market sectors, due to the lack of consistent definitions, the complexity of the manufacturing industry, and the overlap in technology and risks across applications. All available information specific to manufacturing is clearly identified in the chapter.

2.1.3. Brief History of IoT

The concept of IoT emerged in the 1970s with a shift toward smaller and eventually personal computers [5]. In the 1980s, the Chief Technologist at Xerox coined the phrase "ubiquitous computing," which anticipated the future where these types of devices are widely present and available to everyone. The first true IoT device—a Coke machine that enabled users to remotely track whether it was stacked with drinks—was invented by a graduate student in Carnegie Mellon University David Nichols in the early 1980s [6]. The term "internet of things" was proposed a decade later by Massachusetts Institute of Technology (MIT) scientist Kevin Ashton while he was working on the idea of using radio-frequency identification to tag and track objects automatically [7].

Many important developments in IoT followed in quick succession. In 2000, the South Korean firm LG tried to market the first internet-connected refrigerator, but the product was too expensive for the added functionality and ultimately failed. Other early devices included a mechanical rabbit and a webcam to monitor the amount of coffee in a coffee pot, with IoT increasingly appearing in books and popular media [7; 8]. In a testament to its growing importance, the United Nations published a report on IoT in 2005 and the U.S. National Intelligence Council announced IoT as one of the six potentially disruptive technologies in 2008 [9]. Cisco's Internet Business Solutions Group has declared that the number of devices connected to the internet surpassed the number of people between 2008 and 2009 [10]—some scholars consider this moment the birthday of IoT [7].

The number and range of devices rapidly proliferated after 2010 (Figure 1), and IoT has made its way to virtually every industry. Thermostats and home lighting using sensors to probe the surrounding environment entered the market in 2013–2014, and Dublin, Ireland, became the first "smart city" by installing sensors to monitor carbon, flood water, and noise levels. In 2017, the U.S. Army established an alliance to advance the use of IoT in military operations, and in 2018, IoT became more common in healthcare with improved quality of wearable monitoring devices. The number of Things continues to expand rapidly, with some experts estimating that 75 billion devices will be connected to the internet by 2025, nearly 10 times the projected world population [11; 12].

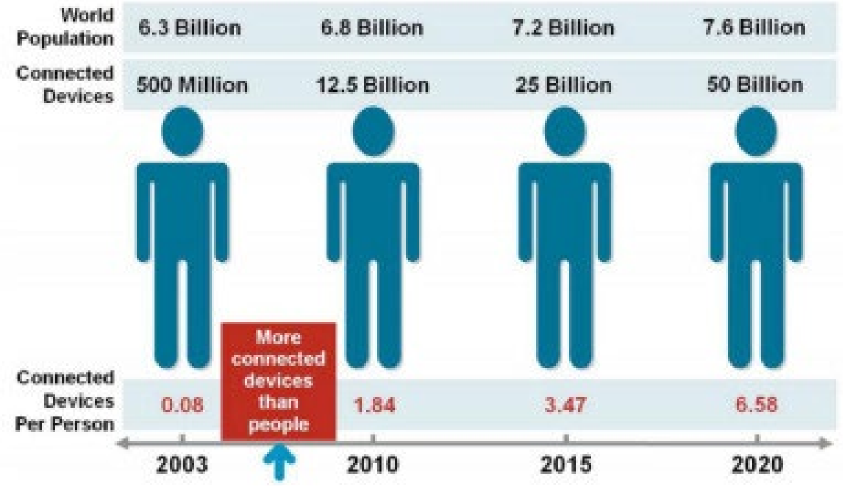


Figure 1. Trends in the Number of People and Devices over Time

2.1.4. Organization of the Chapter

In addition to the main body that describes the landscape of IoT/IoT in manufacturing and offers recommendations for the secure development and use of these devices, the chapter contains several appendices. Appendix D presents a list of common abbreviations used in this chapter. Appendix E presents a World of IoT map showing nine sectors of IoT technology and associated applications. Appendix F includes additional industry consortia and associations, standards development organizations, and cybersecurity organizations that were too numerous to include in the main body of the chapter, where a few examples are highlighted. Appendix G describes design considerations for mandatory or voluntary standards.

2.2. Background

2.2.1. Objectives and Scope

In the Consolidated Appropriations Act of 2021 (Public Law 116-260, Division FF, Title XV, §1501), Congress tasked the National Institute of Standards and Technology (NIST) to prepare a series of reports on critical and emerging technologies and their impact on the U.S. economy. This chapter focuses on the Internet of Things (IoT) and IoT in manufacturing as one of its sectors, and addresses the following topics:

- Industry sectors that develop and promote IoT
- Public-private partnerships (PPPs) and interagency activities related to IoT
- Industry bodies that develop IoT standards
- Federal agencies with IoT jurisdiction
- Laws and regulations developed by the Federal Government
- Federal resources for consumers
- Market trends for IoT in manufacturing
- Risks to supply chains, marketplace, U.S. national security (including economic security)
- Recommendations for the safe and effective use of IoT

As noted by NIST and other sources, one of the challenges of IoT is the lack of a consistent and agreed-upon definition. NIST highlights two "essential concepts" of IoT: "the capacity to support … networked relationships between components" and "the presence of sensors and/or actuators that allow the components to interact with the physical world." [1]. For purposes of this report, IoT is defined as "the network of physical objects – 'Things' – that are embedded with sensors, actuators, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet" [2]. IoT in manufacturing, also called "Industrial IoT (IIoT), Industry 4.0, smart factories, and smart manufacturing," is an emerging form of production that integrates manufacturing assets with sensors, computing platforms, communication technology, networks, simulation, data intensive modeling, and predictive engineering. It is one of several sectors within IoT.

This chapter draws on peer-reviewed publications, reports, websites, interviews with several experts, comments submitted in response to NIST's Request for Information (RFI), and observations at the S4x22 IoT security conference [13]. Given the enormous scope of IoT, the chapter does not attempt to apply the topics listed above to each market sector. Rather, it describes the general state of the IoT landscape using manufacturing as a case study (the Consolidated Appropriations Act of 2021 directs NIST to focus on IoT in Manufacturing as one of the emerging technologies).

2.2.2. IoT Industry Sectors

As IoT products and services have penetrated every market sector, various classification schemes have been proposed to impose order on this complex landscape. While acknowledging other options, this study used the "World of IoT Sector Map" introduced by Beecham Research in 2008 [14], which divided IoT into nine sectors. IoT in manufacturing is a sub-sector of IIoT in the Beecham scheme, along with mining and agriculture. IoT applications within manufacturing span the entire product lifecycle, including product design, remote production control, predictive maintenance, management of assets, and targeted delivery.

2.2.3. Non-Government Entities That Support IoT Adoption

Many organizations have been established in the past 10–20 years to remove obstacles to the development and seamless use of IoT. These organizations include industry consortia, associations, standards development organizations (SDO), open-source foundations, and alliances. Well-known examples of these entities that are involved in IoT are the International Organization for Standardization (ISO), the European Telecommunications Standards Institute (ETSI), Clean Energy Smart Manufacturing Innovation Institute (CESMII), Cybersecurity Manufacturing Innovation Institute (CyManII), Institute of Electrical and Electronics Engineers (IEEE) Standards Association, Open Manufacturing Platform, the Consumer Technology Association (CTA), Connectivity Standards Alliance, The International Telecommunication Union (ITU), and Internet Engineering Task Force (IETF). These organizations play in some cases multiple roles in issuing standards, as well as standards verification, dissemination, and advocacy.

2.2.4. U.S. Federal Government Support for IoT

The Federal Government participates in the promotion and safe and secure adoption of IoT by engaging with commercial and non-commercial stakeholders to establish an appropriate legal and regulatory framework and baseline requirements; creating laws, standards, and guidance; and funding research and development projects. No single agency has exclusive jurisdiction over IoT, and interagency work in this area has until recently been limited (a recently formed Interagency Working Group was established in January 2022 to address IoT applications). One example of early interagency work was a collaboration between NIST, the Department of Defense (DOD), the U.S. Food and Drug Administration (FDA), and several other agencies to establish IoT core capability baselines in 2020. Another example is the Interagency International Cybersecurity Standardization Working Group (IICSWG) established in December 2015 by the National Security Council’s Cyber Interagency Policy Committee to coordinate major issues in international cybersecurity standardization, which produced NIST IR 8200 [15; 16]. Yet another example of interagency work is the Networking and Information Technology Research and Development program's Computing-Enabled Networked Physical Systems Interagency Working Group – co-chaired by the National Science Foundation and the National Security Agency – which coordinates Federal R&D to advance and assure integrated IT-enabled cyber, physical, and human systems – spanning complex, high-reliability, safety- /security-critical, real-time computing and engineered systems with varying degrees of autonomy and human-system interaction.

Over the past five years, Congress has passed several relevant laws, and the executive branch has issued several Executive orders relevant to IoT. These efforts are expected to raise awareness of the risks of IoT technology and establish baseline cybersecurity requirements, which should incentivize manufacturers to develop safer products. Key examples of these legislative and executive efforts include:

- *Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, issued in 2017, which instructed the Department of Commerce and the Department of Homeland Security (DHS) to investigate the threat of botnets and recommend actions to mitigate risks.
- The *IoT Cybersecurity Improvement Act 2020*, which required Federal agencies to acquire only devices that meet minimum cybersecurity requirements and charged NIST with developing and regularly updating the necessary guidance.
- The *National Defense Authorization Act 2020*, which instructed the Secretary of Defense to establish secure wireless network components and capabilities, including IoT devices.
- *The National Defense Authorization Act 2021*, which directed the Department of Commerce to establish an interagency working group of Federal agencies and an advisory committee to advise the Federal working group. These bodies will deliver report to Congress on barriers to IoT adoption.
- *Executive Order 14028*, *Improving the Nation's Cybersecurity*, issued in 2021, which charged the Federal Government to initiate programs to educate the public about IoT and identify criteria for consumer labeling of IoT products.

NIST has been involved in many efforts to promote safe and secure use of IoT. As a result of Executive Order (E.O.) 13800, the Report delivered to the White House identified IoT devices as a specific risk to the internet. In the Roadmap accepted by the White House, NIST was directed to develop a core baseline that would identify the common security capabilities that all IoT devices should provide. This resulted in the NIST IR 8259 series (8259, 8259A, 8259B, and 8259C). To comply with the mandate in the *IoT Cybersecurity Improvement Act 2020*, NIST released a compendium of publications to ensure that the Federal Government and designers of IoT devices have a shared understanding of cybersecurity requirements for IoT products used by the agencies. These include NIST Special Publications (SP) 800-213 and 800-213A, which built on the 8259 series. As instructed by E.O. 14028, *Improving the Nation's Cybersecurity,* NIST also issued a white paper that recommended consumer label criteria for IoT products and software, along with considerations for label design, consumer education, and conformity assessment. NIST also developed a report that summarized the process used to arrive at labeling recommendations.

2.2.5. U.S. Federal Government Engagement with Industry

The Federal Government uses multiple strategies to interact with industry on the development and safe adoption of IoT. Importantly, in October 2022, the White House brought together companies, associations, and government partners to discuss the development of a label for IoT devices so that Americans can easily recognize which devices meet the highest cybersecurity standards to protect against hacking and other cyber vulnerabilities. In addition, Federal agencies seek input on frameworks, guidance, regulations, criteria, and policies from a broad range of stakeholders by sponsoring workshops, holding public hearings, posting notices in the Federal Register, and soliciting comments to draft documents. Industry firms coalesce into groups that, in some cases, include Federal agencies; the Industry IoT Consortium is an example of this collaboration. Finally, the Federal Government interacts with industry by funding research, development, and deployment projects, both through ad hoc programs, such as the Silicon Valley Innovation Program launched by the DHS, the government-wide, long-standing Small Business Innovation Research (SBIR) program, and the Manufacturing Extension Partnership (MEP).

2.2.6. Market Trends in IoT Use in Manufacturing

The literature yielded several estimates of the market size for IoT in manufacturing, which varied by nearly tenfold, from approximately $28 billion in a 2018 estimate to $238 billion in a 2021 estimate [17]. Despite these large discrepancies, all studies agreed that the IoT market was large and rapidly growing, and one source also suggested that manufacturing represented the largest market share [18–20; 17; 21]. Within the manufacturing sector, predictive maintenance comprises the largest share, followed by real-time workforce tracking and emergency/incident management. Recent research from McKinsey & Company revealed that IoT in manufacturing can unlock $1.43 billion to $3.32 billion in economic value [22], exceeding other sectors. Factors that facilitate the adoption of IoT include perception of benefits resulting from these technologies; recent important technological developments in sensors, hardware, digital storage, battery power, and machine learning tools; and better, cheaper, and increasingly accessible digital communication and connectivity.

2.2.7. Risks Posed by IoT Technologies

Given the ubiquity of IoT in our society, it is critical to understand and mitigate the multiple risks posed by these technologies. One of these is the risk to the entire supply chain, which encompasses protection of proprietary information and data, reliability and resilience of delivery mechanisms, quality and durability of component parts and final products, and potentially the viability of the vendor. Rapidly evolving and poorly regulated, IoT systems are attractive targets for malicious actors, posing risks to national security, including economic security. For example, an attack in October 2016 by IoT malware called *Mirai* brought down websites for several major news and other organizations in the United States and Europe. This "distributed denial-of-service" (DDoS) attack, which made the sites inaccessible for much of the day, is considered to be the largest of its kind at that time [23]. More recent DDoS attacks include Mēris v. Google, 2022-06 [24]; Mantis v. CloudFlare, 2022-06 [25], and Undisclosed v. CloudFlare, 2022-04 [26]. IoT in the energy sector represent especially appealing targets for hostile governments and individuals because they are integrated with the most sensitive infrastructure in the United States, have high commercial value, and yet are still developing cybersecurity protections [27]. The generally slow transition from legacy systems to connected machines, sensors, industrial control systems, and IT networks generates a number of difficult-to-resolve cybersecurity issues. Industrial IoT devices are sourced in different countries and contain many components, each with its own supply chain that can be compromised at multiple points. Once the industrial IoT environment is breached, it puts all control and production systems at risk. Furthermore, it may take weeks or months before the effects become apparent, and additional time to respond when a vulnerability is localized.

Users of IoT are also at serious risk for loss of privacy. IoT devices aggregate information from multiple sources over time, which provides not only data that are directly collected, but also potentially sensitive information that can be inferred or derived from these data. Without guardrails in place, the public will increasingly lose control of information about their movements, habits, preferences, and daily occupations. And an increasing use of biometric authentication combined with IoT technology poses additional risks to individual privacy and freedom.

Finally, while IoT devices generate and collect a wealth of personal data, legal and ethical questions about data ownership and retention remain unresolved. For example, companies that collect data at "smart cities" may be able to privatize this information—including personal data—without obtaining consent from the subjects. The rights of consumers enshrined in future laws and regulations will play an essential role in how and to what extent these data can be monetized.

2.3. Observations

2.3.1. Industry Sectors That Develop, Implement, and Promote the Use of the Internet of Things

All industry sectors are increasingly using IoT devices, and various attempts have been made to organize this complex landscape. Recent systematic review of the literature identified two types of taxonomies: one based on the quality of the IoT system (e.g., as security, privacy, trust, interoperability, scalability, and reliability) and the other on the elements of the system (i.e., the nature of devices, mode of communication, type of software and data, mode of deployment, and user) [28]. No consensus classification is available at this time, and rapid development and adoption of IoT technology across industries makes such classification difficult.

While acknowledging other taxonomies, this study used the *World of IoT Sector Map* introduced in 2008 by Beecham Research and regularly updated to reflect changing market conditions [29]. The map contains nine market sectors that use IoT, the types of application within each sector, and the Things connected through the internet. The map itself is very complex (Appendix E), but Table 1 shows the brief summary of market sectors with example applications.

IIoT is one of the sectors on the map, which is further divided into three application groups: agriculture and mining, distribution, and manufacturing. Table 2 describes several use cases that span the manufacturing lifecycle. For example, manufacturers can collect information on the production outcomes to ensure they meet expectations (i.e., remote production control). Built-in sensors can detect equipment malfunction and alert staff to quickly address the problem and contain damage (i.e., predictive maintenance). Production managers can obtain real-time information about the state of inventory to order needed parts (i.e., asset management). A combination of IoT and other tools, such as artificial intelligence (AI), can computationally model the process of production or equipment performance to avoid physical damage (i.e., digital twins). In general, IoT potentially enables more accurate tracking of the flow of goods and strengthen supply chains. These are just some examples of many potentially powerful IoT applications that can transform manufacturing [29; 30]:

Table 1. Example Applications of IoT in Different Sectors

Sector	Examples
Building and construction	Heating, ventilation, and air conditioning (HVAC), lighting, elevators, security, tool management, security, worker safety, energy efficiency
Energy	Generation, extraction, storage, grid connection, energy monitoring
Consumer and home	Energy management, security alerts, climate control, fire and environmental safety, appliances, entertainment, home health care
Health and life sciences	Treatment, patient management, remote monitoring, drug development, laboratories
Industrial	Manufacturing: assembly, material handling, asset and supply chain management, packaging and distribution, digital twins, equipment monitoring Mining: automation of underground ventilation, atmospheric monitoring of underground environment, equipment monitoring Agriculture: environmental and plant health monitoring; automation of planting, irrigation, harvesting; cattle management and monitoring
Transport and logistics	Tracking movement of goods through the supply chain, traffic, and route management, operational monitoring of train systems and airports, cargo storage, connected motor vehicles
Retail	Automated checkout in hotels and supermarkets, smart shelves, vending machines, security cameras, banking
Security and public safety	Water treatment and environmental monitoring, radar and satellite surveillance, communication, emergency response
Information and communication technology	Data storage, wireless network management, computing, sensor input monitoring

Table 2. Example Applications of IoT to Manufacturing

Domain	Application
Remote Production Control	Manufacturers can collect information on the production processes and outcomes to ensure they meet specific requirements. In addition, devices can be configured, adjusted, and repaired remotely, saving time and effort and streamlining management of equipment. Finally, managers can monitor location of movable assets.
Predictive Maintenance	IoT sensors can detect operational malfunction (e.g., temperature, pressure, voltage) and alert staff about the deterioration of equipment. Advanced analytics software can be integrated with IoT devices to anticipate the need for technical support service.
Industrial Asset Management	Manufacturers can obtain and monitor real-time information on all their assets, such as delivery vehicles, items in warehouses, and resources during the production process. This allows tracking and optimization of assets from supply chain to delivery.
Digital Twins	This technology is based on IoT, artificial intelligence, machine learning, and cloud computing. Digital twins are virtual copies of equipment and spare parts, and can be used to simulate numerous processes, conduct experiments, and discover problems without damaging physical assets.

2.3.2. Public-Private Partnerships Focused on Promoting the Adoption and Use of the Internet of Things

According to the Government Accountability Office (GAO), public-private partnerships (PPP) “typically involve a government agency contracting with a private partner to renovate, construct, operate, maintain, and/or manage a facility or system, in part or in whole, that provides a public service” [31]. In some cases of PPPs, the cost of a service is funded through fees paid by users of the public service, rather than by tax revenues; in other cases, the private sector is contracted to provide the service directly, with the cost partially or completely borne by the government. The government may also support a project by subsidizing revenue through tax breaks or by guaranteeing annual payments for a specified period of time. For projects aimed at sectors that provide durable capabilities like infrastructure, single capital subsidies, such as one-time grants or loans that enable a project to be economically viable, may be provided. Through these types of mechanisms, PPPs enable the sharing of risk between the government and the private sector.

The following are examples of PPPs related to IoT. The Department of the Homeland Security (DHS) is the executive agent for the Public-Private Analytic Exchange Program (AEP) [32]. U.S. Government analysts and private sector partners work through AEP across their different but interlocking areas of responsibility to safeguard the national infrastructure, financial technology, biotechnology, information technology and social media, physical trade, and supply chain integrity. Participants create joint analytic products of interest to both the private sector and the U.S. Government.

Manufacturing USA [33] (previously known as the National Network for Manufacturing Innovation) is a network of 16 research institutes in the United States that focus on developing manufacturing technologies through PPPs among the Federal agencies, industry, and universities. The institutes in the network collaborate to develop solutions for current and future industrial challenges through manufacturing innovation, workforce education, and supply chain development. Several Manufacturing USA institutes work in IoT space, including the Clean Energy Smart Manufacturing Innovation Institute (CESMII), which was created in 2016 with $70 million from the Department of Energy (DOE) to “drive smart manufacturing” through education and workforce development, industry networking, and funding of research projects [34]. Toward these goals, CESMII launched a Smart Manufacturing Innovation Platform as a pilot interoperability solution that could be used by different products. In 2020, DOE launched the Cybersecurity Manufacturing Innovation Institute (CyManII) to address the rising cybersecurity challenges around secure automation and supply chain of manufacturing in the USA [35]. CyManII focuses on early-stage research projects, industry collaborations, and workforce development with particular emphasis on small- and medium-sized manufacturers that may not have cybersecurity expertise.

The Council on Competitiveness [36] includes a diverse and nonpartisan membership of chief executive officers (CEOs), university presidents, labor leaders, and national lab directors representing the major sectors of the economy to shape policies and create programs to jump-start productivity and promote America's economic growth. Among their focus areas is leveraging advanced computing to lead in emerging technology areas like AI and the IoT.

NIST’s Manufacturing Extension Partnership (MEP) is a network of centers in all 50 States and Puerto Rico [37]. The network includes partners from State and local governments; Federal agencies (DOE, DOC, and DOD); academic institutions; trade associations; professional societies; think tanks; economic development organizations; and the private sector, including manufacturers and consulting firms. It offers a broad range of funding opportunities, services, educational resources, and other supports to strengthen competitiveness and promote growth of the manufacturing sector. While MEP’s mission is much broader than development and safe adoption of IoT, it is actively involved in this space. For example, the MEP website lists many resources on cybersecurity for manufacturers, including guidance for IoT devices in two areas: (1) for manufacturers building secure IoT products and (2) for manufacturers moving to IOT production lines (Industry 4.0). To increase small- and medium-sized manufacturers’ awareness and adoption of IoT, recently MEP awarded five Advanced Manufacturing Technology Service awards to help manufacturers increase process and product efficiency and grow capacity.

Additional examples of relationships between the government and the private sector are included in 1.2.7, *Interaction of Federal Agencies with Industry Sectors*.

2.3.3. Industry-Based Bodies That Develop Mandatory or Voluntary Standards for the Internet of Things

This section describes the array of U.S. and international Standards Development Organizations (SDOs), industry consortia, and associations that are responsible for—or influence—the development, maintenance, and adoption of standards in IoT and IoT in manufacturing. These entities' methodologies vary widely, but they have a common interest in enabling the uptake of particular manufacturing processes, strategies, or technologies, while reducing use risks. The research identified numerous organizations involved in IoT standardization (Appendix F), one of which pointedly noted that "dialogue and collaboration among IoT-related SDOs at European and international levels, is more than necessary to foster convergence towards globally interoperable solutions for the IoT across domains." [38] A small subset of key organizations involved at various stages of the standardization lifecycle is described below.

2.3.3.1. Industry Consortia and Associations

These entities play a role in the early stages of product lifecycle. A consortium may identify the need for a standard and initiate the process of its development with an appropriate SDO. The consortium members will then provide the subject matter expertise to help the SDO define the requirements for the standard, test it once it is developed, and advocate for its use in their community. For example, the Industry IoT Consortium (IIC) is an international team of connectivity experts who aim to define the minimum expectations required to build next generation capabilities [39]. In a recently issued foundational document, "The Industrial Internet of Things Connectivity Framework," IIC offers guidance for how to determine the most appropriate core connectivity standard [40]. Consumer Technology Association (CTA) [41], Connectivity Standards Alliance (CSA), and IoXT Alliance are other examples of industry associations that advance IoT standards, especially in cybersecurity [42; 43]. Additional examples of international consortia and associations that focus on the digital ecosystem are included in Appendix F.

2.3.3.2. Standards Development Organizations

A standard is "a repeatable, harmonized, agreed, and documented way of doing something. Standards contain technical specifications or other precise criteria designed to be used consistently as a rule, guideline, or definition" [44]. Standards are designed to make production simpler and increase the reliability, effectiveness, interoperability, safety, security, and trustworthiness of goods and services. This section describes several main SDOs; the IoT standards that they have issued are included in section 2.3.10.

The International Organization for Standardization (ISO) is one of the best-known examples of non-governmental entities that develop standards. ISO is an umbrella for 167 national standards bodies, which come together to develop "voluntary, consensus-based, market-relevant international standards that support innovation." [45].

The European Telecommunications Standards Institute (ETSI) [46] is a standards organization established by the European Conference of Postal and Telecommunications Administrations. ETSI is the regional standards body handling telecommunications, broadcasting, and other electronic communications networks and services. ETSI is one of three European Standards Organizations, along with the European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC) [47], that are recognized by the European Union.

The American National Standards Institute (ANSI) [48] is private, non-profit organization that oversees the development of voluntary standards and conformity assessment systems for products, services, systems, and personnel in the United States [49]. ANSI represents 270,000 companies worldwide and collaborates with stakeholders from industry and government to develop solutions to global priorities. ANSI does not issue its own standards, but oversees their development by accrediting the procedures of standards-making organizations. ANSI is also responsible for coordinating U.S. and international standards.

Finally, the Institute of Electrical and Electronics Engineers (IEEE) Standards Association [50] develops standards by bringing together a broad stakeholder community. IEEE standards, specifications, and best practices—which are based on the latest scientific and technological knowledge—cover multiple areas, such as wired and wireless connectivity, encryption, data security, and others. IEEE maintains an active portfolio of 1,076 standards, including several that are directly relevant to IoT.

Additional standards development organizations are included in Appendix F.

2.3.3.3. Open-Source Foundations (OSF)

OSFs are non-profit organizations whose mission is to provide support for open and collaborative software by developing programming languages, definitions, frameworks, coding practices, and other technical efforts [51]. OSFs also provide non-technical support, including advocacy, legal and financial aid, and governance for free and open-source software projects.

At least 89 OSFs [51] focus on various open-source software development, language, and coding projects, of which the Linux [52], Apache [53], and Eclipse foundations [54] are most relevant to IoT. The Linux Foundation, for example, is a non-profit technology consortium founded in 2000 to develop the operating system that bears its name and to support its growth and commercial adoption [52]. As a neutral home for code and collaboration, the foundation works to democratize coding by providing open-source software technology and supporting programs for developer enablement. The Linux Foundation is one of the predominant operating systems in industrial IoT devices and the embedded systems that control these devices, and it has developed the body of technical knowledge to deliver smart connected products and solutions that take advantage of the rapid evolution of IoT technologies [55]. SOM Research Labs [56] maintains a comprehensive database of OSFs that includes information on their roles in developing, maintaining, and promoting standards.

2.3.3.4. Industry Alliances

Industry alliances are consumers of standards. These organizations become involved in the product development cycle after the standards are published by participating in advocacy, verification, and dissemination. One industry alliance that focuses on IoT in manufacturing is the Open Manufacturing Platform (OMP) [57] under the Linux Foundation. The association between these two entities illustrates the overlap between organizations involved in standardization. Founded in 2019, OMP is an international alliance of companies that promote cross-industry collaboration, knowledge and data sharing, and access to new technologies to accelerate innovation in manufacturing.

2.3.3.5. Cybersecurity Guidance Organizations

These organizations aim to promote good security practices, increase adopter knowledge, and raise user confidence in IoT. Examples of contributions these organizations have made include a comprehensive IoT Security Assurance Framework with recommended steps for creating IoT products and services [58] as well as a variety of other publications on different aspects of IoT security for a range of applications, from health care to smart buildings. The IoT Security Foundation (IoTSF) [59], an international, vendor-neutral, collaborative non-profit initiative, is one example of this type of organization. Additional cybersecurity guidance organizations that are directly addressing IoT are included in Appendix F.

2.3.4. Status of Industry-Based Mandatory or Voluntary Standards

IoT in manufacturing (also known as IIoT) is a domain that spans technologies ranging from sensor communication to machine learning (ML). Consequently, the list of potentially relevant standards is long, including dozens of items issued by various SDOs [60], some of which are legacy protocols while others are emerging protocols borrowed from other domains.[38] IIC advised manufacturers to use this “shopping list” when considering their own technology areas. Examples of industry standards that had been implemented are listed in Section 2.3.10 *Guidelines, Mandatory Standards, Voluntary Standards, and Other Policies Implemented by Industry-Based Bodies.*

2.3.5. Description of the Ways Entities of Industry Sectors Develop, Implement, and Promote the Use of the Internet of Things

The adoption of IoT devices has been more rapid than expected due to the proliferation of smart home products. Additionally, the shortage in manpower, increased reliance on delivery services, and remote operation of equipment due to social distancing stemming from the COVID-19 pandemic further spurred investment and innovation in IoT, including in the manufacturing sector [61]. Appropriate industry standards—especially those governing cybersecurity and privacy of devices—remain the true enablers for secure and privacy preserving uptake of IoT across industry sectors [62]. In addition to standards, industry alliances and consortia, foundations, and similar bodies are working to remove technical obstacles related to the seamless use of IoT, such as interoperability of IoT products and data management protocols.

The previous sections mention various efforts by industry players and other entities to develop, implement, and promote IoT and IoT in manufacturing. For example, Beecham Research maintains an IoT World Map [29] branching out from nine industry sectors, through 28 application groups (technology categories by industry), to 104 application types

[38] *Comment on FR Doc # 211116-0234 available at https://www.regulations.gov/comment/NIST-2021-0007-0032*

(industry use cases with information on key market influences), to 92 discrete "things" (controllers, sensors, and other edge devices). Each sector contains information on leading suppliers, which can be drilled down further to applications and "things" within that sector. By navigating the map, a user can identify potential partners and engage with the industry sector in multiple ways.

Section 2.3.10 *Guidelines, Mandatory Standards, Voluntary Standards, and Other Policies Implemented by Industry-Based Bodies* describes efforts by existing industry groups and SDOs to influence and promote adoption of technologies, practices, and processes applicable to different IoT domains and market sectors. Among these efforts is the creation of new subordinate or associated organizations, such as focused OSFs, to spur development of software languages with the necessary attributes for controlling and operating IoT devices. IoT consortia have formed within several industry segments to help with the transition to new technology. Similarly, the SDOs have launched working groups specifically dedicated to developing and promulgating standards for the technologies that comprise the IoT, with strong drivers by the manufacturing sector to harness the economic benefits of automated processes enabled by the IoT. Section 2.3.10 *Guidelines, Mandatory Standards, Voluntary Standards, and Other Policies Implemented by Industry-Based Bodies* discusses ongoing efforts to develop these IoT standards and gives specific examples.

Section 2.3.4, *Status of Industry-Based Mandatory or Voluntary Standards* describes the basic technology categories where common standards that have been previously developed are evolving, or new standards are being generated to address the IoT. These technology standards are organized around operating systems, data management, information exchange, systems modeling and interoperability, cloud development and deployment technologies, security, and AI and ML. Standards across these technology categories are essential for the advancement and widespread adoption of the IoT and associated devices. For the manufacturing sector in particular, these standards provide incentives by reducing the economic barriers and business risks associated with adoption.

PPPs as well as industry-led efforts have already emerged in all of these areas, but IoT and IoT in manufacturing can nevertheless benefit from Federal oversight to continue to drive the regulatory and legal process and help establish clear boundaries for accountability within market segments. Examples of incentives that could be employed through legislation and serve as strong drivers in the manufacturing industry, where profit margins directly affect competitiveness.

Given the potentially catastrophic loss due to IoT-based attacks,[39] the manufacturing industry has begun to take steps to address IoT security challenges, despite large capital investment required for retooling. The number of industry conferences to share, promote, and coordinate approaches to addressing the cybersecurity risks that IoT introduces into manufacturing infrastructure has grown over the past decade [63]. These conferences have created momentum for developing new risk reduction strategies, such as cybersecurity insurance, and adopting best practices for incident response and recovery.

[39] A report presented at S4x22 by Waterfall Security Solutions of IIoT security incidents over the last 2 years indicated that the number of successful attacks had increased 150% from 2020 to 2021, and is expected to grow exponentially.

2.3.6. Federal Agencies with Jurisdiction

This section identifies Federal agencies with (a) broad, cross-sector jurisdiction over various aspects of IoT, (b) key responsibilities assigned in two recent Executive Orders (E.O.) on software and hardware supply chains, and (c) jurisdiction over applications in selected sectors of IoT.

2.3.6.1. Federal Agencies with Cross-Sector Jurisdiction over IoT

Several Federal agencies have jurisdiction over various aspects of IoT. Those jurisdictional limits are not defined according to the nine market sectors in the World of IoT map. Instead, jurisdiction is tied to topic areas—cybersecurity, spectrum, electronics stewardship, worker safety, and consumer protection—which apply to many or all market sectors. Table 3 provides examples of agency responsibilities specifically targeting IoT. Federal agencies with jurisdiction over worker safety are particularly relevant to IoT in the manufacturing sector, although they also cover sectors such as building, construction, and energy.

Table 3. Federal Agencies with Cross-Sector Jurisdiction over IoT

Topic Area	Agency	Responsibilities or Activities of Agency
Accessibility	Access Board	The Access Board, created in 1973, is an independent federal agency that promotes equality for people with disabilities through leadership in accessible design and the development of accessibility guidelines and standards. Relevant for this chapter on the IoT, the Access Board develops and maintains design criteria for the built environment, transit vehicles, information and communication technology, and medical diagnostic equipment. Recently, the Access Board published an ANPRM on self-service transaction machines (SSTMs) [64].
Cybersecurity – Standards, guidelines, best practices	National Institute of Standards and Technology (NIST)	NIST, founded in 1901, is part of the Department of Commerce. “NIST develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of U.S. industry, Federal agencies and the broader public.” [65]. FISMA (the Federal Information Security Modernization Act of 2014) assigned NIST responsibilities to develop “standards to be used by Federal agencies to categorize information and systems based on the objectives of providing appropriate levels of information security according to a range of risk levels; guidelines recommending the types of information and systems to be included in each category; and

Topic Area	Agency	Responsibilities or Activities of Agency
		minimum information security requirements (management, operational, and technical security controls) for information and systems in each such category." [66]. NIST has a robust Cybersecurity for IoT Program "to cultivate trust in the IoT and foster an environment that enables innovation on a global scale through standards, guidance, and related tools." [67]. Notably, the IoT Cybersecurity Improvement Act of 2020 tasked NIST with developing security standards and guidelines for the appropriate use and management of all IoT devices owned or controlled by the Federal Government and connected to its information systems [68]. See Section 2.3.9.2 of this chapter for further details.
Cybersecurity – Federal civilian networks and critical infrastructure	Cybersecurity and Infrastructure Security Agency (CISA)	CISA, established in 2018, is a Federal agency under oversight of DHS. CISA is the operational lead for Federal cybersecurity, protecting and defending Federal civilian government networks; it coordinates the execution of national cyber defense. CISA is also the National Coordinator for Critical Infrastructure Security and Resilience [69].
Cybersecurity – Policy and oversight	Office of Management and Budget (OMB)	OMB, an office in the Executive Office of the President, "mandates that all Federal agencies implement NIST's cybersecurity standards and guidance for non-national security systems." [65].[40] OMB also works in close partnership with CISA in Federal cybersecurity [69]. OMB is the home of the Federal Chief Information Officer (CIO), who leads the interagency CIO Council [70].
	Office of the National Cyber Director (ONCD)	ONCD is the principal advisor to the President on cybersecurity policy and strategy. See 6 U.S.C. 1500.
Cybersecurity – Encryption	National Security Agency (NSA)	NSA develops cryptographic algorithms and "produces, certifies, and supports" cryptographic systems. NSA is working on post-quantum cryptography [71]. CNSS Policy 15 lists the NSA-

[40] The IoT Cybersecurity Improvement Act of 2020 further codifies responsibilities for OMB in IoT.

Topic Area	Agency	Responsibilities or Activities of Agency
		approved Commercial National Security Algorithm (CNSA) Suite [72].
Cybersecurity – National Security Systems	Committee on National Security Systems (CNSS)	CNSS is an intergovernmental organization established in 2001 but with roots going back to 1953. It sets cybersecurity policies, directives, instructions, operational procedures, guidance, and advisories for Federal departments and agencies for the security of National Security Systems (NSS) [73].
Cybersecurity – DOD	U.S. Cyber Command (USCYBERCOM)	USCYBERCOM, formed in May 2010, "unifies the direction of cyberspace operations, strengthens DOD cyberspace capabilities, and integrates and bolsters DOD's cyber expertise." [74]. USCYBERCOM included IoT Defense as one of the problems in its 2020 set of technical challenge problems, saying it "needs a means to exploit IoT vulnerabilities in order to protect its networks, and gain access to adversary networks in order to move laterally, pivot, and achieve dominance." [75]
Cybersecurity – Cloud Services – General Services Administration	FedRAMP	FedRAMP, established in 2011, is a Federal program residing within the General Services Administration (GSA) and governed by a Joint Authorization Board consisting of the CIOs of DOD, DHS, and GSA. It "promotes the adoption of secure cloud services across the Federal Government by providing a standardized approach to security and risk assessment for cloud technologies and Federal agencies." [76]
Cybersecurity – Cloud Services – DOD	Defense Information Systems Agency (DISA)	DOD Instruction 8500.01 directs that DISA "develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DOD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS, using input from stakeholders." [73] DISA released the Cloud Computing Security Requirements Guide (SRG) Version 1, Release 4, on January 14, 2022 [77].

Topic Area	Agency	Responsibilities or Activities of Agency
Spectrum	Federal Communications Commission (FCC)	The FCC was created by the Communications Act of 1934 to control spectrum access by non-Federal users. The National Defense Authorization Act for FY 2021 required the FCC to issue a Notice of Inquiry (NOI) seeking comment on current and future spectrum needs to enable better connectivity for IoT. The FCC issued the NOI on September 30, 2021 [78].
Spectrum	National Telecommunications and Information Administration (NTIA)	NTIA, part of the Department of Commerce, was created in 1992 to manage spectrum in Federal bands. Congress has authorized NTIA to allow for sharing of Federal spectrum with non-Federal licensees for the purposes of "facilitating the prompt implementation of new technologies or services…." [79].
Electronics stewardship	Environmental Protection Agency (EPA)	EPA, formed in 1970, is a regulatory agency charged with protecting the environment and public health; it maintains and enforces environmental laws. One of its many focus areas is electronics stewardship, which considers environmental impacts across all phases of a product's lifecycle [80]. An example initiative is the Electronic Product Environmental Assessment Tool (EPEAT), a global ecolabel for the information technology sector [81].
Worker Safety – General	Occupational Safety and Health Administration (OSHA)	OSHA, part of the Department of Labor, was created by the Occupational Safety and Health (OSH) Act of 1970 "to ensure safe and healthful working conditions for workers by setting and enforcing standards…." [82].
Worker Safety – General	National Institute for Occupational Safety and Health (NIOSH)	NIOSH, part of the Centers for Disease Control and Prevention, was created by the OSH Act of 1970 as a "research agency focused on the study of worker safety and health…." [83].
Worker Safety – IoT-empowered	NIOSH Center for Direct Reading and Sensor Technologies (NCDRST)	NCDRST, created in 2014, coordinates research on direct-reading methods and sensor technologies, used in mining, oil and gas, manufacturing, construction, etc. These technologies can detect and monitor hazardous conditions, assess intervention strategies, and

Topic Area	Agency	Responsibilities or Activities of Agency
		trigger alarms in the event of unsafe conditions [84].
Worker Safety – Supply Chains	Bureau of International Labor Affairs (ILAB)	ILAB maintains a list of goods and their source countries which it has reason to believe are produced by child labor or forced labor in violation of international standards, as required under the Trafficking Victims Protection Reauthorization Act (TVPRA) of 2005 and subsequent reauthorizations. Relevant to IoT supply chains with critical minerals and rare earths inputs [85].
Consumer Protection – Fraud, privacy, security	Federal Trade Commission (FTC)	FTC, founded in 1914, regulates truth in advertising [86]. It also enforces Federal laws relating to consumers' privacy and security [87].
Consumer Protection – Safety	Consumer Product Safety Commission (CPSC)	CPSC, founded in 1972, protects consumers from unreasonable risk of injury or death from consumer products [88]. CPSC is exploring how to define consumer product safety in terms of the IoT [89].

2.3.6.2. Federal Agencies with Cross-Sector Responsibilities under Recent Executive Orders

This section focuses on agencies with responsibilities under two recent EOs:

- E.O. 14028, *Improving the Nation's Cybersecurity*, May 12, 2021 [90]. Table 4 lists agencies responsible for ensuring that the Federal Government acquires software produced using a secure software development framework designed to mitigate the risks of software vulnerabilities. Section 2.3.9.2 of this chapter covers product labeling programs proposed in EO 14028 to inform consumers about the security capabilities of IoT devices. The Secretary of Commerce, acting through NIST and the FTC are directed to take actions in support of these programs.
- E.O. 14017, *America's Supply Chains*, February 24, 2021 [91]. This E.O. directs reviews of supply chain risks of a number of specific critical goods, some of which are vital to the production of IoT devices and microelectronics in general. The E.O. also directs a number of supply chain assessments for a variety of industrial bases (Energy, Agriculture, Defense, etc.) that include digital elements related to IoT

devices relevant to these sectors. Table 5 lists key agencies taking actions under the EO.

Table 4. Federal Agencies with Responsibilities under E.O. 14028

Topic Area	Agency	Responsibilities or Activities of Agency
Software Supply Chain	NIST	E.O. 14028 4(e): NIST issued guidance, Special Publication (SP) 800-218, identifying software producer practices that enhance the software supply chain [92]. E.O. 14028 4(e): NIST published a white paper, "Software Supply Chain Guidance Under Executive Order (EO) 14028 Section 4(e)," [93] which addresses Section 4(e) from a software purchaser viewpoint.
Software Supply Chain	NTIA	E.O. 14028 4(f): NTIA published a list of the minimum elements required for a software bill of materials (SBOM) [94].
Software Supply Chain	OMB	E.O. 140284(k): OMB is to "take steps to require agencies to comply with Section 4e guidance" (in progress). As NIST clarified in an October 13, 2021 white paper, "The requirements in [E.O. 14028] 4e and 4k related to acquisition apply to all software, not just to critical software." [95]. Thus, they apply to software embedded in IoT devices. EO 14028 4(e) states that NIST "shall issue guidance identifying practices that enhance the security of the software supply chain." E.O. 14028 4(k) states that "the Director of OMB … shall take appropriate steps to require that agencies comply with such guidelines with respect to software procured after the date of this order."

Table 5. Federal Agencies with Responsibilities under E.O. 14017

Topic Area	Agency	Responsibilities or Activities of Agency
Hardware Supply Chain – Critical Minerals	DOD	"DOD awarded $35 million to support separation and processing of rare earth elements at the nation's only operation[al] rare earth mine in Mountain Pass, California." [96].
Hardware Supply Chain – Critical Minerals	Department of the Interior (DOI)	DOI published USGS's updated list of critical minerals [96]. Regarding the Mining Law of 1872, which governs mining of most critical minerals on Federal lands: DOI established an Interagency Working Group (IWG) that is reviewing potential legislative and regulatory reform of mine

Topic Area	Agency	Responsibilities or Activities of Agency
		permitting and oversight. The IWG will deliver recommendations to Congress [96].
Hardware Supply Chain – Critical Minerals	DOE	DOE released a Funding Opportunity Announcement (FOA) for a demonstration project to extract rare earths from mine waste material [97].
Hardware Supply Chain – Critical Minerals	U.S. Geological Survey (USGS)	USGS will launch a mapping initiative to support recovery of minerals from mine waste [96].
Hardware Supply Chain – ICT	Department of Commerce (DOC)	"DOC and DHS assessed the supply chains of critical sectors and subsectors of the ICT industrial base. As the global semiconductor shortage demonstrates, the U.S. economy is vulnerable to disruptions in this critical supply chain. These vulnerabilities have grown over the past several decades, due to a combination of increased reliance on ICT devices and decreased U.S. share of global electronics manufacturing, from 30 percent to five percent over the past 25 years. To develop a resilient ICT industrial base, DOC and DHS issued eight recommendations" [96].
Hardware Supply Chain – ICT	DHS	*See* DOC.
Hardware Supply Chain – ICT	DOD	"Reliance on single-source and foreign sources presents risks to the U.S. defense industrial base…. DOD prioritized four supply chains with critical vulnerabilities that pose pressing threats to national security: kinetic capabilities; energy storage and batteries; castings and forgings; and microelectronics…To continue building long-term resilience, DOD recommends focusing efforts on four areas: (1) internal practices; (2) working with the interagency to better coordinate across economic sectors and develop whole-of-government solutions where DOD does not drive demand; (3) international efforts like increasing opportunities for co-development and coproduction; and (4) working with industry, including to explore greater standardization of requirements" [96].

2.3.6.3. Federal Agencies with Sector-Specific Jurisdiction over IoT

Table 6 lists Federal agencies with jurisdiction over sample applications from the following sectors: health and life sciences, buildings and construction, transportation and logistics, industrial, and energy. No Federal agencies with specific jurisdiction over IoT in manufacturing were identified.

Table 6. Federal Agencies with Sector-Specific Jurisdiction over IoT

Application	Agency	Responsibilities or Activities of Agency
Medical Devices	Food and Drug Administration (FDA) Center for Devices and Radiological Health (CDRH)	FDA's Center for Devices and Radiological Health (CDRH) is responsible for regulating firms that manufacture, repackage, relabel, and/or import medical devices sold in the United States [98]. In a recent plan, the FDA describes key actions it will take in several areas, including medical device cybersecurity [99].
Smart Buildings	General Services Administration (GSA)	Starting around 2005, GSA's Smart Building (SB) program focused on advanced metering and fault detection and diagnostics (FDD) technology in Federal buildings. Advancements in operational technology and broader implementation of IoT has prompted the SB community to formulate a directive "to support consistency within the program and to achieve alignment on the implementation approach as technology offerings continue to be adopted within the Public Buildings Service (PBS) portfolio [100].
Connected Motor Vehicles	National Highway Traffic Safety Administration (NHTSA)	NHTSA is one of several modal operating administrations in the Department of Transportation (DOT), and it is the operating administration responsible for overseeing motor vehicle safety.
Unmanned Aircraft Systems (UASs)	Federal Aviation Administration (FAA)	FAA, another operating administration in DOT, emulates UASs (drones), registers UASs, and certifies remote pilots [101].
Transportation – Non-traditional and emerging	Non-Traditional and Emerging Transportation Technology (NETT) Council	The NETT Council is a new DOT body established under the Infrastructure Investment and Jobs Act. It is tasked with identifying and resolving jurisdictional and regulatory gaps—resulting from DOT's siloed regulatory structure—that may impede the deployment of new technology [102].

Application	Agency	Responsibilities or Activities of Agency
Smart farms	U.S. Department of Agriculture (USDA)	FarmBeats is a digital agriculture platform that facilitates data management and analysis from sensing technologies deployed in farm fields. The system improves sparse communications in rural areas through use of television white space technology. The idea is to provide actionable data to farmers. USDA is exploring standardization [103].
Smart grids	Federal Energy Regulatory Commission (FERC)	FERC is an independent agency that regulates the interstate transmission of natural gas, oil, and electricity. FERC, along with NIST, has responsibilities for smart grid guidelines and standards [104].
Smart grids	North American Electric Reliability Corporation (NERC)	The North American Electric Reliability Corporation (NERC), which FERC certified as the Nation's Electric Reliability Organization, develops Critical Infrastructure Protection (CIP) cybersecurity reliability standards [104].

2.3.7. Interaction of Federal Agencies with Industry Sectors

Within the IoT ecosystem, Federal agencies interact with industry bodies in multiple ways, which differ in the formality of engagement. First, agencies such as NIST and the Consumer Product Safety Commission (CPSC) seek input from various stakeholders, including industry firms and consortia, by sponsoring workshops, holding public hearings, posting notices in the Federal Register, and soliciting comments to draft reports, policy, and guidance. For example, in May 2018, CPSC held a public hearing on the Internet of Things and Consumer Product Hazards, which had been announced in the Federal Register, and 13 organizations provided testimony [89]. The National Cybersecurity Center of Excellence (NCCoE), a group within NIST, "is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address industries' most pressing cybersecurity challenges." [105] NCCoE lists IoT as one of its technologies of interest. Another initiative is the NIST National Online Informative Reference Program (OLIR), a NIST effort to facilitate subject matter experts (SMEs) in defining standardized online informative references (OLIRs) between elements of their documents, products, and services and elements of NIST documents like the Cybersecurity Framework Version 1.1, Privacy Framework Version 1.0, NISTIR 8259A, or NIST SP 800-53 Revision 5 [106].

Second, industry firms organize into consortia, which in some cases include Federal agencies. For example, IIC was established in 2014 to "deliver transformative business value to industry, organizations, and society by accelerating adoption of a trustworthy Internet of Things" [107]. IIC membership includes representatives from key industries that leverage IoT (such as healthcare, information technology, manufacturing, transportation, and finance), domestic and international academic institutions (e.g., Princeton University, Vanderbilt University, University of Bologna, and Tomsk State University), and government organizations (NIST and Pacific Northwest National Laboratory).

The IIC website contains dozens of IoT-related technical and policy publications on best practices, guidance, and assistance to develop and deploy enabling technologies and technical reports. For example, in 2016, a group of members including Intel Corporation, AT&T, the University of Pennsylvania, and several other industry and academic organizations issued "The Industrial Internet Security Framework (IISF)"—a nearly 200-page document intended to establish a broad consensus on how to secure IoT systems [108]. The Consortium also organizes IoT technology pilots, hosts a repository of use cases for IoT applications for its priority industry sectors, and even publishes its own journal several times a year.

Another example of a large consortium is Cloud Security Alliance (CSA), which focuses on raising awareness of best practices to enable a secure cloud environment [109]. CSA hosts various working groups that develop best practices, perform research, and create tools for cloud security. CSA hosts the IoT Working Group (WG), which "is dedicated to understanding relevant use cases for IoT deployments and defining actionable guidance for security practitioners to secure their IoT ecosystem" [110]. Its partners include IIC, several IoT-focused non-profits, and the FCC. A search of CSA publications produced 25 hits, including recently released *Cybersecurity Best Practices for the Manufacturing Industry* [111]. Connectivity Standards Alliance creates standards to build the foundation and the future of the IoT, by creating, managing, and promoting standards, and assisting members with product and platform certification [42]. These are just three of many examples of consortia that include Federal members.

A third way for Federal agencies to interact with industry is by funding adaptations of commercially available technology. For example, in 2015, DHS launched a funding mechanism called the "Silicon Valley Innovation Program." The program leverages DHS's Other Transaction Authority, which operates outside the boundaries of the Federal Acquisition Regulation, thus facilitating DHS engagements with start-ups and other small businesses. The first solicitation was focused on IoT security solutions. Several companies received funding for IoT projects, such as Ionic Security Inc., which proposed to develop capabilities for securing video streams from smart cameras. A more recent solicitation, issued in May 2021, listed IoT security and unmanned aerial systems security as topic areas.

In addition to such ad hoc opportunities, the Federal Government supports commercial entities through the Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) programs. A query of award data available on the sbir.gov website [112] using "internet of things" identified 292 grants to 221 small businesses, with the top three funders being the National Science Foundation (129 grants), the Department of Defense (DOD) (80), and the DOE (37).

2.3.8. Interagency Activities

The Interagency International Cybersecurity Standardization WG issued an interagency report explicitly covering IoT in November 2018 [16]. The WG included representatives from NIST, DOD, Department of Veterans Affairs (VA), National Telecommunications and

Information Administration (NTIA), Food and Drug Administration (FDA), National Security Agency (NSA), and DHS. The report described the state of cybersecurity standardization for five IoT technology application areas (connected vehicles, wearables and mobile devices, health data, smart buildings, and smart manufacturing) and analyzed cybersecurity objectives, risks, and threats for these examples and for IoT more broadly. More recently, the Department of Commerce has established the Internet Policy Task Force, which is conducting a review of the benefits, challenges, and potential roles for the government in fostering the advancement of IoT [113]. The White House held an IoT Labeling Summit on October 19, 2022 "to discuss what is needed to foster an effective IoT security labeling ecosystem." [114]

Additional relevant interagency activities are taking place across the Federal Government but are more difficult to identify as they do not include "IoT" in the title. For example, CPSC organized and led an Interagency WG on Consumer Product Safety of Internet-Connected Products, with NIST, the FDA, the FTC, the FCC, DOE, and DHS participating [89]. The purpose of the WG is to understand each agency's role, identify gaps, create collaborative opportunities, and promote the development of standards and guidance. Other working groups have been established in related areas, such as 5G wireless technology [115].

The FY21 NDAA (Public Law 116-283) [116] instructed the Department of Commerce to convene a WG of Federal stakeholders to "(1) identify Federal laws and regulations, grant practices, budgetary or jurisdictional challenges, and other sector-specific policies that inhibit IoT development; (2) consider policies or programs that encourage and improve coordination among Federal agencies with relevant responsibilities; (3) consider implementing recommendations from the steering committee; and (4) examine how Federal agencies can benefit from, use, prepare for, and secure the IoT." The law further stipulated that the WG will receive recommendations from an IoT advisory board composed of non-Federal stakeholders; NIST is currently in the process of identifying 16 candidates for this board [117]. The IoT Federal WG has been meeting monthly since it was established in January 2022.[41]

Finally, NICE is a government-wide effort that began in 2010 to identify knowledge and skills necessary for cybersecurity work. The NICE Framework described in NIST Special Publication 800-181 is the result of these efforts [118]. The Framework is intended for employers to evaluate their cybersecurity workforce needs; for workers to understand what knowledge and skills are in demand in the industry; and for training and education providers to be used as a reference for curriculum development, launching of new programs, and other workforce building activities.

2.3.9. Regulations, Guidelines, Mandatory Standards, Voluntary Standards, and Other Policies Implemented by Federal Agencies

As IoT enters all sectors of society, industry, and economy, it becomes subject to general law, including public law, business law, insurance law, tax law, civil liability law, consumer protection law, and privacy/data protection law [119]. Like the internet, IoT also may require legislation to address specific situations that might occur in its operations and applications

[41] https://www.federalregister.gov/documents/2022/01/13/2022-00419/establishment-and-call-for-nominations-to-serve-on-the-internet-of-things-advisory-board

but that may be outside of the bounds of general law. Some groups argue that for sustainable development of IoT and its fair and equitable use in society, proper legal and ethical frameworks—which includes legislation, regulation, ethics principles, standards, and guidelines—should be established collaboratively with industry and consumers.

The legal and regulatory landscape for IoT is rapidly changing, with numerous bills, resolutions, and amendments being introduced. In addition, some states, such as California [120] and Oregon [121], have passed local IoT laws. Both laws require manufacturers of connected devices to equip the device with "reasonable security feature or features" appropriate for its function and the information they collect.

Finally, general U.S. legislation that protects civil rights, such as the Electronic Communication Privacy Act (1986) [122] and the Privacy Act (1974) [123], also applies to IoT activities. Given the size and complexity of this landscape, this chapter focuses only on legal, guidance, and policy documents that explicitly reference IoT and were issued in the past five years, starting in 2017.

2.3.9.1. Federal IoT Laws

Several recent laws and EOs explicitly address IoT (Table 7):

- *E. O. 13800 (2017), Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* focused Federal efforts on modernizing Federal information technology infrastructure, working with state and local government and private sector partners to more fully secure critical infrastructure, and collaborating with foreign allies.
- *IoT Cybersecurity Improvement Act of 2020* (first introduced in 2017) required Federal agencies to increase cybersecurity of their IoT devices and charged NIST with developing and regularly updating the necessary guidance.
- *The National Defense Authorization Act 2020* instructed the Secretary of Defense to establish secure 5G wireless network components and capabilities, including IoT devices.
- *Infrastructure Investment and Jobs Act of 2021* charged the Secretary of Transportation to submit a report that assesses the use of digital tools and platforms, including IoT, as climate solutions.
- *William M. (Mac) Thornberry National Defense Authorization Act of 2021* instructed the Secretary of Commerce to convene a WG of Federal stakeholders and a nongovernmental Steering Committee and provide two reports to Congress about the benefits and challenges to development, deployment, and adoption of IoT by the Federal Government and the private sector and reduce barriers to adoption.
- *E.O. 14028 (2021), Improving the Nation's Cybersecurity* charged the Federal Government to initiate programs to educate the public about IoT and identify

criteria for labeling of consumer IoT products, and authorized NIST to develop appropriate standards, guidance, and resources.

- *E.O. 14017 (2021), America's Supply Chains* required a variety of actions and studies to address manufacturing capabilities.

These early efforts are expected to have far-reaching consequences by creating better awareness of IoT risks among customers and establishing baseline cybersecurity requirements for Federal agencies, which should incentivize manufacturers to develop safer products.

Table 7. Federal Laws, Executive Orders, and Standards Relevant to IoT

Title	Became Law	Provision Relevant to IoT
Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, E.O. 13800	2017	Focused Federal efforts on modernizing Federal information technology infrastructure [124].
Internet of Things (IoT) Cybersecurity Improvement Act (HR 1668) PL 116-501	2020	Established minimum security standards for IoT devices owned or controlled by the Federal Government. Required agencies to increase cybersecurity for IoT devices owned or controlled by the Federal Government by applying relevant guidance, for NIST to provide this guidance and update it every five years, and for OMB to review information security policies and principles at Federal agencies on the basis of the NIST standards and guidelines [68].
National Defense Authorization Act for Fiscal Year 2020 (S 1790) PL 116-92	2020	Instructed the Secretary of Defense to establish secure fifth-generation wireless network components and capabilities, which includes IoT devices [125].
Infrastructure Investment and Jobs Act (HR 3684) PL 117-58	2021	Instructed the Secretary of Transportation to submit a report that assesses using digital tools and platforms as climate solutions, including IoT [126].
William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (HR 6395) PL 116-283	2021	Instructed FCC to convene a Working Group on IoT and establish a private sector Steering Committee to examine regulatory, budgetary, practice, and other challenges to development and deployment of IoT, to facilitate coordination among Federal agencies with jurisdiction, and to examine how Federal agencies might benefit from IoT [116].

Title	Became Law	Provision Relevant to IoT
Improving the Nation's Cybersecurity, E.O. 14028	2021	Instructed the Secretary of Commerce in coordination with other agencies to initiate pilot programs to educate the public on the security capabilities of IoT devices and software development practices, and to consider ways to incentivize manufacturers and developers to participate in these programs. Also, required the Secretary of Commerce to identify cybersecurity criteria for a consumer labeling program and to consider whether it may be operated in conjunction with or modeled after similar existing government programs [90].
America’s Supply Chains, Executive Order 14017	2021	Required a variety of actions and studies to address manufacturing capabilities [91].

2.3.9.2. NIST Guidance

The *IoT Cybersecurity Improvement Act of 2020* charged NIST with developing guidance to help the Federal Government increase cybersecurity of IoT devices in its use. However, NIST had already issued several relevant documents that preceded the Act, including NIST Interagency Report (NISTIR) 8228, illustrating the range of unique concerns for managing cybersecurity and privacy risks presented by the adoption of IoT (Table 9). To comply with the mandate in the Act, NIST released a compendium of interrelated publications intended to ensure that the Federal Government and IoT device designers have a shared understanding of cybersecurity requirements for devices used by Federal agencies (Table 8).

NISTIR 8259 series

In response to E.O. 13800 and the Botnet Report and Roadmap delivered to the White House, NIST developed the NISTIR 8259 series that offered general voluntary guidance to help IoT device manufacturers identify the appropriate cybersecurity capabilities for their IoT products as well as a baseline (NIST IR 8259A and NIST IR 8259B) starting point intended to be tailored as needed.

NIST 8259 enumerates cybersecurity-related activities that manufacturers could consider performing pre-market, before their IoT devices are sold to customers, and post-market [127]. NISTIRs 8259A and 8259B provided a baseline of specific technical capabilities and non-technical supporting activities, respectively, and suggested ways for manufacturers to ensure that they are addressing cybersecurity needs and goals of customers. These documents represent a common set of core baseline capabilities that apply across a range of IoT applications. Given the complexity of the IoT landscape, NIST anticipated that manufacturers would adapt this guidance to their unique needs [128].

NISTIR 8259C (Draft) described a process that can be used by any organization to apply core baseline guidance provided in 8259A and 8259B and explained how to integrate these guidelines with industry standards to develop a cybersecurity profile appropriate for specific IoT customers or applications. Finally, 8259D (draft, obsoleted) was a "worked example" of applying the 8259C process. Katerina Megas, program manager for NIST's Cybersecurity for IoT Program, explained: "We help a manufacturer start with a baseline set of capabilities and then tailor it to their market needs. Whoever they are, we want to help them improve their security in a world where things are still developing" [129].

SP 800-213 and SP 800-213A

SP 800-213 was the NIST response to the IoT Cybersecurity Improvement Act of 2020 and provided specific guidelines related to IoT security requirements to Federal agencies. It included background and recommendations to help Federal agencies determine what minimum security capabilities are needed for an IoT device to be compatible with their Federal information systems. SP 800-213A is an accompanying catalog of IoT device cybersecurity capabilities to further help establish device cybersecurity requirements for Federal agencies and manufacturers as they use SP 800-213. It also provides an example of the set of minimum-security capabilities for an IoT device to support the minimum cybersecurity baseline requirements in NIST SP 800-53.

Consumer IoT Product Labeling

The Executive Order on Improving the Nation's Cybersecurity 2021 (E.O. 14028) instructed NIST to launch an initiative to develop a strategy for labeling of consumer IoT products. Specifically, NIST was required to identify IoT cybersecurity criteria and best practices for consumer labeling [130]. Following an extensive stakeholder engagement process that included issuing draft papers proposing labeling criteria, holding workshops and other venues for public comment, and incorporating this feedback in subsequent drafts, in February 2022 NIST issued two documents that recommended criteria for cybersecurity labeling of IoT products and software. In accordance with the E.O., NIST also published a summary report describing the input from the public on the drafts of these documents [130].

NIST has launched several programs to examine all aspects of IoT, which are likely to yield additional guidance and standards in the near future. Numerous events and publications are listed on the NIST Cybersecurity for IoT Program website [67].

Table 8. NIST Guidance

Title	Year Issued	Description
Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (NISTIR 8200)	2018	Intended to help Federal agencies with standards planning and coordination [16].
Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks (NISTIR 8228)	2019	Intended to help Federal agencies and other organizations better understand and manage the cybersecurity and privacy risks associated with their IoT

Title	Year Issued	Description
		devices. Provided the foundation for a planned series of publications on IoT to help Federal agencies and other organizations better understand and manage the cybersecurity and privacy risks [131].
Cyber-Physical Systems and the Internet of Things (SP 1900-202)	2019	Described the origins of the terms "Cyber-Physical Systems" and "IoT," examined definitions and how these change over time, and clarified the relationship between these terms [3].
Foundational Cybersecurity Activities for IoT Device Manufacturers (NISTIR 8259)	2020	Defined a set of activities for IoT manufacturers to follow as they develop and support a wide range of IoT devices. Described recommended activities related to cybersecurity that manufacturers should consider before selling their IoT devices to customers, including carefully considering which cybersecurity capabilities to design into their devices [127].
IoT Device Cybersecurity Capability Baseline (NISTIR 8259A)	2020	Provided a starting baseline for organizations to use in identifying cybersecurity capabilities for new IoT devices they will manufacture, integrate, or acquire.
IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements (SP 800-213)	2021	Provided IoT-specific guidance for Federal organizations in understanding and defining their IoT cybersecurity requirements, explained the role of IoT devices as elements of Federal systems, and provided guidance for addressing the unique risks such devices can present [132].
IoT Device Cybersecurity Requirements Catalog (SP 800-213A)	2021	Provided a catalog of IoT device cybersecurity capabilities that can help organizations determine and establish device cybersecurity requirements as they use SP 800-213 [133].

Title	Year Issued	Description
IoT Non-Technical Supporting Capability Core Baseline (NISTIR 8259B)	2021	Provided a starting baseline for organizations to use in identifying non-technical supporting capabilities for new IoT devices they will manufacture, integrate, or acquire [113].
Recommended Criteria for Cybersecurity Labeling of Consumer Internet of Things (IoT) Products	2022	Recommended IoT product label criteria, label design, and consumer education considerations, and considerations for conformity assessment [130]. Superseded by NIST IR 8425, below.
Profile of the IoT Core Baseline for Consumer IoT Products (NISTIR 8425)	2022	Documented the consumer profile of IoT core baseline and identified cybersecurity capabilities commonly needed for the consumer IoT sector [134].

2.3.9.3. Guidance from Other Agencies

A study conducted by the Government Accountability Office (GAO) in 2020 revealed that with the exception of the NIST documents described in the previous section, Federal guidance related to IoT is limited. GAO surveyed representatives from 115 agencies about their experiences and found that 56 of 90 that responded used IoT technologies, typically to control or monitor equipment or systems (42 respondents), control access to devices or facilities (39), and track physical assets (28). However, all but two agencies relied on general IT policies to manage their IoT technologies [135]. In addition to NIST, the exception included DHS, which had issued two IoT-targeted guidance documents: one to set forth strategic principles for securing network-connected devices [136] and the other to recommend that acquisition teams enhance their evaluation of IoT supply chain, vendor, and technology prior to purchase [137]. Finally, as mentioned in the section on interagency activities, the Department of Commerce has established the Internet Policy Task Force, which is conducting a review of the benefits, challenges, and potential roles for the government in fostering the advancement of IoT [138]. However, no outputs from the Task Force were available at the time of writing. No guidance or policies specific to IoT in manufacturing were found.

2.3.10. Guidelines, Mandatory Standards, Voluntary Standards, and Other Policies Implemented by Industry-Based Bodies

Standards are key to the success of IoT in manufacturing and other market sectors. As the current base of manufacturing systems evolves to adopt the latest developments in IoT, a diverse set of standards that reflect industry operations from the production floor to the executive suite will be needed to enable the communication of information between various devices and applications across the entire operational lifecycle.

Dozens of standards related to communication, connectivity, integration, interoperability, applications, architecture, security, and privacy applicable to IoT and its devices have already been issued by industry organizations and similar bodies [139]. Table 9 includes a small subset of published standards that explicitly reference IoT, of which only one (ISO/IEC TR 30166:2020) focused on industrial IoT. Additional standards are under development by ISO, IEEE, ASTM International, and other organizations.

Table 9. IoT Standards and Guidance Published by Industry Bodies

Name	Published Date	Summary
ISO/IEC 29161:2016 Information technology — Data structure — Unique identification for the Internet of Things (IoT)	2016, confirmed in 2022	Established a unique identification scheme for IoT based on existing and evolving data structures [140].
ISO/IEC 20924:2021 Internet of Things (IoT) — Vocabulary	2021	Provided a definition of IoT; document is a terminology foundation for IoT [141].
ISO/IEC 21823-2:2020 Internet of things (IoT) — Interoperability for IoT systems	2020	Specified a framework and requirements for transport interoperability, to enable the construction of IoT systems with information exchange, peer-to-peer connectivity, and seamless communication between and within IoT systems [142].
ISO/IEC TR 30164:2020 Internet of things (IoT) — Edge computing	2020	Described the common concepts, terminologies, characteristics, use cases, and technologies of edge computing for IoT systems applications [143].
ISO/IEC TR 30166:2020 Internet of things (IoT) — Industrial IoT	2020	Described the general Industrial IoT systems and landscapes and considerations for the future standardization perspective of IIoT [144].
ISO/IEC 30141:2018 Internet of Things Reference Architecture	2018	Provided a standardized IoT reference architecture using a common vocabulary, reusable designs, and industry best practices [145].
IEEE P2413-2019 Standard for an Architectural Framework	2020	An architecture framework description for IoT that conforms to the international

Name	Published Date	Summary
for the Internet of Things (IoT)		standard ISO/IEC/IEEE 42010:2011 [146].
ANSI/CTA 2088-A Baseline Cybersecurity Standard for Devices and Device Systems	2021	Specified baseline security requirements and recommendations for devices and device systems to address the destructive potential of botnets and other security threats [147].
IEEE 1451-99 Standard for Harmonization of Internet of Things (IoT) Devices and Systems	2020	Defined a method for data sharing, interoperability, and security of messages over a network, regardless of underlying communication technology [148].
ITU-T SG20 Q2 Y.4003 Overview of smart manufacturing in the context of industrial Internet of Things (IoT)	2018	Provided an overview of smart manufacturing in the context of IoT-identified fundamental system characteristics and high-level requirements, specified a reference model, and provided some use cases [149].
ETSI EN 303 645 V2.1.0 Cyber Security for Consumer Internet of Things: Baseline Requirements	2020	Specified high-level security and data protection provisions for consumer IoT devices and their interactions with associated services [150].
Connectivity Standards Alliance	2022	Matter 1.0 standard and certification program [151].

In addition to developing standards and guidance, several industry alliances and associations also issue testing procedures and promote certification labels and compliance-testing procedures to signal conformity with proposed guidelines for IoT security. Examples of these tools are shown in Table 10 [152].

Table 10. Testing and Certification of IoT Guidelines

Industry Association and Guideline	Compliance Testing	Certification
Online Trust Alliance (OTA) IoT Security and Privacy Trust Framework	Online trust audit	Honor rolls
Cloud Security Alliance (CSA) New Security Guidance for Early Adopters of the IoT Future Proofing the Connected World	Cloud control matrix Consensus assessment initiative Questionnaire	Self-assessment, third party, or continuous monitoring certification
Open Connectivity Foundation (OCF) Security Specifications	Testing and certification program	Certification mark
IoT Security Foundation (IoTSF) Connected Consumer Products Best Practice Guidelines Vulnerability Disclosure Best Practices	IoT security compliance framework	Best practices user mark
Industrial Internet Consortium (IIC) Industrial Internet Security Framework	Security checklists and verticals Maturity models for industrial systems	Not applicable

Additional standards and guidance related to IoT in manufacturing are likely to emerge. The efforts for the standardization community will probably be significant because while many of the types of devices used in manufacturing (such as sensors and actuators) are well established, the extension of their range and span of control will need to be carefully considered. Furthermore, interoperability, cybersecurity, integration, functional equivalency, and varied deployment models—such as the use of Cloud Computing to host IoT-based system applications—will have to be addressed [153]. The standards will need to be adaptive to the political and geographical diversity of key manufacturing players in Europe, North America, and Asia. Finally, in a public comment submitted to NIST's RFI, the Association for Advanced Manufacturing Technology (AMT) noted that a "persistent gap" between standards developed by international bodies such as ISO and those used by U.S. manufacturers has "created friction around standardization and slowed technology adoption."[42]

2.3.11. Federal Government Resources for Consumers and Small Businesses to Evaluate the Use of Internet of Things

As discussed in Section 2.3.6.2, the Executive Order on *Improving the Nation's Cybersecurity* (E.O. 14028) instructed NIST to initiate consumer labeling programs for

[42] *Comment on FR Doc # 211116-0234 available at https://www.regulations.gov/comment/NIST-2021-0007-0023*

devices and software development practices [130]. These programs have been launched, with numerous events and other activities taking place [67]. In addition, NIST issued Interagency Report (IR) 8228 to assist organizations that use IoT in managing their cybersecurity and privacy risks. The document *Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products* and NIST's report on the response to those criteria entitled *Report for the Assistant to the President for National Security Affairs (APNSA) on Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software* contain additional recommendations regarding the implementation of the labeling program [154; 155]. Literature searches yielded limited guidance recently issued to businesses by the FTC on how they can assess IoT-related security risks and protect customers (*Careful Connections: Keeping the Internet of Things Secure* [156]). As described in other sections, IoT guidance and community norms had been developed primarily by organizations or groups outside of the Federal Government, such as the IoT Security Foundation [157]. In contrast, the Government of Canada posted links to various consumer resources on weighing the risks and benefits of IoT devices, which are easy to find using simple internet queries [17].

2.4. IoT Use in Manufacturing: Marketplace and Supply Chain

This section begins with a brief market overview, followed by the description of risks to the marketplace, supply chain, and national security of the United States, including its economic security.

2.4.1. Market Overview

Several estimates of the IoT in manufacturing have been published. The estimates varied from approximately $28 billion in a 2018 estimate to $238 billion in a 2021 estimate (Table 11) and no methodological details were available to assess their validity or accuracy. It is likely that the year of estimate as well as the definition of what constitutes IoT in manufacturing (on which there is no consensus) contributed to produce these differences. However, the studies agreed that the market for IoT in manufacturing was large and rapidly growing—at rates ranging from 11% to 22%, depending on the study. Furthermore, according to the International Data Corporation, IoT in manufacturing represents a large share of the IoT market, $78 billion of $119 billion in 2019 [18]. Recent studies concluded that all small- and medium-sized enterprises in China will adopt some form of IoT [21] and that China will soon surpass the U.S. to become the world's largest IoT market [158].

Table 11. IoT in Manufacturing Market and Growth Rates

Current Market Size	Future Market Size	Compound Annual Growth Rate
$27.7 billion in 2018 [19]	$136.8B by 2026	22%
$175.3 billion in 2020 [20]	$399.1B by 2026	15%
$51.5 billion in 2021 [159]	$134.9B by 2030	11%
$237.6 billion in 2021 [160]	$451.5B in 2025	17%
$80.1 billion in 2021 [161]	$134.9B by 2026	11%

Some market studies concluded that IoT-enabled predictive maintenance—which utilizes sensors, networks, data analytics, AI, and ML to optimize performance, extend asset lifecycles, and reduce operational downtime and cost—represents the largest share of IoT in the manufacturing sector. Real-time workforce tracking and emergency/incident management share the second spot. Global spending on IoT was projected to grow by 24% in 2021, and by 27% annually after that [162]. The fastest growth was predicted for Asia-Pacific region, followed by North America and Europe.

Recent research from McKinsey & Company moved beyond the IoT market size to estimate its potential economic value. The study concluded that based on current trends, IoT in manufacturing (specifically, in the factory setting) can unlock $1,430 billion to $3,320 billion in economic value, including the value captured by consumers of IoT products and services [163]. The benefit in the manufacturing sector significantly exceeded other sectors, including retail ($650 billion–$1,150 billion in potential value) and healthcare ($550 billion–$1,770 billion). McKinsey concluded that smart factories will reap the largest share of economic value from IoT by 2030, at around 26%.

McKinsey also identified various factors that would drive the adoption and impact of IoT [164]. One of these was an improved perception by the public that IoT offers benefits compared to a similar study conducted in 2015. The advantages of IoT were also noticed by industry: The Manufacturers Alliance for Productivity and Innovation reported that 80% of surveyed manufacturers were investing in new IoT products and services and 41% had seen positive returns on investment in the previous year of up to 5% [165]. Technological developments and better/cheaper digital communication and connectivity were also identified by McKinsey as enabling factors for IoT adoption. Recent years have seen remarkable advances in sensors, hardware, digital storage, battery power, and developments in analytics and ML tools. Connectivity, the essential element of IoT, is becoming ubiquitous: McKinsey estimated that by the end of 2020, 80% of global population had access to 4G coverage and by 2030 90% will have some level of 5G coverage.

However, considerable barriers to the safe and secure use of IoT technology in manufacturing remain and concerted efforts from scientists, governments, industry associations, and other stakeholders are needed to overcome them. These are described in the next sections.

2.4.2. Risks Posed to the Marketplace and Supply Chain

Supply chain and market risk fall into two categories: availability and trustworthiness. Availability risk involves the financial viability of the vendor; the availability of raw or processed materials or people to manufacture and maintain hardware, firmware, and software; and the reliability and resilience of delivery mechanisms to natural catastrophes, human-made events, and economic changes [166]. Trustworthiness risk is the degree of confidence that the item being delivered was built properly and has not been corrupted prior to being received and cannot be corrupted after put into use. Trustworthiness supply chain risks include defective or counterfeit items as well as cybersecurity risks (e.g., baby monitors or smart light bulbs that transmit data to China) [167].

The use of IoT in manufacturing raises a number of security risks due to the complexity of manufacturing facilities. Given the commercial value of industrial data and the possibility of industrial espionage, manufacturing sites are attractive targets for cybercriminals [168]. The generally slow transition from legacy systems to connected machines, sensors, industrial control systems, and IT networks generates a number of difficult-to-resolve cybersecurity issues.

Finally, industrial IoT devices are sourced in different countries and contain many components [169]. Each of these has a supply chain that can be compromised at various points, including by the manufacturer, the software libraries, the shippers, warehousing, and in maintenance and patching after being put into use. Furthermore, it could be difficult to track the origins of the internal elements that comprise IoT devices—a single device may be made from parts supplied by dozens of component manufacturers [170]. Once the industrial IoT environment is breached, it puts control and production systems at risk, and it may take weeks or months before the effects are apparent, and additional time to respond once a vulnerability is localized. Finally, as IoT devices age they may no longer be supported by the original manufacturer and become cybersecurity risks due to an inability to update them. Updates themselves also pose a risk, if the firmware supply chain is corrupted. Updates need to address the changing threat landscape as attack methods also change. Many of these risks are being addressed by the NIST Cybersecurity Supply Chain Risk Management (C-SCRM) efforts [171].

Several challenges must be overcome to address market and supply chain risks of IoT in manufacturing and other sectors [172]. These include (a) understanding trade-offs between security, operational efficiency, and interoperability; (b) managing and implementing security, privacy, and data protection in an integrated manner, with associated third parties across the IoT ecosystems; and (c) resolving legal uncertainty over IoT product and service liability, data protection, and data integrity, especially due to highly complex data flows. Industry bodies and national governments can take several steps to mitigate these risks. One of these is to continue to publicize IoT vulnerabilities listed in the CVE® program, which identifies, defines, and catalogs publicly disclosed cybersecurity vulnerabilities [173]. The Vulnerability Exploitability Exchange is one current approach to this requirement [174]. Creating a standardized process for identification, testing, verification, and ongoing maintenance of devices and products containing IoT, as well as standards for compliance certification, is another potential direction. Finally, smart devices can be rated according to their levels of cybersecurity, which will allow consumers to fully understand the risks and uses of the data collected by products and devices and make informed decisions before purchase [175], although NIST has advised against this approach as being misguided, given the collective risks posed by insecure IoT products, preferring a baseline approach that specifies minimums against broad outcomes.

2.4.3. Risks to the National Security of the United States

As discussed throughout this chapter, IoT and IoT in manufacturing generate risks and can have significant impacts on the national security, including economic security, of the United States. In 2017, GAO published a report on the risks posed by IoT to DOD [176]. GAO concluded that while DOD had issued policies and guidance for personal and infrastructure-related IoT devices, these steps did not address some security risks. Consequently, GAO recommended that DOD perform further risk assessments and update its IoT security strategy.

Recent events have shown the risks posed by IoT devices to U.S. security, including economic security, such as the October 2016 cyberattack with an IoT-based cyber weapon called the *Mirai* botnet [23]. The victim of the attack was a company called Dyn, which controls one of the internet domains. The company remained under attack for most of the day, which brought down Twitter, Netflix, CNN, and many other sites in Europe and the United States. Representatives of Dyn estimated that the attack involved "100,000 malicious endpoints" and was extraordinary in its strength. The U.S. Government responded by issuing E.O. 13800, which directed the Department of Commerce to investigate the threat of botnets [124].

In April 2022, an advisory about a new hacker tool capable of disrupting a wide range of industrial control system equipment was released by Federal agencies.[43] According to one expert, this is the most expansive tool ever identified, which has the capability to "hijack target devices, disrupt or prevent operators from accessing them, permanently brick them, or even use them as a foothold to give hackers access to other parts of an industrial control system network" [177].

Some IoT systems are an especially appealing target because they are not secure but are connected to critical infrastructure [169]. For example, a large retailer can be attacked via a network of connected HVAC systems. The breach is then propagated via internal systems until it reaches the point-of-sale systems resulting in a huge loss of customer data, including credit card information. Manufacturing IoT systems can be hacked to damage equipment, steal information, spy on the environment in which they are installed, and disrupt or interfere with operation or production. Attacks on this sector can be very impactful. For example, the breach of a system that controls a power plant can cause an outage affecting thousands of customers disrupting communication, medical systems, and other emergency services. The increasing automation of sophisticated multi-step cyberattacks combined with the lack of cybersecurity protections, standards, and regulations will likely lead to a growing number of attacks with increasing economic and human costs.

2.4.4. Harms to Rights, Opportunities, and Access to Critical Resources and Services

IoT poses several risks to the American public's rights, opportunities, and access to critical resources and services.

For example, IoT systems take advantage of large amounts of data, in many cases the most sensitive data, such as financial, biometric data, or health information. Consequently, concerns over both privacy and cybersecurity are paramount to users of IoT devices.

Loss of privacy is a significant risk to users. This risk of potential disclosure of sensitive information is shared with non-IoT mobile and communication technologies, but IoT enables "the collection of personal information, habits, locations, and physical conditions over time,

[43] Released by Department of Energy, the Cybersecurity and Infrastructure Security Agency, the National Security Agency, and the Federal Bureau of Investigation: https://www.cisa.gov/uscert/ncas/alerts/aa22-103a

which may allow an entity that has not directly collected sensitive information to infer it" [178]. For example, in theory "smart cities" are the embodiment of futuristic ideal. However, to be successful, today's smart cities not only bring together vast amounts of data about residents, collected continuously and without consent [179]. There is an urgent need to use privacy enhancing technologies (PETs) to minimize the privacy and related security and equity issues arising from current products and implementation choices. If guardrails are not put in place, the public will increasingly lose control over information about their movements, habits, preferences, and daily occupations [180]. Furthermore, increasing use of biometrics combined with IoT systems has untold ramifications for privacy and democracy. To help mitigate these concerns, it will be important to protect consumers from violations of privacy through design choices that ensure such protections are included by default, including ensuring that data collection conforms to reasonable expectations, that only data strictly necessary for the specific context is collected, that users are notified when data is being collected, and that safeguards such as planned discarding of data or client-side-only processing be employed. The burden must fall on companies, not consumers, to minimize data collection. Designers, developers, and deployers of IoT systems should seek consumers' permission and respect consumers' decisions regarding collection, use, access, transfer, and deletion of their data in appropriate ways and to the greatest extent possible; where not possible, alternative privacy by design safeguards should be used.[44]

Finally, while IoT devices generate and collect a wealth of personal data, legal and ethical questions about ownership and retention of these data remain unresolved [63]. Under most current regulatory regimes, data ownership is split between consumers and a data-collecting entity. Consequently, companies that collect data at "smart cities" may soon be able to privatize this information (including personal data), despite not having obtained informed consent from the subjects. Cities should retain rights to the data collected, as well, to ensure public benefit. Consumer data ownership rights will play an essential role in how and to what extent these data can be monetized.

Additionally, cybersecurity threat is of paramount concern to users of IoT devices. While laptops, computers, and smartphones are also subject to cybersecurity risks, vulnerability for IoT devices is higher because they lack the cybersecurity programs and routine security updates used for most computers and smartphones and are generally not actively managed [181].

2.4.5. Emerging Risks and Long-Term Trends in the Marketplace and Supply Chain

Information relevant to this section is covered in 2.4.1. (market overview) and 2.4.2. (risks to the marketplace).

2.5. Recommendations

Review of the literature and conversations with industry experts revealed several challenges that must be addressed to enable safe development and adoption of IoT. This section

[44] Drawn from "Data Privacy" section of *Blueprint for an AI Bill of Rights*, White House Office of Science and Technology Policy, https://www.whitehouse.gov/ostp/ai-bill-of-rights/data-privacy-2/

describes these challenges (which apply to all IoT sectors to various extents) and offers mitigating solutions.

Challenge 1: IoT technologies present significant cybersecurity and privacy risks. Many developers and users of IoT devices may be unaware of these risks or uncertain how to mitigate them or to leverage privacy enhancing technologies.

> **Recommendation 1:** The Federal Government should encourage manufacturers and service providers to anticipate and address potential risks to safety and rights of users during early stages of product development, rather than as add-ons or modifications to a near-final product or as post-market fixes.
>
> **Recommendation 2:** The Federal Government should continue to play a role in educating consumers and businesses about the risks and benefits of IoT; how to safely use IoT devices; and what choices customers have in accepting or rejecting IoT technologies and services.
>
> **Recommendation 3:** The Federal Government should promote the development of technologies and other innovations that would enable customers to easily and effectively control collection, use, access, transfer, and deletion of their data.
>
> **Recommendation 4:** The Federal Government should continue to develop and disseminate flexible frameworks and guidance, so that manufacturers can implement protections for safety and rights that are commensurate with risks posed by their products or services.

Challenge 2: IoT technologies vary significantly in their complexity, type and scope of data collected, and nature of application, which may require different solutions to existing challenges.

> **Recommendation 5:** The Federal Government should continue to encourage the transition to smart manufacturing and other IoT systems in areas that have no ownership, are too risky for commercial investment, have been resistant to solutions, or require coordination across multiple stakeholders.
>
> **Recommendation 6:** The Federal Government should continue to engage with industry consortia, non-profit organizations, and academic institutions to obtain input on its standards development activities and promote awareness among stakeholders.

Challenge 3: The international standards landscape for IoT remains complex and fragmented.

> **Recommendation 7:** The Federal Government should continue to advance work to develop international standards on IoT.

Challenge 4: U.S. competitors are making significant investment in IoT. For example, a recent study concluded that in 2024 China will surpass U.S. to become the largest IoT market.

> **Recommendation 8:** The Federal Government should support IoT research and development projects, innovation hubs, centers of excellence, and testing facilities to ensure that the United States maintains intellectual leadership in this space.

Challenge 5: Small- and medium-sized businesses may be unable or unwilling to commit resources to adopt smart manufacturing technologies.

> **Recommendation 9:** The Federal Government should analyze potential impacts of incentives, such as tax credits, to help small- and medium-sized manufacturers invest in secure but potentially costly IoT technologies.

Challenge 6: A quarter of manufacturers are experiencing shortages of appropriately trained workers (including with expertise to choose data collection and storage technology, application development, data analysis capabilities, and risk mitigation expertise) [165] and this need will only grow as digital transformation continues.

> **Recommendation 10:** The Federal Government should collaborate with industry to define required skills and sponsor programs to help businesses train and retrain workers.

References

[1] Eric Simmon. “Internet of Things (IoT) Component Capability Model for Research Testbed.” NISTIR 8316, 9/2020. https://doi.org/10.6028/NIST.IR.8316.

[2] Oracle. “What Is IoT?.” Accessed June 30, 2022. https://www.oracle.com/internet-of-things/what-is-iot/.

[3] Christopher Greer, Martin Burns, David Wollman, and Edward Griffor. “Cyber-Physical Systems and Internet of Things: NIST Special Publication 1900-202.” Gaithersburg, MD, 2019. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1900-202.pdf.

[4] Andrew Kusiak. “Smart Manufacturing.” *International Journal of Production Research* 56, 1-2 (2018): 508–17. Accessed June 30, 2022. https://doi.org/10.1080/00207543.2017.1351644.

[5] Sunyaev, Ali. *Internet Computing: Principles of Distributed Systems and Emerging Internet-Based Technologies*. Cham, Switzerland: Springer International Publishing, 2020. Accessed June 30, 2022. https://doi.org/10.1007/978-3-030-34957-8.

[6] IBM. “The Little-Known Story of the First IoT Device.” Accessed October 14, 2022. https://www.ibm.com/blogs/industries/little-known-story-first-iot-device/.

[7] Detlef Schoder. “Introduction to the Internet of Things.” In *Internet of Things a to Z: Technologies and Applications*. Edited by Qusay F. Hassan, 3–50. Hoboken New Jersey: John Wiley and Sons Inc, 2018. Accessed June 30, 2022.

[8] Eleven Fifty Academy. “The History of the Internet of Things.” Accessed July 1, 2022. https://elevenfifty.org/blog/the-history-of-the-internet-of-things/.

[9] International Telecommunication Union. “ITU Internet Reports 2005: The Internet of Things.” Accessed July 1, 2022. https://www.itu.int/osg/spu/publications/internetofthings/.

[10] Yurong Chen. “Research on the Connotation and Business Model of Internet of Things Under the Background of Globalization.” *Proceedings of Business and Economic Studies (PBES)* 1, no. 2 (2018). Accessed July 1, 2022. https://doi.org/10.26689/pbes.v1i2.490.

[11] Sudip Phuyal, Diwakar Bista, and Rabindra Bista. “Challenges, Opportunities and Future Directions of Smart Manufacturing: A State of Art Review.” *Sustainable Futures* 2 (2020): 100023. Accessed July 1, 2022. https://doi.org/10.1016/j.sftr.2020.100023.

[12] Worldometer. “World Population Projections.” Accessed July 1, 2022. https://www.worldometers.info/world-population/world-population-projections/.

[13] S4. “S4x22 ICS Security Event.” Accessed July 1, 2022. https://s4xevents.com/.

[14] Beecham Research. “World of IoT Sector Map.” Accessed July 1, 2022. https://www.beechamresearch.com/download-details/world-of-iot-sector-map/.

[15] Hogan, Michael, and Ben Piccarreta. “Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT).” *National Institute of Standards and Technology*, 2018. https://doi.org/10.6028/NIST.IR.8200. https://csrc.nist.gov/publications/detail/nistir/8200/final.

[16] National Institute of Standards and Technology. “Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT):

NISTIR 8200." National Institute of Standards and Technology (NIST), 2018. https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8200.pdf.

[17] Office of Consumer Affairs. "Internet of Things (IoT) Checklist for Consumers." Accessed July 7, 2022. https://ised-isde.canada.ca/site/office-consumer-affairs/en/modern-marketplace/guide-apparel-and-textile-care-symbols/internet-things-iot-checklist-consumers.

[18] Finley Engineering. "IDC Report: IoT Spending to Reach More Than $1 Trillion by 2022." Accessed July 7, 2022. https://finleyusa.com/idc-report-iot-spending-to-reach-more-than-1-trillion-by-2022/.

[19] Fortune Business Insights. "IoT in Manufacturing Market Size, Trends | Global Analysis, 2026." Accessed July 7, 2022. https://www.fortunebusinessinsights.com/industry-reports/internet-of-things-iot-in-manufacturing-market-101677.

[20] Mordor Intelligence. "Internet-of-Things (IoT) Market Size, Growth | 2022 - 27 | Industry Trends." Accessed July 7, 2022. https://mordorintelligence.com/industry-reports/internet-of-things-in-manufacturing-market.

[21] Zhengxin Wang, Minghuan Shou, Shuai Wang, Ruinan Dai, and Keqian Wang. "An Empirical Study on the Key Factors of Intelligent Upgrade of Small and Medium-Sized Enterprises in China." 3, Sustainability, 2019. https://doi.org/10.3390/su11030619.

[22] James Manyika, Michael Chui, Peter Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin, and Dan Aharon. "The Internet of Things: Mapping the Value Beyond the Hype: McKinsey Global Institute." Journal of Data Analysis and Information Processing, 2015. https://www.mckinsey.com/~/media/mckinsey/industries/technology%20media%20and%20telecommunications/high%20tech/our%20insights/the%20internet%20of%20things%20the%20value%20of%20digitizing%20the%20physical%20world/unlocking_the_potential_of_the_internet_of_things_executive_summary.pdf.

[23] Nicky Woolf. "DDoS Attack That Disrupted Internet Was Largest of Its Kind in History, Experts Say." *The Guardian*, October 26, 2016. Accessed June 30, 2022. https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

[24] Greig, Jonathan. "Google Says It Stopped the Largest DDoS Attack Ever Recorded in June." *The Record by Recorded Future*, August 19, 2022. https://therecord.media/google-says-it-stopped-the-largest-ddos-attack-ever-recorded-in-june/.

[25] Yoachimik, Omer. "Cloudflare Mitigates 26 Million Request Per Second DDoS Attack." *The Cloudflare Blog*, June 14, 2022. https://blog.cloudflare.com/26m-rps-ddos/.

[26] Yoachimik, Omer. "Cloudflare Blocks 15M Rps HTTPS DDoS Attack." *The Cloudflare Blog*, April 27, 2022. https://blog.cloudflare.com/15m-rps-ddos-attack/.

[27] Deloitte. "Cybersecurity for Smart Factories in the Manufacturing Industry." Accessed October 14, 2022. https://www2.deloitte.com/us/en/pages/energy-and-resources/articles/smart-factory-cybersecurity-manufacturing-industry.html.

[28] Fahed Alkhabbas, Romina Spalazzese, and Paul Davidsson. "Characterizing Internet of Things Systems Through Taxonomies: A Systematic Mapping Study." *Internet of*

Things 7 (2019): 100084. Accessed July 1, 2022. https://doi.org/10.1016/j.iot.2019.100084.

[29] Beecham Research. “World of IoT Sector Map - Beecham Research.” Accessed July 18, 2022. https://www.beechamresearch.com/download-details/world-of-iot-sector-map/.

[30] Sakovich, Natallia. “IoT in Manufacturing: Ultimate Guide and Use Cases.” *SaM Solutions*, July 2, 2021. Accessed July 1, 2022. https://www.sam-solutions.com/blog/iot-in-smart-manufacturing/.

[31] United States General Accounting Office. “Public-Private Partnerships: Key Elements of Federal Building and Facility Partnerships.” Report to the Honorable Stephen Horn Committee on Government Reform House of Representatives, United States General Accounting Office (GAO), Washington, D.C., 02/1999. https://www.gao.gov/assets/ggd-99-23.pdf.

[32] U.S. Department of Homeland Security. “AEP Overview and Documents.” Accessed July 1, 2022. https://www.dhs.gov/publication/aep-overview-and-documents.

[33] Manufacturing USA. “Manufacturing USA.” Accessed July 1, 2022. https://www.manufacturingusa.com/.

[34] Clean Energy, Smart Manufacturing, Innovation Institute. “CESMII – the Smart Manufacturing Institute.” Accessed July 1, 2022. https://www.cesmii.org/.

[35] The Cybersecurity Manufacturing Innovation Institute. “Cyber Innovation to Secure U.S. Manufacturing.” Accessed October 13, 2022. https://cymanii.org/.

[36] Council on Competitiveness. “Smart Manufacturing: Leveraging the Democratization of Innovation.” Accessed July 1, 2022. https://compete.secure.nonprofitsoapbox.com/programs/compete-energy-manufacturing/smart-manufacturing-emcp.

[37] National Institute of Standards and Technology. “Manufacturing Extension Partnership (MEP) | NIST.” Accessed June 30, 2022. https://www.nist.gov/mep.

[38] Next Generation IoT. “Standardization Bodies.” Accessed July 1, 2022. https://www.ngiot.eu/standardization-bodies/.

[39] Industry IoT Consortium. “The Industrial Internet of Things Connectivity Framework - Industry IoT Consortium.” Accessed July 1, 2022. https://www.iiconsortium.org/iicf/.

[40] Rajive Joshi, Paul Didier, Christer Holmberg, Jaime Jimenez, and Timothy Carey. “The Industrial Internet of Things Connectivity Framework: An Industry IoT Consortium Foundational Document.” Industry IoT Consortium, n.d. https://www.iiconsortium.org/wp-content/uploads/sites/2/2022/06/IIoT-Connectivity-Framework-2022-06-08.pdf.

[41] Consumer Technology Association. “Home.” Accessed July 1, 2022. https://www.cta.tech/.

[42] Connectivity Standards Alliance. “CSA-IOT.” Accessed November 16, 2022. https://csa-iot.org/.

[43] ioXt. “About the IoXt Alliance: The Global Standard for IoT Security.” Accessed July 1, 2022. https://www.ioxtalliance.org/about-ioxt.

[44] CIO Wiki. “Standard.” https://cio-wiki.org/wiki/Standard.

[45] International Organization for Standardization. “ISO - International Organization for Standardization.” Accessed July 1, 2022. https://www.iso.org/home.html.

[46] European Telecommunications Standards Institute. “ETSI - Welcome to the World of Standards!.” Accessed July 1, 2022. https://www.etsi.org/.

[47] CEN-CENELEC. “CEN-CENELEC.” Accessed July 1, 2022. https://www.cencenelec.eu/areas-of-work/cenelec-sectors/digital-society-cenelec/emerging-technologies/.

[48] American National Standards Institute. “ANSI Home.” Accessed July 1, 2022. https://www.ansi.org/.

[49] American National Standards Institute. “ANSI Introduction.” Accessed July 7, 2022. https://www.ansi.org/about/introduction.

[50] Institute of Electrical and Electronics Engineers. “IEEE: The World's Largest Technical Professional Organization Dedicated to Advancing Technology for the Benefit of Humanity.” Accessed July 1, 2022. https://www.ieee.org/.

[51] Livable Software. “The Role of Foundations in Open Source Projects - Livable Software.” Accessed July 1, 2022. https://livablesoftware.com/study-open-source-foundations/.

[52] Linux Foundation. “Linux Foundation - Decentralized Innovation, Built with Trust.” Accessed July 1, 2022. https://www.linuxfoundation.org/.

[53] The Apache Software Foundation. “Welcome to the Apache Software Foundation!.” Accessed July 1, 2022. https://www.apache.org/.

[54] Eclipse Foundation. “The Eclipse Foundation.” Accessed July 1, 2022. https://www.eclipse.org/org/foundation/.

[55] Linux Foundation. “Explore Full Catalog - Training.” https://training.linuxfoundation.org/full-catalog/?_sft_topic_area=embedded-development.

[56] Internet Interdisciplinary Institute. “Research Lines - SOM Research Lab.” Accessed July 1, 2022. https://som-research.uoc.edu/research-lines/.

[57] Linux Foundation. “Open Manufacturing Platform.” Accessed July 1, 2022. https://open-manufacturing.org/.

[58] IoT Security Foundation. “Secure IoT – IoT Security Foundation.” Accessed July 1, 2022. https://www.iotsecurityfoundation.org/best-practice-guidelines/.

[59] IoT Security Foundation. “IoT Security Foundation – the Global Home of IoT Cybersecurity.” Accessed July 1, 2022. https://www.iotsecurityfoundation.org/.

[60] European Telecommunications Standards Institute. “SmartM2M; IoT Standards Landscape and Future Evolutions.” TR 103 375 - V1.1.1. https://www.etsi.org/deliver/etsi_tr/103300_103399/103375/01.01.01_60/tr_103375v010101p.pdf.

[61] The Economist Intelligence Unit. “The IoT Business Index 2020: A Step Change in Adoption.” 2020. https://armkeil.blob.core.windows.net/developer/Files/pdf/report/economist-iot-business-index-2020-arm.pdf.

[62] U.S. Government Accountability Office. “Internet of Things: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD.” GAO-17-668, 2017. https://www.gao.gov/assets/gao-17-668.pdf.

[63] Jessica Groopman. "IoT Data Privacy Forces Organizations to Rethink Data Ownership." *TechTarget*, September 24, 2019. Accessed July 7, 2022. https://www.techtarget.com/iotagenda/tip/IoT-data-privacy-forces-organizations-to-rethink-data-ownership.

[64] U.S. Access Board. "Home." https://www.access-board.gov/.

[65] National Institute of Standards and Technology. "Cybersecurity | NIST." Accessed July 1, 2022. https://www.nist.gov/cybersecurity.

[66] National Institute of Standards and Technology. "NIST Computer Security Resource Center | CSRC." Accessed July 1, 2022. https://csrc.nist.gov/.

[67] National Institute of Standards and Technology. "NIST Cybersecurity for IoT Program | NIST." Accessed July 1, 2022. https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program.

[68] IoT Cybersecurity Improvement Act of 2020. H.R.1668. U.S. Congress. Accessed July 5, 2022. https://www.congress.gov/bill/116th-congress/house-bill/1668.

[69] Cybersecurity & Infrastructure Security Agency. "ABOUT CISA | CISA." Accessed July 5, 2022. https://www.cisa.gov/about-cisa.

[70] Chief Information Officers Council. "Home: Welcome to CIO.Gov!." Accessed December 20, 2021. https://www.cio.gov/.

[71] National Security Agency. "Quantum Computing and Post-Quantum Cryptography: Frequently Asked Questions." 2021. https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/1/Quantum_FAQs_20210804.PDF.

[72] Committee on National Security Systems. "Use of Public Standards for Secure Information Sharing." 2016. https://imlive.s3.amazonaws.com/Federal%20Government/ID151830346965529215587195222610265670631/CNSSP15.pdf.

[73] Department of Defense. "Department of Defense Instruction: Cybersecurity." NUMBER 8500.01, May 14, 2014. https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodi/850001_2014.pdf.

[74] U.S. Cyber Command. "Mission and Vision." Accessed July 5, 2022. https://www.cybercom.mil/About/Mission-and-Vision/.

[75] U.S. Cyber Command. "Technical Challenge Problem Set 2020." 2020. https://www.cybercom.mil/Portals/56/Documents/2020%20Tech%20Challenge%20Problems%20UNCLASS%20CAO-PAO%20FINAL.pdf.

[76] Federal Risk and Authorization Management Program. "Program Basics | FedRAMP.Gov." Accessed July 5, 2022. https://www.fedramp.gov/program-basics/.

[77] Department of Defense, and Defense Information Systems Agency. "Department of Defense Cloud Computing Security Requirements Guide: Version 1, Release 4." 2022.

[78] Federal Communications Commission. "Spectrum Requirements for the Internet of Things Notice of Inquiry." Accessed July 5, 2022. https://www.fcc.gov/document/spectrum-requirements-internet-things-notice-inquiry.

[79] 47 U.S. Code § 927 - Existing allocation and transfer authority retained*.* 47 USC 927. U.S. Congress. July 5, 2022. Accessed July 5, 2022.

https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title47-section927&num=0&edition=prelim.

[80] Interagency Task Force on Electronics Stewardship. “National Strategy for Electronics Stewardship, July 2011.” June 20, 2011. https://www.epa.gov/sites/default/files/2015-09/documents/national_strategy_for_electronic_stewardship_0.pdf.

[81] U.S. Environmental Protection Agency. “Electronic Product Environmental Assessment Tool (EPEAT) | US EPA.” Accessed July 5, 2022. https://www.epa.gov/greenerproducts/electronic-product-environmental-assessment-tool-epeat.

[82] U.S. Department of Labor. “About OSHA | Occupational Safety and Health Administration.” Accessed July 5, 2022. https://www.osha.gov/aboutosha.

[83] Centers for Disease Control and Prevention. “About NIOSH | NIOSH | CDC.” Accessed July 5, 2022. https://www.cdc.gov/niosh/about/default.html.

[84] Centers for Disease Control and Prevention. “Direct Reading and Sensor Technologies | NIOSH | CDC.” Accessed July 5, 2022. https://www.cdc.gov/niosh/topics/drst/default.html.

[85] U.S. Department of Labor. “List of Goods Produced by Child Labor or Forced Labor.” https://www.dol.gov/agencies/ilab/reports/child-labor/list-of-goods.

[86] Federal Trade Commission. “Federal Trade Commission.” Accessed July 5, 2022. https://www.ftc.gov/.

[87] Federal Trade Commission. “Privacy and Security Enforcement.” Accessed July 5, 2022. https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement.

[88] U.S. Consumer Product Safety Commission. “About Us.” Accessed August 30, 2022. https://www.cpsc.gov/About-CPSC.

[89] Consumer Product Safety Commission. “Status Report on the Internet of Things (IoT) And Consumer Product Safety.” September 25, 2019. https://www.cpsc.gov/s3fs-public/Status-Report-to-the-Commission-on-the-Internet-of-Things-and-Consumer-Product-Safety.pdf.

[90] Executive Order on Improving the Nation's Cybersecurity. EO 14028. Executive Office of the President. May 12, 2021. Accessed July 5, 2022. https://www.govinfo.gov/content/pkg/FR-2021-05-17/pdf/2021-10460.pdf.

[91] Executive Office of the President. “Executive Order on America's Supply Chains: A Year of Action and Progress.” 2022. https://www.whitehouse.gov/wp-content/uploads/2022/02/Capstone-Report-Biden.pdf.

[92] Murugiah Souppaya, Karen Scarfone, and Donna Dodson. “Secure Software Development Framework (SSDF) Version 1.1:: Recommendations for Mitigating the Risk of Software Vulnerabilities.” NIST Special Publication 800-218, 2022. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf.

[93] National Institute of Standards and Technology. “Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e.” February 4, 2022. https://www.nist.gov/system/files/documents/2022/02/04/software-supply-chain-security-guidance-under-EO-14028-section-4e.pdf.

[94] National Telecommunications and Information Administration. “NTIA Releases Minimum Elements for a Software Bill of Materials | National Telecommunications

and Information Administration." Accessed July 5, 2022. https://www.ntia.doc.gov/blog/2021/ntia-releases-minimum-elements-software-bill-materials.

[95] National Institute of Standards and Technology. "Definition of Critical Software Under Executive Order (EO) 14028." October 13, 2021. https://www.nist.gov/system/files/documents/2021/10/13/EO%20Critical%20FINAL.pdf.

[96] Executive Office of the President. "Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth: 100-Day Reviews Under Executive Order 14017." The White House, Washington DC, June 2021. https://www.whitehouse.gov/wp-content/uploads/2021/06/100-day-supply-chain-review-report.pdf.

[97] Department of Energy. "Biden-Harris Administration Announces $156 Million for America's First-of-a-Kind Critical Minerals Refinery." https://www.energy.gov/articles/biden-harris-administration-announces-156-million-americas-first-kind-critical-minerals.

[98] U.S. Food and Drug Administration. "Overview of Device Regulation." Accessed July 5, 2022. https://www.fda.gov/medical-devices/device-advice-comprehensive-regulatory-assistance/overview-device-regulation.

[99] U.S. Food and Drug Administration. "Medical Device Safety Action Plan: Protecting Patients, Promoting Public Health." *FDA*, January 4, 2021. Accessed July 5, 2022. https://www.fda.gov/about-fda/cdrh-reports/medical-device-safety-action-plan-protecting-patients-promoting-public-health.

[100] U.S. Government Accountability Office. "Federal Buildings: GSA Should Establish Goals and Performance Measures to Manage the Smart Buildings Program." GAO-18-200, 2018. https://www.gao.gov/assets/gao-18-200.pdf.

[101] U.S. Federal Aviation Administration. "Certificated Remote Pilots Including Commercial Operators." Accessed July 5, 2022. https://www.faa.gov/uas/commercial_operators.

[102] Infrastructure Investment and Jobs Act. H.R3684. U.S. Congress. 2022. Accessed July 5, 2022. https://www.congress.gov/bill/117th-congress/house-bill/3684/text.

[103] U.S. Department of Agriculture. "FarmBeats: Ag at the Speed of IT." Accessed July 5, 2022. https://www.usda.gov/media/blog/2021/09/30/farmbeats-ag-speed-it.

[104] Federal Energy Regulatory Commission. "Cyber and Grid Security." Accessed July 5, 2022. https://www.ferc.gov/industries-data/electric/industry-activities/cyber-and-grid-security.

[105] National Cybersecurity Center of Excellence. "Mission & Vision | NCCoE." Accessed July 5, 2022. https://www.nccoe.nist.gov/our-approach/mission-vision.

[106] National Institute of Standards and Technology. "National Online Informative References Program: Computer Security Resource Center." Accessed November 16, 2022. https://csrc.nist.gov/projects/olir.

[107] Industry IoT Consortium. "About Us - Industry IoT Consortium." Accessed July 5, 2022. https://www.iiconsortium.org/about-us/.

[108] Sven Schrecker, Hamed Soroush, Jesus Molina, Frederick Hirsch, Jean Pierre Leblanc, Marcellus Buchheit, and Andrew Ginter et al. "Industrial Internet of

Things Volume G4: Security Framework." 2015. https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf.

[109] Cloud Security Alliance. "Home | CSA." Accessed July 5, 2022. https://cloudsecurityalliance.org/.

[110] Cloud Security Alliance. "Internet of Things Working Group | CSA." Accessed July 5, 2022. https://cloudsecurityalliance.org/research/working-groups/internet-of-things/.

[111] Cloud Security Alliance. "Cybersecurity Best Practices for the Manufacturing Industry." February 9, 2022. https://cloudsecurityalliance.org/artifacts/manufacturing-industry-cybersecurity-challenges/.

[112] Small Business Innovation Research. "Award Data | SBIR.Gov." Accessed July 5, 2022. https://www.sbir.gov/sbirsearch/award/all.

[113] Michael Fagan, Jeffrey Marron, Kevin G. Brady, JR., Barbara B. Cuthill, Katerina N. Megas, and Rebecca Herold. "IoT Non-Technical Supporting Capability Core Baseline: NISTIR 8259B." 2021. https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8259B.pdf.

[114] Baksh, Mariam. "White House's Internet of Things Security Initiative Gets an Official Meeting Date." *Nextgov*, October 12, 2022. https://www.nextgov.com/cybersecurity/2022/10/white-houses-internet-things-security-initiative-gets-official-meeting-date/378354/.

[115] Federal Register. "Telecommunications Interagency Working Group (TIWG)." Accessed July 5, 2022. https://www.federalregister.gov/documents/2021/12/21/2021-27755/telecommunications-interagency-working-group-tiwg.

[116] William M. (Mac) Thronberry National Defense Authorization Act for Fiscal Year 2021. Public Law 116-283. U.S. Congress. Accessed July 5, 2022. https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf.

[117] Federal Register. "Establishment and Call for Nominations to Serve on the Internet of Things Advisory Board." Accessed July 5, 2022. https://www.federalregister.gov/documents/2022/01/13/2022-00419/establishment-and-call-for-nominations-to-serve-on-the-internet-of-things-advisory-board.

[118] National Institute of Standards and Technology. "Workforce Framework for Cybersecurity (NICE Framework): NIST Special Publication 800-181 Revision 1." 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf.

[119] Tzafestas, Spyros. "Ethics and Law in the Internet of Things World." *Smart Cities* 1, no. 1 (2018): 98–120. https://doi.org/10.3390/smartcities1010006. https://www.mdpi.com/2624-6511/1/1/6.

[120] Deborah George. "IoT Manufacturers – What You Need to Know About California's IoT Law." *The National Law Review*, January 28, 2020. Accessed July 5, 2022. https://www.natlawreview.com/article/iot-manufacturers-what-you-need-to-know-about-california-s-iot-law.

[121] Deborah George. "Oregon's New IoT Law." *The National Law Review*, January 3, 2019. Accessed July 5, 2022. https://www.natlawreview.com/article/oregon-s-new-iot-

law#:~:text=Oregon's%20New%20IoT%20Law&text=Oregon%20became%20the%20latest%20state,Bill%202395%20amending%20ORS%20646.607.

[122] Bureau of Justice Assistance, and U.S. Department of Justice. "Electronic Communications Privacy Act of 1986 (ECPA) | Bureau of Justice Assistance." Accessed July 5, 2022. https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285.

[123] U.S. Department of Justice. "Privacy Act of 1974." Accessed July 5, 2022. https://www.justice.gov/opcl/privacy-act-1974.

[124] Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. EO 13800. Executive Office of the President. May 11, 2017. Accessed October 11, 2022. https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure.

[125] National Defense Authorization Act for Fiscal Year 2020. Public Law 116-92. U.S. Congress. 2019. Accessed July 5, 2022. https://www.congress.gov/116/plaws/publ92/PLAW-116publ92.pdf.

[126] Infrastructure Investment and Jobs Act. Public Law 117-58. U.S. Congress. Accessed July 5, 2022. https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf.

[127] Michael Fagan, Katerina Megas, Karen Scarfone, and Matthew Smith. "Foundational Cybersecurity Activities for IoT Device Manufacturers." Gaithersburg, MD, 2020. https://csrc.nist.gov/publications/detail/nistir/8259/final.

[128] National Institute of Standards and Technology. "NISTIR 8259 Series | NIST." Accessed July 5, 2022. https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/nistir-8259-series.

[129] National Institute of Standards and Technology. "NIST Releases Draft Guidance on Internet of Things Device Cybersecurity." Accessed July 5, 2022. https://www.nist.gov/news-events/news/2020/12/nist-releases-draft-guidance-internet-things-device-cybersecurity#:~:text=%E2%80%9CWe%20help%20a%20manufacturer%20start,where%20things%20are%20still%20developing.%E2%80%9D.

[130] National Institute of Standards and Technology. "Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software | NIST." Accessed July 5, 2022. https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/cybersecurity-labeling-consumers-0.

[131] Katie Boeckl, Michael Fagan, William Fisher, Naomi Lefkovitz, Katerina N. Megas, Ellen Nadeau, Danna Gabel O'Rourke, Ben Piccarreta, and Karen Scarfone. "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks: NISTIR 8228." 2019. https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf.

[132] Michael Fagan, Jeffrey Marron, Kevin G. Brady, JR., Barbara B. Cuthill, Katerina N. Megas, Rebecca Herold, David Lemire, and Brad Hoehn. "IoT Device Cybersecurity Guidance for the Federal Government: NIST Special Publication 800-213." 2021. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-213.pdf.

[133] Michael Fagan, Katerina N. Megas, Jeffrey Marron, Kevin G. Brady, JR., Barbara B. Cuthill, Rebecca Herold, David Lemire, and Brad Hoehn. "IoT Device Cybersecurity Guidance for the Federal Government: NIST Special Publication 800-213A." 2021. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-213A.pdf.

[134] Cuthill, Barbara. "Profile of the IoT Core Baseline for Consumer IoT Products." *National Institute of Standards and Technology*, 2022; NISTIR 8425. https://doi.org/10.6028/NIST.IR.8425. https://csrc.nist.gov/publications/detail/nistir/8425/final.

[135] U.S. Government Accountability Office. "Internet of Things: Information on Use by Federal Agencies." Accessed July 5, 2022. https://www.gao.gov/products/gao-20-577.

[136] U.S. Department of Homeland Security. "Strategic Principles for Securing the Internet of Things (IoT)." Washington, D.C., 2016. https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf.

[137] U.S. Department of Homeland Security, and Cybersecurity & Infrastructure Security Agency. "Internet of Things Acquisition Guidance: Information Technology Sector." n.d. https://www.cisa.gov/sites/default/files/publications/20_0204_cisa_sed_internet_of_things_acquisition_guidance_final_508_1.pdf.

[138] National Telecommunications and Information Administration. "Internet of Things." Accessed July 5, 2022. https://www.ntia.doc.gov/category/internet-things.

[139] European Commission. "H2020 Work Programme 2014-2015 ICT-30-2015: Internet of Things and Platforms for Connected Smart Objects Duration: 24 Months Supporting Internet of Things Activities on Innovation Ecosystems: IoT Standards Landscape." Deliverable 05.01, February 8, 2017. https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5b04ab182&appId=PPGMS.

[140] International Organization for Standardization. "ISO/IEC 29161:2016." Accessed July 7, 2022. https://www.iso.org/standard/45240.html.

[141] International Organization for Standardization. "ISO/IEC 20924:2021." Accessed July 7, 2022. https://www.iso.org/standard/82771.html.

[142] International Organization for Standardization. "ISO/IEC 21823-2:2020." Accessed July 7, 2022. https://www.iso.org/standard/80986.html.

[143] International Organization for Standardization. "ISO/IEC TR 30164:2020." Accessed July 7, 2022. https://www.iso.org/standard/53284.html.

[144] International Organization for Standardization. "ISO/IEC TR 30166:2020." Accessed July 7, 2022. https://www.iso.org/standard/53286.html.

[145] International Organization for Standardization. "ISO/IEC 30141:2018." Accessed July 7, 2022. https://www.iso.org/standard/65695.html.

[146] IEEE Standards Association. "IEEE SA - IEEE Standard for an Architectural Framework for the Internet of Things (IoT)." Accessed July 7, 2022. https://standards.ieee.org/ieee/2413/6226/.

[147] Consumer Technology Association. "Consumer Technology Association: R14WG1 - CTA-2088-A, Baseline Cybersecurity Standard for Devices and Device Systems."

Accessed October 11, 2022. https://standards.cta.tech/apps/group_public/project/details.php?project_id=677.

[148] IEEE Standards Association. "IEEE SA - Standard for Harmonization of Internet of Things (IoT) Devices and Systems." Accessed July 7, 2022. https://standards.ieee.org/ieee/1451.99/10355/.

[149] International Telecommunication Union. "ITU-T Work Programme: [2022-2024] [SG20] [Q2/20]." Accessed July 7, 2022. https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=17949.

[150] European Telecommunications Standards Institute. "CYBER: Cyber Security for Consumer Internet of Things: Baseline Requirements: ETSI EN 303 645." n.d. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.00_30/en_303645v020100v.pdf.

[151] Connectivity Standards Alliance. "Matter Arrives Bringing a More Interoperable, Simple and Secure Internet of Things to Life." Accessed November 16, 2022. https://csa-iot.org/newsroom/matter-arrives/.

[152] Irina Brass, Leonie Tanczer, Madeline Carr, Miles Elsden, and Jason Blackstock, eds. *Standardising a Moving Target: The Development and Evolution of IoT Security Standards: 28-29 March 2018*. Stevenage, UK: IET, 2018. http://ieeexplore.ieee.org/servlet/opac?punumber=8358783.

[153] Claude Baudoin, Erin Bournival, and Erich Clauer. "Global Industry Standards for Industrial IoT." An Industrial Internet Consortium White Paper. https://www.iiconsortium.org/pdf/IIC_Global_Standards_Strategy_Whitepaper.pdf.

[154] National Institute of Standards and Technology. "Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products." National Institute of Standards and Technology (NIST), Gaithersburg, MD, February 4, 2022. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf.

[155] National Institute of Standards and Technology. "Report for the Assistant to the President for National Security Affairs (APNSA) On Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software." National Institute of Standards and Technology (NIST), May 10, 2022. https://www.nist.gov/system/files/documents/2022/05/24/Cybersecurity%20Labeling%20for%20Consumers%20under%20Executive%20Order%2014028%20on%20Improving%20the%20Nation%27s%20Cybersecurity%20Report%20%28FINAL%29.pdf.

[156] Federal Trade Commission. "Careful Connections: Building Security in the Internet of Things." n.d. https://www.ftc.gov/system/files/documents/plain-language/913a_careful_connections.pdf.

[157] IoT Security Foundation. "Consumer IoT Guidance – IoT Security Foundation." Accessed July 7, 2022. https://www.iotsecurityfoundation.org/consumer-iot/.

[158] IANS. "China to Surpass US to Become Worlds Largest IoT Market in 2024: Report." *Business Standard*, January 17, 2021. Accessed November 16, 2022. https://www.business-standard.com/article/international/china-to-surpass-us-to-become-world-s-largest-iot-market-in-2024-report-121011700382_1.html.

[159] Verified Market Research. "IoT in Manufacturing Market Size and Forecast." Accessed July 7, 2022. https://www.verifiedmarketresearch.com/product/iot-in-manufacturing-market/.

[160] The Business Research Company. "IoT in Manufacturing Global Market Report 2021: COVID-19 Growth and Change to 2030." Accessed July 7, 2022. https://www.reportlinker.com/p06151604/IoT-in-Manufacturing-Global-Market-Report-COVID-19-Growth-And-Change-To.html?utm_source=GNW.

[161] Markets and Markets. "Smart Factory Market Size & Share | Industry Report, 2021-2026 | MarketsandMarkets™." Accessed July 7, 2022. https://www.marketsandmarkets.com/Market-Reports/smart-factory-market-1227.html.

[162] Philipp Wegner. "Global IoT Spending to Grow 24% in 2021, Led by Investments in IoT Software and IoT Security." *IoT Analytics GmbH*, June 16, 2021. Accessed July 7, 2022. https://iot-analytics.com/2021-global-iot-spending-grow-24-percent/.

[163] Michael Chui, Mark Collins, and Mark Patel. "IoT Value Set to Accelerate Through 2030: Where and How to Capture It." November 8, 2021. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/iot-value-set-to-accelerate-through-2030-where-and-how-to-capture-it.

[164] Michael Chui, Mark Collins, and Mark Patel. "The Internet of Things: Catching up to an Accelerating Opportunity." 11/2021. Accessed July 7, 2022. https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/iot%20value%20set%20to%20accelerate%20through%202030%20where%20and%20how%20to%20capture%20it/the-internet-of-things-catching-up-to-an-accelerating-opportunity-final.pdf.

[165] Industrial Distribution. "Survey: Industrial IoT Involvement a Must for Industrial Manufacturers." *Industrial Distribution*, July 26, 2017. Accessed July 7, 2022. https://www.inddist.com/home/article/13774434/survey-industrial-iot-involvement-a-must-for-industrial-manufacturers.

[166] Massachusetts Institute of Technology, and MIT Center for Transportation & Logistics. "3 Types of Risk That Will Impact Supply Chains in 2018." Accessed July 7, 2022. https://ctl.mit.edu/news/3-types-risk-will-impact-supply-chains-2018.

[167] Nat Meysenburg. "How Secure Is a Smart Baby Monitor? Finding Out Is Far Too Difficult." *Tech Policy Press*, March 4, 2021. Accessed July 7, 2022. https://techpolicy.press/how-secure-is-a-smart-baby-monitor-finding-out-is-far-too-difficult/.

[168] UL Solutions. "Leveraging Cybersecurity for Industry 4.0 into a Business Advantage." Accessed July 7, 2022. https://www.ul.com/insights/leveraging-cybersecurity-industry-40-business-advantage.

[169] Mario Ayala, Rob Cantu, Richard Holder, Jeff Huegel, Niten Malik, Michalina M, Adrienne Raglin, Ashley Reichert, Kimberley Sanders, and Ash M. Richter. "The Industrial Internet of Things (IIoT): Opportunities, Risks, Mitigation." 2019. https://www.dhs.gov/sites/default/files/publications/ia/ia_iiot-intercommections.pdf.

[170] Rich Castagna. "IoT Supply Chain Vulnerability Poses Threat to IIoT Security." *IoT World Today*, February 1, 2021. Accessed July 7, 2022. https://www.iotworldtoday.com/2021/02/01/iot-supply-chain-vulnerability-poses-threat-to-iiot-security/.

[171] National Institute of Standards and Technology. "Cybersecurity Supply Chain Risk Management | CSRC." Computer Security Resource Center. Accessed

November 16, 2022. https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management.

[172] Irina Brass, Kruakae Pothong, and Mariyam Hasham. “Navigating and Informing the Internet of Things (IoT) Standards Landscape: A Guide for SMEs and Start-Ups.” 04/2019. https://www.researchgate.net/publication/335176530_Navigating_and_Informing_the_Internet_of_Things_IoT_Standards_Landscape_A_Guide_for_SMEs_and_Start-ups.

[173] Mitre. “CVE - CVE.” Accessed July 7, 2022. https://cve.mitre.org/.

[174] National Telecommunications and Information Administration. “Sharing and Exchanging SBOMs.” July 6, 2020. https://www.ntia.doc.gov/files/ntia/publications/ntia_sbom_framing_sharing_july9.pdf.

[175] Markets and Markets. “IIoT Platform Market Size, Share and Global Market Forecast to 2026.” Accessed July 7, 2022. https://www.marketsandmarkets.com/Market-Reports/industrial-iot-platform-market-11186318.html.

[176] U.S. Government Accountability Office. “GAO-17-668, Internet of Things: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD.” https://www.gao.gov/assets/gao-17-668.pdf.

[177] Andy Greenberg. “Pipedream Malware: Feds Uncover 'Swiss Army Knife' for Industrial System Hacking.” *WIRED*, April 13, 2022. Accessed July 7, 2022. https://www.wired.com/story/pipedream-ics-malware/.

[178] Federal Trade Commission. “Internet of Things: Privacy & Security in a Connected World.” 01/2015. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[179] Emilie Scott. “The Trouble with Informed Consent in Smart Cities.” *International Association of Privacy Professionals*, February 28, 2019. Accessed July 7, 2022. https://iapp.org/news/a/the-trouble-with-informed-consent-in-smart-cities/.

[180] Ryan Johnston. “Digital Privacy Concerns Will Follow Sidewalk Labs to Next Venture, Says Former Consultant.” *StateScoop*, May 27, 2020. Accessed July 7, 2022.

[181] Jordan M. Buckwald, and Gary E. Marchant. “Improving Soft Law Governance of the Internet of Things: IEEE.” 12/2021. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9639442&tag=1.

Appendix D. Abbreviations

ACT-IAC	American Council for Technology and Industry Advisory Council
ADS	Automated Driving System
AEP	Analytic Exchange Program
AFNOR	French Standardization Association
AI	Artificial Intelligence
AIOTI	Alliance for Internet of Things Innovation
BSI	British Standards Institute
CAN	Controller Area Network
CCI	Control Correlation Identifier
CDRH	Center for Devices and Radiological Health
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CEPT	Conference of Postal and Telecommunications Administrations
CESMII	Clean Energy Smart Manufacturing Innovation Institute
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CISA	Cybersecurity and Infrastructure Security Agency
CLS	Cybersecurity Labeling Scheme
CNCF	Cloud Native Computing Foundation
CNI	Container Network Initiative
CNSS	Committee on National Security Systems
CPSC	Consumer Product Safety Commission
CSA	Cloud Security Alliance
CSCRM	Cybersecurity Supply Chain Risk Management
CSS	Central Security Service
CTIA	Cellular Telecommunications and Internet Association
CYManII	Cybersecurity Manufacturing Innovation Institute
DDoS	Distributed Denial-of-Service
DDS	Data-Distribution Service for Real-Time Systems
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DOC	Department of Commerce
DoD	Department of Defense
DOE	Department of Energy
DOI	Department of the Interior
DOT	Department of Transportation
EO	Executive Order
EPA	Environmental Protection Agency
EPEAT	Electronic Product Environmental Assessment Tool
ESO	European Standards Organization
ETSI	European Telecommunications Standards Institute
FAA	Federal Aviation Administration
FAIR	Findable, Accessible, Interoperable, and Reusable

FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FDA	Food and Drug Administration
FDD	Fault detection and diagnostics
FERC	Federal Energy Regulatory Commission
FMVSS	Federal Motor Vehicle Safety Standards
FTC	Federal Trade Commission
GAO	Government Accountability Office
GSA	General Services Administration
GSMA	Groupe Speciale Mobile Association
HR	House Resolution
HVAC	Heating, Ventilation, and Air Conditioning
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IIC	Industry IoT Consortium
IIoT	Industrial Internet of Things
IoT	Internet of Things
IoTSF	IoT Security Foundation
ISA	International Society of Automation
ISO	International Organization for Standardization
ITU	International Telecommunication Union
ITU-T	ITU’s Telecommunication Standardization Sector
IWG	Interagency Working Group
JTC	Joint Technical Committee
M2M	Machine-to-Machine
ML	Machine Learning
MQTT	Message Queuing Telemetry Transport
NCCoE	National Cybersecurity Center of Excellence
NCDRST	NIOSH Center for Direct Reading and Sensor Technologies
NEMA	National Electrical Manufacturers Association
NERC	North American Electric Reliability Corporation
NETT	Non-Traditional and Emerging Transportation Technology
NHTSA	National Highway Traffic Safety Administration
NIOSH	National Institute for Occupational Safety and Health
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Reports
NSS	National Security System
NSA	National Security Agency
NTIA	National Telecommunications and Information Administration
OASIS	Organization for the Advancement of Structured Information Standards
OCF	Open Connectivity Foundation

OCI	Open Container Initiative
OGC	Open Geospatial Consortium
OLIR	NIST National Online Informative References Program
OMB	U.S. Office of Management and Budget
OMG	Object Management Group
OMP	Open Manufacturing Platform
OOIE	Open Industrial Interoperability Ecosystem
OSF	Open Source Foundation
OSGi	Open Services Gateway initiative
OSHA	Occupational Safety and Health Administration
OWASP	Open Web Application Security Project
OWL	Web Ontology Language
PBS	Public Buildings Service
PETRAS	Privacy, Ethics, Trust, Reliability, Acceptability, and Security
PKI	Public Key Infrastructure
POSC	Petroleum Open Standards Consortium
PPP	Public-Private Partnership
PSA	Platform Security Architecture
RDF	Resource Description Framework
RFC	Request for Comments
RFI	Request for Information
RMF	Risk Management Framework
SB	Smart Building
SBIR	Small Business Innovation Research
SBOM	Software Bill of Materials
SENSR	Simple Electronic Notation for Sensor Reporting
SDO	Standards Development Organization
SP	Special Publication
SRG	Security Requirements Guide
STIG	Security Technical Implementation Guide
STPI	Science and Technology Policy Institute
STTR	Small Business Technology Transfer
SVIP	Silicon Valley Innovation Program
SysML	Systems Modeling Language
TR	Technical Report
UA	Unified Architecture
UAS	Unmanned Aircraft System
UML	Unified Modeling Language
USA	United States of America
USDA	U.S. Department of Agriculture
USGS	United States Geological Survey
VA	Department of Veterans Affairs
VDE	Association for Electrical, Electronic & Information Technologies
VDI	Association of German Engineers

VDMA	Mechanical Engineering Industry Association
W3C	World Wide Web Consortium
WG	Working Group
ZVEI	German Electrical and Electronic Manufacturers Association

Appendix E. World of IoT

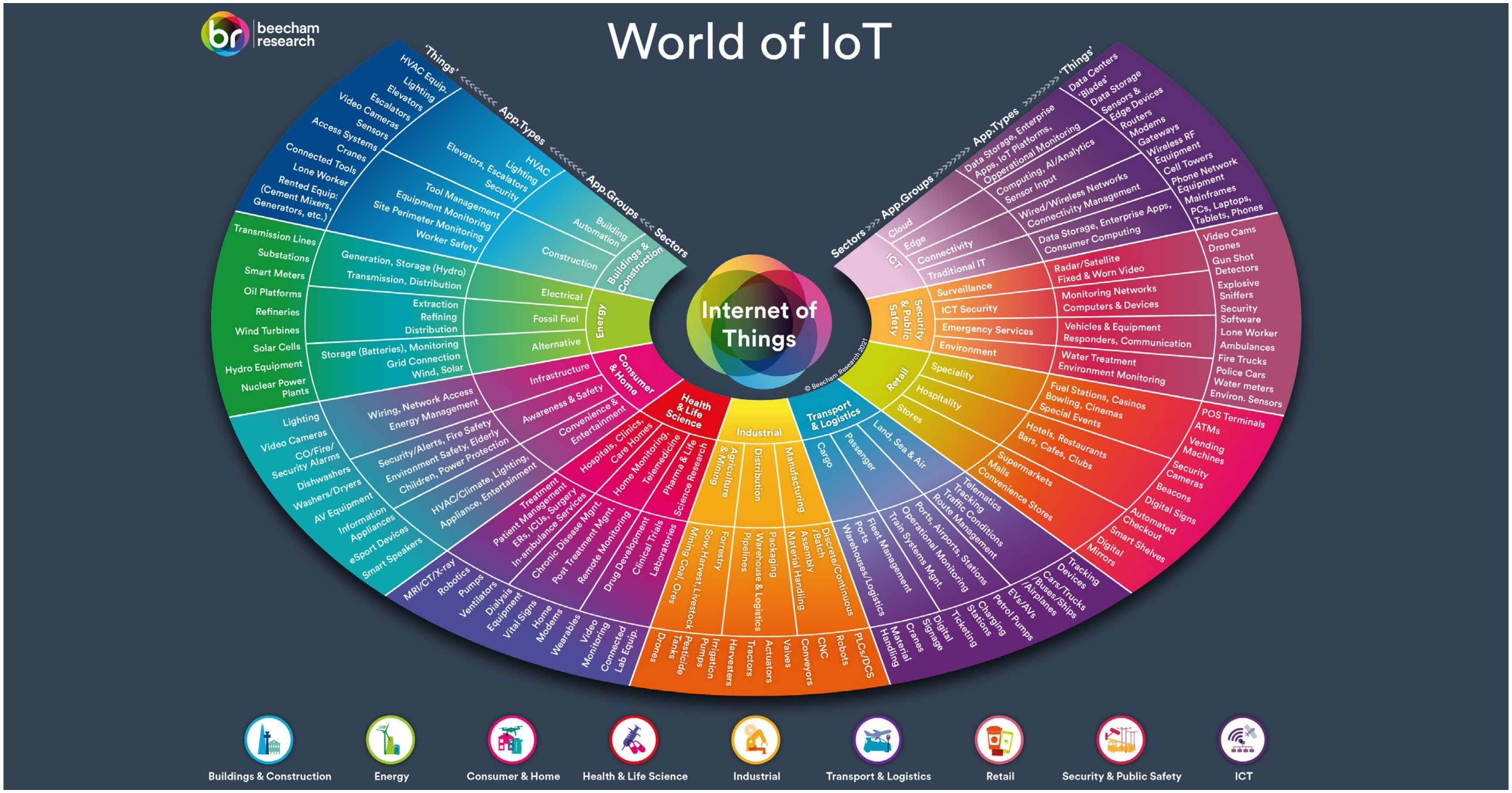


Figure 2. World of IoT [4]

Appendix F. Additional Organizations Involved in IoT

Note: Some of the organizations are included in Table 12 and Table 13.

Table 12. Industry Consortia and Associations

Organization and Website	Focus
China Alliance of Industrial Internet (AII) en.aii-alliance.org (not secure)	AII supports the transformation and upgrading of the advanced manufacturing industry in China and abroad [1].
Alliance for IoT Innovation (AIOTI) aioti.eu/	AIOTI seeks to lead in IoT and edge computing research, standardization, and ecosystem building. The goal of AIOTI is the creation of a dynamic European IoT ecosystem to support competitiveness of Europe [2].
ANT+ Alliance (ANT+) thisisant.com/	The ANT+ Alliance is a leader in low power sensor technology. It facilitates interoperability between devices using the ANT protocol [3].
America Makes americamakes.us/	America Makes, founded in 2012, is a public-private partnership for additive manufacturing. It is the DoD's national manufacturing innovation institute and part of the Manufacturing USA network [4].
Avnu Alliance avnu.org/	The Avnu Alliance is creating an interoperable ecosystem for applications with precise timing and low latency requirements using open standards through certification [5].
Bitkom bitkom.org/EN	Bitkom, founded in 1999, is Germany's digital association, representing more than 2,000 companies. Bitkom advocates the digitization of the economy, the society, and public administration [6].
CESMII, the Smart Manufacturing Institute cesmii.org/	CESMII, a program at the University of California, Los Angeles (UCLA), was created in 2016 with Department of Energy funding to drive Smart Manufacturing, which is "the ultimate solution to deliver performance, productivity, agility, continuous Innovation, and the cleanest energy of all, the energy that was not used in production, wasted with scrap or during periods of inefficient operation." [7].
CAN in Automation (CiA) can-cia.org/	CiA is an international users' and manufacturers' group for future developments of the CAN (Controller Area Network) standards and technology [8].
Eclipse IoT iot.eclipse.org/	The Eclipse Foundation, created in 2004 as an independent not-for-profit corporation to provide stewardship of IBM's Eclipse Project, is now home to

Organization and Website	Focus
	over 350 open-source projects, including several Eclipse IoT projects [9; 10].
Energistics www.energistics.org/	Energistics is an open consortium for the oil and gas industry to define, develop, and maintain standards. It seeks to ensure a rapid and effective adoption of standards in the pursuit of interoperability, efficiency, and data integrity [11].
Industry IoT Consortium (IIC) iiconsortium.org/	IIC, formerly the Industrial Internet Consortium, serves industry, organizations, and society by building a foundation for trustworthy Industrial IoT. It is a program of the Object Management Group (OMG) [12].
Learning System Platform plattform-lernende-systeme.de/startseite.html	The Learning System Platform is a network of experts on artificial intelligence. Launched in 2017 by the German Federal Ministry of Education and Research, its goal is to serve as an independent broker, to promote interdisciplinary exchange and social dialogue on artificial intelligence [13].
LonMark International (LonMark) lonmark.org/	The purpose of LonMark is to promote and advance the efficient and effective integration of open, multi-vendor control systems using ISO/IEC 14908-1 and related standards [14].
NAMUR, the User Association of Automation Technology in Process Industries	NAMUR, established in 1949, is an international association of over 150 user companies and represents their interests in automation technology [15].
Open Connectivity Foundation (OCF) openconnectivity.org/	The OCF developed the OCF specification to address secure interoperability—to enable connected devices to discover one another and to communicate, regardless of manufacturer, operating system, chipset, or physical transport. OCF manages a certification program, aimed at ensuring that OCF-certified products can communicate. OCF is the former OIC (Open Interconnect Consortium) [16].
Open Geospatial Consortium (OGC) ogc.org	The OGC is an international consortium of more than 500 businesses, government agencies, research organizations, and universities whose mission is to make geospatial information and services FAIR—findable, accessible, interoperable, and reusable [17].
Organization for the Advancement of Structure Information Standards	OASIS is a non-profit, international consortium that promotes industry consensus and produces worldwide standards for machine-to-machine (M2M), IoT, cloud computing, security, privacy, content technologies,

Organization and Website	Focus
(OASIS) www.oasis-open.org	business transactions, emergency management, and other applications. The Message Queuing Telemetry Transport (MQTT) is OASIS standard for IoT [18].
OPC Foundation (OPC) www.opcfoundation.org	The OPC Foundation, founded in 1996, manages a global organization that creates and maintains OPC-branded data transfer standards for multi-vendor, multi-platform, secure and reliable interoperability in industrial automation [19].
OSGi Working Group osgi.org/	The OSGi Working Group, derived from the former OSGi Alliance, manages the OSGi Specification Project, an open-source initiative, which is now a project within the Eclipse Foundation [20].
Privacy, Ethics, Trust, Reliability, Acceptability, And Security National Center of Excellence (PETRAS) petras-iot.org/	PETRAS, a consortium of 22 research institutions in the United Kingdom, seeks to ensure that technological advances in IoT are developed and applied safely and securely in consumer and business contexts. It considers social and technical issues relating to the cybersecurity of IoT devices, systems, and networks [21].
Plattform Industrie 4.0 plattform-i40.de/IP/Navigation/EN/Home/home.html	The Plattform Industrie 4.0 is led by the German Government and supported by the associations Bitkom, VDMA, and ZVEI. The goal is to secure and expand Germany's leading position in the manufacturing industry by taking on the challenges of the fourth industrial revolution and to drive national and international exchanges in information technology security and standardization [22].
Secure Technology Alliance securetechalliance.org/	The Secure Technology Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, and widespread application of secure solutions, including smart cards, embedded chip technology, and related hardware and software to promote technologies for authentication, commerce, and IoT. The Secure Technology Alliance was previously the Smart Card Alliance [23].
Association for Electrical, Electronic & Information Technologies (VDE) vde.com/en	VDE, one of the largest technology organizations in Europe, has stood for innovation and technological progress for more than 125 years. It combines science, standardization, testing, certification, and application consulting [24].
Association of German Engineers (VDI) vdi.de/en/home	VDI has been supporting, advancing, and representing engineers in their work for more than 160 years. VDI provides them with a professional base and maintains a

Organization and Website	Focus
	lively network at regional, national, and international levels [25].
Association for Mechanical Engineering Industry (VDMA) vdma.org/en/	VDMA has more than 3,400 member companies in the mechanical and plant engineering industry in Germany and Europe. It represents the common economic, technical, and scientific interests of the industry [26].
World Wide Web Consortium Web of Things (W3C WoT) Interest Group w3.org/WoT/ig/	The W3C WoT Working Group addresses the fragmentation of the IoT through standard complementing building blocks, such as metadata and application program interfaces that facilitate integration across IoT platforms and application domains [27]. The W3C WoT Interest Group supports the Working Group by organizing and running interoperability and testing events, conducting outreach, developing supporting materials, and exploring new ideas [28].
German Electro and Digital Industry Association (ZVEI) zvei.org/en/	ZVEI is a leading manufacturers' association in Germany. It represents the interests of its 1,600-member companies with a wide and dynamic product portfolio. ZVEI is committed to the common interests of the electro and digital industry in Germany and at the international level [29].

Table 13. Standards Developing Organizations

Organization and Website	Focus
The American National Standards Institute (ANSI) https://www.ansi.org/	A private, non-profit organization that administers and coordinates the U.S. voluntary standards and conformity assessment system [30]. In 2018, it partnered with NIST to release "IoT-Enabled Smart City Framework."
French Standards Association (AFNOR) https://www.afnor.org/	AFNOR acts as a central oversight body for standardization in France, identifying standardization needs, and mobilizing interested parties [31]. France's new standardization, launched in 2019, has several focus areas related to IoT [32].
British Standards Institute (BSI) https://www.bsigroup.com/	BSI is the United Kingdom's national standards organization. The BSI IoT/1 Committee addresses horizontal standardization issues on IoT privacy, security, safety, and interoperability [33].
The European Committee for Standardization (CEN) and The European Committee for Electrotechnical	CEN and CENELEC, along with ETSI, have been officially recognized by the European Union and the European Free Trade Association as being responsible

Organization and Website	Focus
Standardization (CENELEC) www.cencenelec.eu/	for developing and defining voluntary standards at the European level [34].
German Institute for Standardization (DIN) www.din.de/en	DIN, founded in 1917, supports standardization in Germany and worldwide. In 1975, it entered a public-private partnership with the German Federal Republic in which DIN is acknowledged as the sole national standards body in Germany [35].
German Electrotechnical Standards Board (DKE) www.dke.de/en	DKE, a non-profit organization, is a joint organization of DIN and the Association for Electrical, Electronic & Information Technologies (VDE). It is responsible for the creation and maintenance of standards and safety specifications for electrical engineering, electronics, and information technology in Germany [36].
ECLASS Association www.eclass.eu/en	ECLASS is an international standard for uniform and consistent classification and description of products, materials, systems, and services. The ECLASS Association is a non-profit organization which defines and further develops and spreads this standard without consideration of sector borders [37].
European Telecommunications Standards Institute (ETSI) www.etsi.org	ETSI is a regional standards body dealing with telecommunications, broadcasting, and other electronic communications networks and services. ETSI, together with CEN and CENELEC, has its standards recognized as European standards [38]. ETSI is involved in standardizing a wide range of IoT components, including machine-to-machine communications, semantic interoperability, and information management protocols [39].
International Electrotechnical Commission (IEC) www.iec.ch	IEC is a global, not-for-profit organization, founded in 1906, that prepares and publishes international standards for all electrical, electronic, and related technologies [40]. In 2017, ISO/IEC Joint Technical 1 launched Subcommittee 41 on Internet of Things and Digital Twins [41].
Institute of Electrical and Electronics Engineers Standards Association (IEEE SA) standards.ieee.org	IEEE SA is the standards-making body of the IEEE. It is a consensus building organization that facilitates standards development and standards-related collaboration [42]. IEEE has many ongoing activities in IoT [43].
Internet Engineering Task Force (IETF) www.ietf.org	IETF is a large, open, international community of network designers, operators, vendors, and researchers that develops and maintains internet standards [44]. Several IETF Working Groups are developing protocols

Organization and Website	Focus
	and best common practices that are directly relevant to the communication and security aspects of IoT [45].
International Society of Automation (ISA) www.isa.org	ISA is a non-profit association of engineers, technicians, and managers providing foundational standards-based technical resources for industrial automation [46]. The ISA-95 Committee is evolving to support smart manufacturing and the IIoT [47].
International Organization for Standardization (ISO) www.iso.org	ISO is an independent, non-governmental international organization with 167 national standards bodies as members. It brings together experts to develop voluntary, consensus-based, market-relevant International Standards that support innovation and provide solutions to global challenges [48]. In 2017, ISO/IEC Joint Technical 1 launched Subcommittee 41 on Internet of Things and Digital Twins [41]. In 2018, ISO and IEC published ISO/IEC 30141:2018, Internet of Things (loT) — Reference Architecture [49].
International Telecommunication Union (ITU) www.itu.in	ITU, founded in 1865 to facilitate international connectivity in communications networks, allocates global radio spectrum and satellite orbits, develops the technical standards that ensure networks and technologies seamlessly interconnect, and strives to improve access to ICTs to underserved communities. ITU Study Group 20, Internet of things (IoT) and smart cities and communities (SC&C), has an active work program [50], including "Requirements and framework of Industrial IoT (IIoT) infrastructure for smart manufacturing." [51].
Object Management Group (OMG) www.omg.org	The mission of OMG is to develop technology standards that provide real-world value for vertical industries and, importantly, to revise these standards as technologies change throughout the years [52]. It has a number of IoT-related standards [53]. OMG also lists the Digital Twin Consortium and the Industry IoT Consortium (IIC) as managed programs [54].
oneM2M www.onem2m.org	oneM2M, launched in 2012, develops open and accessible IoT standards to enable interoperable, secure, and simple-to-deploy services for the IoT ecosystem [55].
OPC Foundation (OPC) www.opcfoundation.org	The OPC Foundation, founded in 1996, manages a global organization that creates and maintains OPC-branded data transfer standards for multi-vendor, multi-platform,

Organization and Website	Focus
	secure and reliable interoperability in industrial automation [19].
The American National Standards Institute (ANSI) https://www.ansi.org/	A private, non-profit organization that administers and coordinates the U.S. voluntary standards and conformity assessment system [30]. In 2018, it partnered with NIST to release “IoT-Enabled Smart City Framework.”
Organization for the Advancement of Structure Information Standards (OASIS) www.oasis-open.org	OASIS is a non-profit, international consortium that promotes industry consensus and produces worldwide standards for machine-to-machine (M2M), IoT, cloud computing, security, privacy, content technologies, business transactions, emergency management, and other applications. The Message Queuing Telemetry Transport (MQTT) is OASIS standard for IoT [18].

Appendix G. Mandatory or Voluntary Standards Technology Design Considerations

Operating Systems [56]

Most modern IoT systems use standard operating systems; frequently using open-source Linux, often stripped down to better leverage resource constrained environments.

Data Management

Relational data management standards are well established but new areas of focus, such as machine learning (ML) and data analytics, require the development of new structures specifically developed for these disciplines. Ontologies and knowledge graphs reflected in standards such as RDF (Resource Description Framework) [57], OWL (Web Ontology Language) [58], or SPARQL [59] (RDF database query language) are key methods of knowledge representation. As required capabilities progress from mere storage and retrieval of data to understanding data, standards are evolving for semantic building blocks in the specific context of various industries, based on these languages. These standards include business vocabularies and modeling such as ISO 15000-5:2014 [60] and the Unified Modeling Language (UML) [61]. Essential data quality standards include industrial data standards, ISO TC 184/SC 4 [62] on industrial data, as well as the ISO 8000 data quality standards [63]. Working groups addressing product characteristics, industrial data quality, digital manufacturing, and covering the oil/gas/process/power industries, extend the SC 4 standards effort.

Information Exchange

There are multiple competing data communications standards covering many potential interoperable implementations to provide reliable and secure real-time data communication. Determining which of these protocols is preferable can be challenging, even if the decision is based on specific system requirements, and may require involvement in the corresponding organizations to maintain currency. Current widely adopted standards for IoT system component communications include MQTT (Message Queuing Telemetry Transport) [64], adopted as ISO/International Electrotechnical Commission (IEC) 20922, developed by OASIS; OPC/UA [65] (Open Platform Communications Unified Architecture), standardized as IEC 62541, developed by the OPC Foundation, and DDS, an Object Management Group [54] (OMG) standard. OMG also developed the SENSR (Simple Electronic Notation for Sensor Reporting) [66] standard, adopted in 2019, to standardize the format of the information that flows from sensors to systems.

Systems Modeling and Interoperability

Systems Modeling Language (SysML) v2 [67], an update to SySML will add modeling extensions to expand the already well supported language, that was itself based on UML. The Open Industrial Interoperability Ecosystem (OOIE) [68], tightly coupled to the ISO 15926 standard, developed by the MIMOSA industry association, is one effort to address investment intensive systems with long operational lives such as energy production facilities. The longevity of these installations requires capture of design, build, and maintenance documentation that may only exist in paper format if at all.

Cloud Deployment Technologies

Risk of vendor lock-in will drive employment of cloud portability, interoperability, and orchestration standards such as those developed by the Kubernetes project [69] or the Open Container Initiative (OCI), the Cloud Native Computing Foundation (CNCF), and the Container Network Interface (CNI) project promoted by the Linux foundation [70]. CSA's Matter standard is designed to help.

Security

IoT system security is fundamentally the same as non-IoT system security and subject to the same standards and approaches. For example, Public Key Infrastructure (PKI) derived from IETF Request for Comments (RFCs) 2510 and 2511 [71], used for authentication of devices and encryption of data traffic, is directly applicable to IoT devices, including sensors. Since many IoT devices and interconnects are in non-physically isolated and unprotected environments, this technical control becomes essential. Other standards such as the security extensions for information exchange protocols are equally necessary. Larger frameworks such as the Risk Management Framework (RMF) [72], the Open Web Application Security Project (OWASP) [73], and recommendations by the Cloud Security Alliance (CSA) [74] provide useful guidance that cuts across industry sectors.

Artificial Intelligence and Machine Learning

AI/ML will be central to a truly automated and autonomous IIoT, even if the preferred model is one employing human-in-the-loop oversight. While penetration of AI/ML into certain spaces has a high demand signal for the benefits it may bring, there are few published standards and none have been widely adopted. However, the need for standards is underlined by studies of current inherent weakness or "brittleness" of AI/ML. Standards organizations are starting to focus on aspects of AI/ML. In 2019, OMG formed an Artificial Intelligence Platform Task Force [75] to address the overall lack of standards. The ISO subcommittee on AI, ISO/IEC JTC 1/SC 42 [76], began work on evaluation of AI trustworthiness in 2020, after previously working to develop a big data reference model. Standards for "ethical AI" are also being pursued by organizations, including a scorecard developed by the American Council for Technology and Industry Advisory Council (ACT-IAC) [77]. Areas of concern for developing standards under the OMG effort are metadata for training data sets, a standard format for the exchange of classifier data, neural network sensitivity metrics, and explainable AI. One shared concern across the AI/ML and IoT communities is the fear that overly strict or prescriptive standards could stifle innovation, maturation, and progress in commercialization of these nascent domains.

Quantum Computing

Chapter Contents

List of Tables

List of Figures

3. Quantum Computing

Summary

In the Consolidated Appropriations Act of 2021, Congress tasked the National Institute of Standards and Technology (NIST) to prepare a series of studies on critical and emerging technologies, including quantum computing (QC), and their impact on the U.S. economy [1]. This chapter addresses:

- industry sectors that implement and promote the use of QC,
- public-private partnerships (PPPs) focused on promoting adoption of QC,
- industry-based bodies developing and issuing standards for QC,
- the status of mandatory and voluntary QC standards, both Federal and industry-based,
- Federal agencies with expertise and jurisdiction in industry sectors implementing QC,
- interagency activities relevant to QC,
- Federal regulations, guidelines, mandatory standards, voluntary standards, and other policies concerning QC implemented by Federal agencies and industry-based bodies,
- Federal resources that exist for consumers and small businesses to evaluate the use of QC,
- risks to the QC supply chain and marketplace,
- QC-related risks to the national security, including economic security,[45] of the United States, and
- emerging risks and long-term trends in QC.

This section provides a high-level overview of these topics, which are discussed in more detail in Sections 3.2 through 3.5 of this chapter.

3.1. Overview

QC, first conceptualized in the 1980s, is a fundamentally different approach to information processing that leverages phenomena from quantum mechanics, such as superposition and entanglement. In theory, QC could be markedly faster than today's "classical" computing for

[45] The Consolidated Appropriations Act of 2021 refers to "economic and national security," and economic security is understood to be part of national security for the purposes of authorities such as the Consolidated Appropriations Act of 2021 and Section 232 of the Trade Expansion Act of 1962 (Public Law 87-794).

certain tasks; realizing this “quantum advantage” for practical tasks remains a major challenge for scientists and engineers.

Early-stage quantum computers have been built based on a variety of different quantum hardware platforms. These early systems are driving numerous innovative research, development, startups, investment, and business activities—leading to new discoveries and application ideas. However, these systems are still at low levels of technological maturity—namely, they are relatively unstable and have not yet demonstrated scalability. Competitive commercial applications have not yet been implemented, and it is not yet clear when or whether they will emerge—though the pace of scientific progress in this field has recently accelerated. Despite this uncertainty, the potential for large-scale QC to be transformative if realized—along with the frontier nature of the underlying science and engineering—make QC R&D and security risk mitigation important national priorities. While substantial scientific and engineering breakthroughs will be needed for QCs to achieve their full potential, the volume of research and pace of discovery have accelerated in recent years.

In 2018, Congress passed the National Quantum Initiative Act (NQIA) to codify a coordinated Federal effort to support and advance Quantum Information Science (QIS) R&D through strategic investments, partnerships, and coordination across Federal agencies. Currently, the QC industry comprises companies conducting R&D on QC hardware, software, and applications; integrating QC system components; providing cloud-based access to experimental QC hardware and software; simulating QC on classical systems; and working toward business and industrial applications. It includes a few large, established technology companies and system integrators; cloud service providers; consultants and potential end-user companies; and numerous small businesses and startup companies. Access to early-stage QC systems for experimentation and testing is now commonly provided via the cloud. Given the early stages of technology development, the market has not consolidated around a single, “winning” QC platform or firm, and this may never happen. Several or a hybrid combination of technologies could prove viable—and the industry may evolve in several directions as QC technology advances. QC R&D has also stimulated advances in classical computing methods, such as “quantum-inspired” approaches that work analogously to QCs, and by stimulating competition between quantum and classical computer scientists vying for increasingly efficient algorithms.

3.1.1. Industry Sectors and Public-Private Partnerships

Both those working to develop QC technologies and potential end-users are actively working to identify and elucidate commercial use cases for QC in the near and long term. While information technology is considered general-purpose, QCs are not expected to offer improvements for all types of computations. However, it is not yet clear for which computations or in which areas QCs will provide an advantage—QCs could potentially be useful for many industry sectors. Preliminary findings from the Quantum Economic Development Consortium (QED-C) Technical Advisory Committee on Use Cases suggest that the most common areas in which applications are being pursued include advanced materials, life sciences, pharmaceuticals, chemicals, automotive (manufacturing/logistics), and finance. Individuals and companies in industry sectors ranging from aerospace to pharmaceuticals have begun exploring how QC could affect their business via writings, events, R&D, and consultations. Much of this effort is motivated by a desire to reduce time-consuming trial and error processes in product development. QC is indirectly disrupting the cybersecurity industry by driving a transition to post-quantum cryptography—new cryptographic protocols expected to be resistant to potential future QC-based attacks.

Multisector activities that leverage Federal funding or other resources to advance QC can broadly be considered PPPs. The QED-C, launched by NIST in 2018 as part of the National Quantum Initiative (NQI) and managed by SRI International with NIST funding under an Other Transaction Authority (OTA) agreement, is working to support the emerging QIS and QC industries by facilitating community development and collaboration among industry, academic, and government stakeholders; conducting studies and road mapping exercises; and providing a broad industry perspective to the U.S. Government [2]. In addition, NIST has long been a leader in QC (and other quantum technology research), and can leverage cooperative research and development agreements (CRADAs) and other types of agreements to partner with outside researchers. NIST also participates as a partner in several research institutes: JILA with the University of Colorado; the Joint Quantum Institute (JQI) with the University of Maryland (UMD) and the Laboratory for Physical Sciences (LPS); the Joint Center for Quantum Information and Computer Science with UMD.

Given the technological maturity level of QC, partnerships generally focus on multi-sector R&D collaborations, including those at National Science Foundation (NSF) and the Department of Energy (DOE) research centers that were explicitly authorized in the NQIA. In alignment with this authority, in 2020 and 2021, NSF announced five Quantum Leap Challenge Institutes each to be funded at $25M over 5 years to advance the QIS fields, three of which are focused on QC; each is a multi-organization collaboration and most have or are establishing partnerships with industry. In 2020, DOE announced the establishment of five National QIS Research Centers to be funded at up to $115M each by FY2025; the centers and National Labs engage industry and other partners in a variety of ways, including as research collaborators and via QED-C. DOE offers CRADAs, Strategic Partnership Projects (SPPs), Agreements for Commercializing Technology (ACTs), and Technical Assistance to facilitate collaboration with the DOE National Labs.

The Department of Defense's (DoD) Quantum Information Science Research Centers—at the Air Force Research Laboratory, the Naval Research Laboratory, and LPS—also comprise or engage in partnerships. For example, the nonprofit Innovare Advancement Center was established by the U.S. Air Force, the Griffiss Institute, Oneida County, and the State University of New York. LPS is a partner in the JQI and currently seeking partners for its Qubit Collaboratory.

In 2020, the White House Office of Science and Technology Policy (OSTP) and NSF launched the multisector National Q-12 Education Partnership to harness QIS-relevant education opportunities at the K-12 level. International efforts across Europe, Asia, and Australia have also established PPPs for QIS alongside national initiatives or coordinated efforts.

3.1.2. Industry-Based Standards

Since 2018, international standard development organizations (SDOs) have begun to work on—but have not yet published—standards for QC, including terms and definitions and standards for quantum simulation, QC architecture, quantum algorithm design and development, and QC benchmarking, as well as a standardization roadmap. Entities involved in this work include working groups within QED-C, the Institute for Electrical and Electronics Engineers, the Joint Technical Committee 1 of the International Organization for Standardization and the International Electrotechnical Commission, and the European Committee for Electrotechnical Standardization. In additional to formal standards, companies, consortia, and researchers have established informal or ad-hoc standards to support their R&D and system benchmarking that may be adopted more broadly as convenient or valuable conventions. Several private sector and academic organizations are actively working to develop quantitative benchmarks for measuring progress in QC and for estimating hardware requirements for achieving them under the Defense Advanced Research Projects Agency's (DARPA) Quantum Benchmarking Program.

3.1.3. Federal Government Standards and Regulations

Today no formal standards or comprehensive regulatory framework exist for QC technologies, though existing authorities to regulate industries that adopt QC could be applicable. Most Federal activities have focused on approaches to support QC R&D or to address the potential security risks QCs pose should a QC capable of practical cryptanalysis be built. NIST is conducting a years-long process to identify QC-resistant (or "post-quantum") cryptography systems; an initial set of algorithms were selected in July of 2022 and final standards are anticipated in 2024. Several National Security Memoranda and an Executive Order direct Federal agencies to assess potential QC risk or develop post-quantum resilience in agency and other information technology systems. Another Executive Order reconstituted the National Quantum Initiative Advisory Committee under the current Administration as a Presidential advisory committee.

3.1.4. Interagency Coordination

Interagency coordination of QIS is overseen by the National Quantum Coordination Office within OSTP, and the National Science and Technology Council (NSTC) Subcommittees on Quantum Information Science (SCQIS) and Economic and Security Implications of Quantum Science (ESIX), along with several interagency working groups. These entities convene multisector events and interagency meetings that help raise awareness about, coordinate, and implement the NQI. They also produce reports to support this coordination and augment the 2018 National Strategic Overview for QIS; other strategic documents pertaining to the QIS workforce, quantum sensing, and quantum networking; and an annual report on the NQI Supplement to the President's Budget. The website quantum.gov is a clearinghouse for these and other reports and information for the public about the NQI.

3.1.5. Federal Government Resources

In addition to the reports and other information available to the public at quantum.gov, Federal Government resources have supported testbeds (research infrastructure for experimenting with technologies) that can be helpful for evaluating the use of early-stage QCs and seeking practical and commercial applications. For example, the Quantum

Computer User Program at Oak Ridge National Laboratory enables researchers to apply for time on commercial QC systems and access them via the cloud. Since 2017, DOE's Advanced Scientific Computing Research program funded two quantum testbeds, enabling researchers to experiment with two different types of QC technologies hosted at the labs. Furthermore, as part of the 2022 CHIPS and Science Act (P.L. 117-167), the Quantum User Expansion for Science and Technology (QUEST) was authorized at approximately $166M over 5 years to provide users with access to QC hardware and cloud services. JILA, NIST, and Google also collaborated to create the Boulder Cryogenic Quantum Testbed in which researchers may test their superconducting microwave resonators. In 2021, LPS established a foundry service for gate-based superconducting quantum computing technologies to enable researchers to overcome the high barrier to entry associated with device fabrication.

3.1.6. Risks to the QC Supply Chain and Marketplace

While there are publicly traded QC companies, and more than a billion dollars in venture capital funding, the industry is nascent. Much of the associated market activity focuses on R&D for building and scaling QC systems, experimentation with early-stage QC technologies, and evaluating potential commercial applications. The QC supply chain includes all materials, components, hardware, software, and support technologies required to research, develop, build, and operate QC technologies; it overlaps substantially with the QIS and broader physics R&D supply chain. Each technical approach to QC hardware often utilizes a few suppliers, many of which are small companies, and many of which are headquartered overseas. Given the early stages of QC technologies and the variety of QC hardware implementations being pursued, demand for QC components is currently too low to establish a robust, scalable QC supply chain. Difficulty in finding needed components with the correct specifications poses challenges to developers and system integrators and may impede progress in establishing a market. For the QC components used in other industries, the QC industry share of demand is likely too low to drive suppliers' production. QC developers often have unique component specification requirements. Before components are used, QC developers often expend substantial resources conducting their own tests of component performance. Some QC systems include a variety of government-designated critical minerals, specialized isotopes, or otherwise hard-to-acquire materials. Given uncertainty about which QC technologies will prove commercially successful, it is currently unclear which materials will be most in demand from the future QC industry. As with all U.S. industries, it will be necessary to ensure due diligence in mitigating risks of forced labor, child labor, and other labor abuse in the QC supply chain.

Many QC companies have expressed concern about the current and future workforce supply. The QC industry requires workers with a range of physical science, engineering, and other technical backgrounds at the PhD, master's, and bachelor's levels. Today, most QC-specific curricula exist only at the graduate level although efforts have recently emerged to develop curricula to help build QIS-relevant skills and knowledge across all educational levels. QIS is a highly interdisciplinary field that crosses these traditional academic boundaries. This is a challenge for higher education curriculum developers and often requires new collaborations between different academic departments. Key academic fields of importance to QC include physics, electrical engineering, computer science, materials science, chemistry, and mathematics. An insufficient supply of individuals with these backgrounds or with QC-specific expertise could limit development of the U.S. QIS industry. In recent years, a large share of the U.S. doctoral degrees in these fields have been awarded to international students (with U.S. temporary resident status), of whom remain to live and work in the United States and play an important role in the U.S. QIS industry. New graduates may stay temporarily through a 1–3-year Optional Practical Training (OPT) program or an approved temporary employment petition. The process of obtaining a visa for longer-term work can be complicated and time-consuming.

Large amounts of venture capital have gone to QC startups in the past decade. However, several large companies in established technology industries are also making substantial investments in QC. It is unclear whether private risk capital will be available in quantities sufficient to support small-companies' participation and competitiveness in the industry over time. Furthermore, funding decisions present opportunity costs across the range of potentially successful QC technologies; concentration of investment in a subset of potential approaches to QC may limit funds to pursue other areas. Regardless of technology type, and despite rapid technical advancements, levels of QC technological readiness are relatively low, and sustained investment in R&D over many years—including basic research—will likely be needed to develop QC technologies and enable commercialization. Inflated expectations for the technology in its early stages of development could result in a funding decline for QC R&D, which would risk a loss of momentum for longer-term progress. The nascent QC industry is underpinned by the discovery and innovation in the open research landscape.

3.1.7. Risks to the National Security, Including Economic Security, of the United States

As with science and technology writ large and the economy, in general, the QC ecosystem is global and involves international R&D collaborations and supply chains. Biased standards, unstable or untrusted supply chains and industry base, or undue influence on nature of QC technology development would threaten the security of U.S. QC developers and the United States' overall competitiveness in QC. These risks can be mitigated through leadership in QC technology development from countries with strong democratic values, ensuring that technology standards are created in a fair and equitable way, and that QC components are cutting edge and readily available from trusted partners. While the United States has long been a leader in QC R&D, the field has become more internationally competitive in recent years.

QCs are expected to be dual-use technologies, meaning that certain future uses of QCs could pose security risks in the hands of bad actors. The best-known example for QC is the technology's potential to be used for cryptanalysis, which could break the public key cryptography currently used to protect communications and secure access to critical infrastructures. Given that some data, such as trade secrets, remain sensitive long after they are created, transmitted, or stored, the encryption used today should remain strong for decades to protect against future exploitation. Thus, identification and deployment of post-quantum, or "quantum-safe," cryptography will be needed well in advance of the realization of a QC capable of practical cryptanalysis, a "cryptographically-relevant QC" (CRQC), to protect against future compromise of data intercepted by adversaries today.

Technical PQC standards are under development by NIST and the National Security Agency (NSA); their release is expected in 2024, with a goal of transitioning U.S. Government assets to PQC and mitigating risk to the extent feasible by 2035. These and other activities under National Security Memorandum 10 (NSM-10) are underway to identify and mitigate risks posed by a future CRQC. As QC technology matures and additional security-related applications of QC emerge, provision of QC systems and services in the marketplace could also present opportunity for improper use. Export controls (the Export Administration Regulations and the Commerce Control List) can mitigate risk by limiting the ability to acquire technologies with national security implications—however, such protections could impose additional burdens or barriers to international collaboration or U.S. private sector development of QC if not properly balanced.

3.1.8. Recommendations

The Federal Government has demonstrated substantial commitment to QC and the broader field of QIS through its longstanding support for R&D in quantum science and technology and the acceleration of these efforts with the establishment of the NQI. Its ongoing support for R&D and infrastructure, national coordination, multisector partnerships with the nascent QC industry, and risk mitigation should be sustained and strengthened, including via the following recommendations:

Recommendation 1: The Federal Government should continue to support QC and QC-related R&D across the spectrum from fundamental to applied with a science-first approach in accord with the National Strategic Overview for QIS.

Recommendation 2: The Federal Government should continue its support and develop strategies towards use-inspired QC R&D aligned with national priorities to work toward practical solutions and stimulate quantum technology development.

Recommendation 3: The Federal Government should continue to support and evaluate the impact of efforts to make quantum computers available to researchers and students at all levels for experimentation, education, and training.

Recommendation 4: The Federal Government should identify additional QC equipment and facilities categories that are expensive, provide high value for research, and are sharable, and consider maintaining such equipment and facilities at central locations—for example, at Federal or National Laboratories.

Recommendation 5: The Federal Government should consider improvements to technology transfer practices at Federal facilities, such as training and incentives for government researchers to enhance the value of their QC patents, better tracking of available government inventions, and simplified and expedited licensing processes and agreements.

Recommendation 6: The Federal Government should consider a centralized certification service to help ensure that high-priority QC components meet user-desired performance standards, for example, through Federal or National Laboratories, or to promote risk-based assessment tools for these components.

Recommendation 7: The Federal Government should continue to support QC-related education and training programs, including characterization of necessary QC-relevant knowledge and skills and associated curriculum development, to broaden the range of individuals positioned for opportunities in the QC industry.

Recommendation 8: The Federal Government should consider QIS and QC as priority fields in its efforts to make it easier for foreign-born individuals who wish to live and work in the United States to contribute to the innovation ecosystem.

Recommendation 9: The Federal Government should establish a mechanism for regularly assessing and stress-testing potential risks to the QC supply chain, to include characterization of key components and their available sources and suppliers, to inform potential decisions about use restrictions and domestic production or research and engineering for alternative technical approaches.

Recommendation 10: While acknowledging the place of technology protections, regulations, and export controls, the Federal Government should consider the implications of such controls and regulations on the progress of QC R&D in its decision making.

Recommendation 11: The Federal Government should continue to support the development of PQC algorithms, protocols, and standards, and support and collaborate with industry and open-source developers to facilitate a smooth and timely transition to PQC deployment.

3.2. Background

The Consolidated Appropriations Act of 2021 (Public Law 116-260) mandated the Department of Commerce and Federal Trade Commission prepare a series of studies on critical and emerging technologies, including QC, and their impact on the U.S. economy. In support of this mandate, NIST entered into an agreement with SRI International—an independent, nonprofit research institute that administers the QED-C—to conduct a study on the QC industry. To do so, SRI staff interviewed QED-C participants knowledgeable about QC, the development of mandatory or voluntary QC standards, the QC R&D landscape, supply chains and marketplace, and security and economic considerations; reviewed relevant literature; leveraged past case studies; and conducted a survey of QED-C member organizations that participate in the QC industry. This chapter is based primarily on the QED-C study provided by SRI and supplemented with information from publicly available and published sources, as well as Federal agency expertise. As prescribed in the statute, this chapter highlights key aspects of the QC industry and its interaction with the Federal Government; identifies current, emerging, and long-term QC market, supply chain, economic, and national security risks; and provides recommendations for enhancing the ability of the United States to benefit from QC technologies.[46]

3.2.1. Introduction to Quantum Computing

QC falls within the domain of QIS, which also includes quantum sensing and metrology and quantum communications and networking. This chapter focuses on QC while acknowledging overlap between both the theoretical underpinnings and technological components of all

[46] The text of the statute is provided in Appendix I

quantum information technologies. Advances in these technologies will likely be intertwined to some degree.

Quantum computers leverage the properties of quantum phenomena such as superposition and entanglement to process information, unlike computers currently in use, which rely on the principles of classical physics. While classical computers encode information as “bits,” which can be zero or one, quantum computers encode information as quantum bits, or “qubits,” [47] which can be zero, one, or simultaneously some combination of both. Qubits enable fundamentally different ways of processing information that could, for some tasks, provide an exponential speedup over what is possible on today’s “classical” computers [3].

The idea of QC was first proposed more than 40 years ago as a means for modeling the behavior of quantum physical systems more accurately than possible with classical computers. Over the next two decades, the first quantum algorithms (instructions for processing information encoded as qubits) were developed that theoretically offer exponential speedup[48] over classical approaches. Some of these algorithms could in theory be used to break cryptographic systems that are currently widely used to protect the confidentiality of digital communications and stored data—should a quantum computer capable of running these algorithms (a CRQC), be built.

Quantum systems are in general extremely sensitive to their environment and easily perturbed; their performance is generally limited by “decoherence”—the extent to which they succumb to unwanted interactions with their surroundings that destroy the state in which they need to operate. Over the past few decades, scientific advances have made it possible to design and control quantum systems to the point where small,[49] proof-of-principle quantum computers have been built. A variety of quantum systems have been used to implement “physical qubits” and create small quantum processors, including trapped atomic ions, neutral atoms, Josephson junctions (small superconducting loops that form artificial “atoms”), nanoparticles, nitrogen-vacancy centers (engineered crystal defects) in diamonds, defects in semiconductor materials, and photons (light particles). The environmental conditions required for a quantum processor to work properly—along with the physical mechanism for implementing a quantum computation—depend on the type of physical qubit involved. Many require protection against vibrations, and some require extremely low temperatures. The mechanism for processing information encoded in a collection of qubits depends on the physical system or systems underlying the quantum hardware, but can include laser, infrared, or radiofrequency fields and pulses. Researchers are exploring other physical systems, such as anyons (quasiparticles theorized to exist in two-dimensional materials) as alternative platforms for QC.

3.2.1. QC Technologies Are in Early Stages of R&D

Several different models of quantum information processing are being pursued by researchers and developers. Gate-based QC is the most directly analogous to classical digital computing: algorithms are broken into individual logical operations on one or more qubits,

[47] A qubit encodes information as a superposition of two states. It is also possible for quantum information to be encoded in superpositions of more than two states; such systems are referred to as qudits.

[48] In this context, “speed” is defined in terms of the number of computational steps required.

[49] Small in terms of numbers of qubits and processing power, not in terms of physical footprint.

such that the number of steps required to complete a computation can be estimated as a function of the problem size. The number of operations, or "depth," of an algorithm that can be implemented by a quantum system, is limited by the extent of errors introduced into the system as a result of unwanted interactions between the processor and its environment. Substantial research is underway on a class of quantum algorithms called quantum error correction codes (QECC) to remove the errors in a quantum system and enable computations of arbitrary length. It has been theoretically shown that QECCs could be implemented if the fidelity of qubit operations can meet a certain threshold, depending on the QECC. If this could be achieved for large enough processors (in terms of number of qubits), the processor could in theory be programmed to solve any problem that is fundamentally computable—and at least certain problems could be solved more efficiently than with today's computers. While some early successes have been demonstrated, fully error-corrected or "fault tolerant" QCs have not yet been developed.

Non-gate-based approaches to quantum information processing operate using approaches other than implementing a set of logical operations. In quantum annealing, a set of qubits is initiated in an equal superposition of all possible states. Then, an attribute of the environment (for example, the local electric or magnetic field) is slowly changed until it reflects parameters that correspond to a specific problem; if designed and implemented correctly, the qubits have a high probability of evolving to a state that represents the solution to the problem. In another approach, called direct quantum simulation, the qubits are configured to represent some other (and typically more complex, or more difficult to control, access, or measure) quantum system. Then the environment is changed, which causes the state of the qubits to change; measuring the new state of the qubits can yield insights into the behavior of the quantum system under corresponding conditions. Different models of quantum information processing may be suited to different tasks, but it is too soon to know.

While researchers and QC companies are attempting to scale up each of these technologies, all QC platforms are in sufficiently early stages that the market has yet to consolidate around a single approach, and it may never do so. Different hardware types perform better in different contexts, so there may be no clear "winner" among the current QC hardware platforms being pursued. It is also possible that future quantum computers will utilize more than one sort of quantum technology, to capture the different advantages of each. Furthermore, QCs are not expected to provide substantial speedup for all computational tasks; rather than replacing classical semiconductor technologies, quantum computers are expected to augment classical systems by taking on only some parts of a computation—much like accelerators do today. Hybrid quantum-classical systems that optimize efficiency for both processor types are of substantial interest, and classical computer systems will almost certainly be required to operate quantum computers.

3.2.2. Support for QC R&D

R&D for QC technologies is currently funded through a combination of Federal support and private investment. Because QC is a relatively early stage technology, Federal support comes primarily from the scientific grantmaking and research agencies, including DoD, DOE, the Department of Homeland Security (DHS), the Intelligence Advanced Research Projects Agency, NASA, NIST, NSF, and NSA [4]. NIST has a decades-long history of QC technology development and a substantial internal QC research program. Federal support for QIS and quantum technologies builds on a long history of funding for foundational scientific research in quantum physics and related fields (sometimes referred to as Quantum 1.0), from which the QIS fields (sometimes referred to as Quantum 2.0) emerged.

In 2018, Congress passed the NQIA, formally launching the NQI to accelerate U.S. QIS R&D writ large, including QC. The NQIA provided for the establishment of new QIS R&D centers and institutes, launch of the QED-C, and codification of interagency coordination mechanisms, among other provisions and objectives. In addition to the specific activities articulated in the NQIA and other legislation, numerous Federal agencies continue to actively support or develop extramural research funding programs, partnerships, infrastructure development, and intramural research in QC. In FY2022, estimated Federal Government investment in QIS R&D exceeded $900M (including more than $300M for QC) across six agencies according to the NQI supplement to the President's Fiscal Year 2023 Budget. The proposed QIS R&D budget level for FY2023 is more than $800M (and approximately $250M for QC). Approximately half of the QIS R&D budget is attributed to activities explicitly authorized under the NQIA [4].

In 2021, estimated U.S. private sector investments in QC exceeded the reported Federal investments in QIS R&D. In that year, venture capitalists invested over a billion dollars into QC startups [5; 6]. In addition to venture capital and other investments, large, well-capitalized companies such as IBM, Google, Microsoft, Honeywell, and Intel have also spent considerable sums on QC.

In summary, QC technologies present exciting potential as a fundamentally new type of computation, are expected to offer advantages for some types of tasks in the future, and remain in early stages of development and readiness. QC R&D is ongoing and accelerating across U.S. sectors—including to identify potential applications—and across the globe. Sections 3.3–3.5 of this chapter explore the current and growing U.S. QC industry, Federal activities that support it, and its market, economic, and security risks—and identify recommendations for the U.S. Government to support further the QC industry moving forward. This chapter focuses on the information requested in the American Compete Act rather than providing a comprehensive description of all U.S. Government activities related to QC; further details of Federal activities are available at quantum.gov.

3.3. Observations

3.3.1. Industry Sectors That Develop, Implement, and Promote the Use of Quantum Computing

While QC technologies could one day augment classical computing to offer transformative advantages for certain applications, QC systems are at low stages of maturity and do not yet have market applications. Commercial applications for QC are expected to require quantum processors of increased size and stability relative to today's QC systems, and quantum algorithms that are efficient for commercially relevant tasks (or parts of such tasks).

Because quantum computers could enable advances in information technology writ large, they could potentially be useful for any industry—though it is generally understood that they will not necessarily offer advantages for all kinds of computations. The QC industry and the R&D community are actively seeking to identify and elucidate use cases for QC that can provide economic value, especially use cases that may be feasible in the near term. Promising areas under exploration include algorithms that enable the simulation of quantum mechanical systems, with potential applications for physics, chemistry, materials science, and pharmaceuticals; pattern recognition, useful for cryptography or machine learning; and optimization, with potential applications in finance, logistics, and other fields. The *Quantum Frontiers* report released by the White House National Quantum Coordination Office in 2020 identified “expanding opportunities for quantum technologies to benefit society” as one of eight major frontiers for QIS R&D.

A 2021 study by Hyperion Research, sponsored by QED-C and QCWare, found the most promising markets for QC to include those related to cybersecurity, financial, university/academic, and chemical/chemistry applications [7]. End-users’ interest in using QC is motivated by improving research capabilities, increasing revenue, driving innovation, and achieving competitive advantage [6].

Concerted efforts are being made to facilitate engagement between QC researchers and developers, the potential user base, and potential customers to identify promising use-cases to work toward. A list of U.S.-based quantum consortia is provided in Appendix J.

Broad interest exists across companies and sectors in the potential of QC. Companies and associations in industry user sectors including aerospace, architecture, automotive, defense and intelligence, electronics, energy, finance, logistics, pharmaceuticals, and retail have published thought pieces, organized events, initiated research programs, or enlisted consultants on QC. A rising number of introductory talks on quantum technologies have been held at professional and academic conferences sponsored by the classical computing community. This interest in QC among communities of potential end-users is catalyzing the identification of potential applications, advancing R&D, and promoting the development and use of QC technology in different sectors and domains.

In 2022, the QED-C Use Cases Technical Advisory Committee (TAC) reviewed use cases for QC, drawing upon publicly available data and interviews with more than 20 innovators. Preliminary results suggest that the advanced materials, life sciences, pharmaceuticals, chemicals, automotive (manufacturing/logistics), and finance industries have the most interest in the potential of QC. The Use Case TAC’s final report will explore a range of algorithms and draw a heat map of current use cases that maps applications against an approximation of QC system specifications expected by industry experts to be capable of running the necessary quantum algorithms.

Numerous chief executive officers of large corporations are devoting attention to QC, and have even given speeches on the potential importance of QC for their businesses. QED-C and the Pistoia Alliance, a global not-for-profit life science R&D organization, have established a community of interest for the life sciences and quantum science communities. Trade journals and associations from a variety of industries are communicating the potential value of QC to their members.

3.3.2. Public-Private Partnerships Focused on Promoting the Adoption and Use of Quantum Computing

For the purposes of this chapter, we interpret “public-private partnership” broadly to include major multi-sector partnerships or multi-organization collaborations that involve significant government funding or that involve engagement with the DOE National Labs—16 of 17 of which are government-owned, contractor-operated organizations that may engage in partnerships without using Federal funding. Given the early stages of QC technologies, QC PPPs focus on promotion or execution of R&D, finding QC use cases, building awareness about QC, and building a QC industry, which are necessary precursors to adoption and use of QC technologies. This section describes major government-initiated PPPs. There are also numerous additional national, international, and U.S. regional quantum consortia (see tabulations in Appendix J), many of which involve government participation.

3.3.2.1. QED-C

The NQIA of 2018 called for NIST to convene a consortium of stakeholders in quantum information science and technology “to identify the future measurement, standards, cybersecurity, and other appropriate needs for supporting the development of a robust quantum information science and technology industry in the United States.” Its goals include assessing current research on these needs and identifying associated gaps, and providing recommendations on how NIST and the NQI Program can address these gaps [8].

That year, NIST established a cooperative research and development agreement with SRI International [9] to lead the QED-C in fulfilment of this mandate; its sustainment is supported in part through an agreement under NIST’s other transactional authority. QED-C is governed by a nine-person Steering Committee, on which NIST has one seat. A second government seat rotates between different Federal agencies periodically, and recently changed from DOE to DoD. SRI is bound by specific objectives for the QED-C to enable NIST to meet its obligations under the NQIA, within NIST’s broader mission of promoting U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology. The QED-C is industry led while being responsive to government sponsors.

As of February 2023, QED-C’s membership comprised more than 200 organizations, including 161 corporations and 37 universities, as well as National Laboratories, federally funded research and development center administrators, and others. Federal Employees are welcomed to participate fully in the consortium’s activities [10]. QED-C facilitates collaboration among members and with the U.S. Government to accelerate the development and commercialization of QIS technologies. It also provides a broad industry perspective on QIS to the public and all government agencies, connects government agencies and the public with specific expertise or segments of the quantum ecosystem, and conducts studies on the state of the QIS industries, including the QC supply chain study used as an input for this chapter.

3.3.2.2. NIST Research Partnerships

NIST has long had an active Federal R&D program that includes a wide range of R&D in both Quantum 1.0 and Quantum 2.0, including QC and related areas. NIST expenditures on QIS R&D in FY 2021 are estimated at nearly $50M [11]. NIST research labs leverage CRADAs and other types of agreements with outside R&D partners. NIST also engages in several institute-scale partnerships focused on QIS R&D, including JILA and the JQI.

3.3.2.2.1. JILA

JILA is a research institute founded by NIST and the University of Colorado Boulder in 1962 [12]. Originally created to strengthen the field of laboratory astrophysics, JILA today specializes in research on Quantum Information Science and Technology (QIST), atomic & molecular physics, astrophysics, laser physics, biophysics, chemical physics, nanoscience, and precision measurement. Through JILA, Federal and university researchers are co-located on the university's campus to collaborate in research and training.

JILA's research in QIST emphasizes "entanglement, single atom trapping, magnetism-based quantum simulators, macro quantum objects, and translation of quantum information between light and mechanical motion" [13]. Currently, JILA has 22 principal investigators supporting their QIST efforts across a variety of research topics [13]. These include collaborations to develop the world's first neutral atom quantum computer [14], optical QC research [15], and research on integrating QC into higher-education curricula [16]. Also, at JILA is the Boulder Cryogenic Quantum Testbed, a joint effort between Google, NIST, and CU Boulder. The Testbed allows academic and industry researchers to test their superconducting microwave resonators, leveraging the metrology expertise of the three partners [17; 18].

In addition to research, JILA hosts a variety of community seminars, workshops, and professional development events. The JILA Physics Frontier Center participates in the NSF-funded Partnerships for Informal Science Education in the Community (PISEC) to "teach inquiry-based science to children in grades K-8" with a special focus on children from underrepresented groups, including those with low-income and ethnic minority backgrounds [19]. Other education and outreach events of JILA's in include CU Wizards, the Saturday Physics Series, PhET, and the Physics Education Research Group [20].

3.3.2.2.2. JQI

JQI is a collaboration between NIST, UMD, and LPS dedicated to "controlling and exploiting quantum systems" through various research programs [21]. Established in 2006 and located on UMD's College Park campus, JQI had an initial annual budget of approximately $6 million and objectives to (1) develop a world-class institute for understanding coherent quantum phenomena and enable control and engineering of quantum systems, (2) maintain and enhance U.S. technology leadership through collaborations between NIST, UMD, and LPS, and (3) support interdisciplinary research and exchange of ideas related to QIS. [22; 23]:

The institute has a particular focus on QC and information processing, quantum many-body physics, and quantum measurement and sensing [23]. Research on QC includes topics such as building the first practical quantum computer as part of the Software-Tailored Architecture for Quantum co-design (STAQ) project [24], improving ion trap systems [25], and exploring ways to miniaturize lasers [26].

JQI also hosts an NSF Physics Frontier Center, PFC @ JQI, a research center focused on ways to control and process quantum coherence and entanglement. Initiated in 2008 and renewed in 2014, PFC @ JQI is funded through an NSF cooperative agreement and has three activity areas: topological matter, many-body physics with photons, and dynamics of quantum systems far from equilibrium. JQI also participates in various activities with the community and public including offering traveling lectures to colleges, individual classroom visits, and on-site tours [27].

In 2014, NIST and UMD established the Joint Center for Quantum Information and Computer Science (QuICS) to improve quantum information storing, transport, and processing. QuICS was established to build upon JQI's original objective of improving quantum information research [28]. Research topics include quantum algorithms, error correction, metrology, cryptography, and foundational mechanics [29].

3.3.2.3. National Science Foundation Partnerships

NSF has been funding quantum research and education since the 1980s and continues to provide support to the field [30]. NSF currently supports quantum-related research through three primary areas: research funding, convening multidisciplinary scientists and engineers to accelerate research, and investing in quantum workforce development. In FY2022, NSF was directed by Congress to spend $220 million on QIS, including quantum computing [31]. Their flagship quantum computing-related initiatives include five Quantum Leap Challenge Institutes (three of which are directly focused on QC) and a supplemental funding opportunity to provide researchers with access to commercial quantum computing systems (described in this section), along with various R&D and education funding opportunities and center-scale activities (not discussed in detail here).

3.3.2.3.1. Quantum Leap Challenge Institutes

NSF has funded five Quantum Leap Challenge Institutes (QLCIs) to advance research in several QIS fields, including QC. NSF awarded grants for three of these institutes in July 2020 and two more in September 2021. According to NSF announcements, each will receive $25 million in funding over 5 years [32; 33]. Several of the NSF institutes have publicly announced their industry partners, while others have stated their strategic partnerships with businesses are forthcoming. These partnerships are anticipated to evolve over the lifetime of the institutes.

Of the five established QLCIs, three are directly focused on QC: the Challenge Institute for Quantum Computation (CIQC) at University of California, Berkeley; the Institute for Robust Quantum Simulation (RQS) at UMD, College Park; and the NSF Quantum Leap Challenge Institute for Hybrid Quantum Architectures and Networks (HQAN) at University of Illinois

Urbana-Champaign. A full list of all five QLCIs is provided in Table 1; details of the three QC-specific QLCIs are provided here.

CIQC was established in July 2020 by the University of California at Berkeley and partners [33]to focus on several fundamental challenges in quantum computing: developing quantum algorithms, realizing quantum advantage over classical computers, and scaling quantum technologies [34]. The Center also conducts or hosts various quantum workforce development activities including contributing to the development of a Master of Quantum Science and Technology degree at UCLA and hosting quantum computing workshops. [35] CIQC also offers a research exchange program for graduate students and postdocs that provides financial support for researchers to visit and collaborate with a partnering CIQC research campus, which are listed in Table 1 [36].

UMD hosts RQS, established in September 2021 [32], with three main research challenges related to quantum information processing. These include verifying quantum simulations, understanding quantum error correction by studying interactions between simulators and their environments, and scaling quantum simulations for applications across disciplines [37]. The institute intends to host summer schools and conferences with the broader research community and educational programs to help develop the quantum workforce [38].

The HQAN QLCI, established in July 2020 by the University Illinois Urbana-Champaign [33] and partners, focuses on challenges associated with scaling up quantum processors. The program aims to develop distributed quantum processing and quantum networks using modular, hybrid architectures. This institute has defined three major activities that include developing multi-node heterogeneous networks using proven technologies, developing a distributed computing software stack optimized for the hybrid networks, and integrating next-generation protected qubits into these new devices [39]. Similar to the other two highlighted QLCIs, HQAN includes various educational and workforce development programs including an exchange program with HQAN-affiliated universities [40], internships with private companies focused on QC [41], and training summer camps for local high school teachers about quantum concepts [42].

3.3.2.3.2. Dear Colleague Letter for Cloud-Based Access to Quantum Computing Resources

In June of 2022, NSF released a Dear Colleague Letter (DCL) "Enabling Quantum Computing Platform Access for National Science Foundation Researchers with Amazon Web Services, IBM, and Microsoft Quantum" [43; 44]. The DCL invited NSF-funded researchers to request supplemental funding for their projects to be used for accessing commercial experimental quantum computing systems via the cloud, and to support graduate student training. Namely, the DCL named Amazon Braket, IBM Quantum, and Microsoft Quantum as cloud vendors from whom coordinated access to QC hardware (QCs from Rigetti, IonQ, IBM, and Quantinuum) can be arranged, as well as software and related tools, including for quantum-inspired[50] classical computation. Access was provided through NSF CloudBank, a program that supports NSF researcher access to cloud-based computing resources in general.

[50] One advantage of QC R&D is that it has stimulated progress in classical computing methods, including classical approaches that are informed by quantum algorithms or methods, so-called "quantum-inspired" computing.

Supplemental funding requests of up to $50,000 per principal investigator were considered through July 2022 [43].

3.3.2.4. Department of Energy National Quantum Information Science Research Centers

DOE supports a variety of QC and QC-related research activities and infrastructure. DOE National Laboratories, including one federally operated center and 16 federally funded research and development centers operated by non-government entities, conduct R&D across a wide range of fields. DOE offers several partnership mechanisms, such as CRADAs, SPPs, ACTs, and Technical Assistance to facilitate collaboration with the DOE National Labs.

The NQIA called on DOE to establish large-scale quantum information science research centers through a competitive award process [8]. In January 2020, DOE announced it would award up to $625 million for this program over the next 5 years [45]. DOE describes its investment as a long-term, large-scale commitment of U.S. scientific and technological resources to a highly competitive, promising new area of investigation with enormous potential to transform science and technology [46].

In August 2020, the White House announced an award of up to $625 million in DOE funds to the five centers listed in Table 2, noting an additional $340 million in cost sharing would come from industry and academic partners [46]. The DOE National QIS Research Centers (NQISRCs) each received $15 million in FY2020 out of $115 million in Federal funding intended for each by FY2025. A complete list (as of January 2023) of the DOE NQISRCs is provided in Table 2. The DOE National QIS Research Centers engage industry in a variety of ways. Some have formal industry partners; others have invited industry representatives to sit on their advisory boards. In its call for proposals, DOE stated that the centers are to work with QED-C to promote the transition of results of the centers' research to practical applications in industry. The nature of the NQISRC interactions with QED-C continues to evolve.

3.3.2.5. DoD QC Partnerships

DoD has supported QIS and QC research through numerous programs, including through programs at DARPA, and through intramural research at its Federal labs. Through the National Defense Authorization Act (NDAA) of FY2020, the Secretaries of each military department were authorized to "establish or designate a defense laboratory to accelerate the research, development, and deployment of quantum information sciences and quantum information science-enabled technologies and systems" [47]. As of December 2022 [48], three laboratories have been selected as QIS research centers per the NDAA: the Air Force Research Laboratory (AFRL) Quantum Information Science Center [49], the Naval Research Laboratory Quantum Information Science Center [50], and the Laboratory for Physical Science Qubit Collaboratory [51]. These research centers each engage in or exist as partnerships for QIS, including the QC-focused centers described in the following subsections.

3.3.2.5.1. Innovare Advancement Center

The Innovare Advancement Center is a nonprofit organization created in 2019 through a partnership between the AFRL Information Directorate, the Griffiss Institute (a STEM talent and technology accelerator), New York's Oneida County, and the State University of New York [52]. Located in Rome, NY, the center focuses on collaborative R&D for technology maturation and commercialization in the areas of quantum computing, artificial intelligence and machine learning, neuromorphic computing, nanoelectronics, and uncrewed aerial systems [53]. One of Innovare's first activities was to host a 3-day, global engagement event featuring a $1M pitch competition, the International Quantum U Tech Accelerator [52], and remarks from leaders around the world. The center provides physical R&D facilities that include two quantum laboratories; interested researchers from around the world can visit the center for training and skills development and to participate in research [54]. Individuals or organizations interested in research or other collaborations can enter into a variety of formal, enabling partnership mechanisms with the AFRL, including CRADAs, information transfer agreements, material transfer agreements, patent license agreements, and commercial test agreements [55].

3.3.2.5.2. DoD Quantum Technology Center

The Quantum Technology Center is a partnership between the Army Research Laboratory, the Naval Research Laboratory, and UMD and nine private sector partners that was established in 2019 to "exchange ideas and opportunities to [i]nnovate, [t]ranslate, and [e]ducate in quantum technology." The center's research areas include quantum sensing, computing & simulation, communications & networking, materials, and algorithms. The center has also established a Partners Program with private industry including Leidos, IonQ, Accenture, MITRE, and ColdQuanta to advance research.

3.3.2.5.3. LPS Qubit Collaboratory

The Laboratory for Physical Science Qubit Collaboratory (LQC) is housed at the LPS at UMD, College Park. The LQC is a partnership between LPS and the Army Research Office as a "center without walls" that is "uniquely suited to tackle the most challenging problems in quantum information research" and provide a mechanism for multisector collaborative research [51; 56]. Among their six research thrusts, those related to advancing quantum computing include advanced materials science research for quantum computers, development of qubits that operate in a specific temperature ranges, and workforce development programs for faculty to conduct research in quantum computing [57]. The LQC also hosts various events including workshops, recruitment events, and open houses for students. In July to August 2022, the LQC hosted their second annual Summer of Quantum Short Course, a free virtual program targeted to students from rising undergraduate seniors to second year graduate students [58].

Table 1. NSF Quantum Leap Challenge Institutes.

Center	Federal and National Laboratory Partners	Private Sector or Industry Partners	Academic Partners
Challenge Institute for Quantum Computation [59; 60]	NSF and the Lawrence Berkeley National Laboratory	QED-C, Simons Institute; evolving	University of California-Berkeley,* University of California-Los Angeles, University of California-Santa Barbara, California Institute of Technology (Caltech), University of Southern California, University of Texas at Austin, Massachusetts Institute of Technology (MIT) and University of Washington Seattle
Institute for Robust Quantum Simulation [61]	NSF		University of Maryland-College Park,* Duke University, North Carolina State University, Princeton University and Yale University
NSF Quantum Leap Challenge Institute for Hybrid Quantum Architectures and Networks (HQAN) [62]	NSF, AFRL, MIT Lincoln Laboratory and FermiLab	IBM, Google, ColdQuanta, Toptica, American Family Insurance, AdvR, Northrop Grumman, Quantum Opus, Qubitekk, Xanadu, Microsoft, Aliro Quantum Technologies, FlexCompute, Vescent Photonics, Keysight Technologies	University of Illinois at Urbana-Champaign,* University of Chicago and University of Wisconsin-Madison

Center	Federal and National Laboratory Partners	Private Sector or Industry Partners	Academic Partners
Quantum Systems through Entangled Science and Engineering (Q-SEnSE) [63]	NSF, NIST, Los Alamos National Laboratory, MIT Lincoln Laboratory and Sandia National Laboratories		JILA at University of Colorado Boulder,* Harvard University, MIT, Stanford University, University of Delaware, University of Oregon, University of New Mexico and University of Innsbruck
NSF Quantum Sensing for Biophysics and Bioengineering (QuBBE) [64]	NSF, Argonne National Laboratory	Adámas Nanotechnologies, P33, Somalogic, and Toptica Photonics	University of Chicago,* Chicago State University, University of Illinois at Chicago, University of California Santa Barbara, Harvard University, Solorio Academy High School, and Chicago Quantum Exchange

Notes: Asterisk (*) denotes lead managing university. Partnership information is current as of January 27, 2023. Not all institutes are focused on QC, but all are included in this table.

Table 2. DOE National Quantum Information Science Research Centers.

Center	Federal and National Laboratories Partners	Industry Partners	Academic Partners
Next Generation Quantum Science and Engineering (Q-NEXT) [65]	Argonne National Laboratory,* SLAC National Accelerator Laboratory, and Pacific Northwest National Laboratory	AWS, Applied Materials, Boeing, ColdQuanta, General Atomics, HRL Laboratories, IBM, Intel, JPMorgan Chase & Co., Keysight Technologies, Microsoft, Quantum Opus, Verizon, and Zurich Instruments	Caltech, Cornell University, MIT, Northwestern University, Pennsylvania State University, Stanford University, University of California-Santa Barbara, The University of Chicago, University of Illinois, and University of Wisconsin-Madison
Co-design Center for Quantum Advantage (C^2QA) [66]	Ames Laboratory, Brookhaven National Laboratory,* Jefferson Lab, NASA Ames Research Center, Pacific Northwest National Laboratory, and Princeton Plasma Physics Lab	IBM	MIT, Princeton University, Stony Brook University, Yale University, University of California-Santa Barbara, Caltech, Johns Hopkins University, University of Illinois Chicago, City College of New York, Montana State University, University of Massachusetts-Amherst, Columbia University, University of Pittsburgh, Harvard University, Northwestern University, North Carolina Agricultural and Technical State University, University of Washington, Howard University, SUNY Polytechnic Institute, and Virginia Tech

Center	Federal and National Laboratories Partners	Industry Partners	Academic Partners
Superconducting Quantum Materials and Systems Center (SQMS) [67]	Fermilab,* Ames National Laboratory, NASA Ames Research Center, Jefferson Lab, and NIST	Rigetti, Form Factor, INFN, Goldman Sachs, Lockheed Martin, and Unitary Fund	Northwestern University, University of Colorado Boulder, Colorado School of Mines, Stanford University, Johns Hopkins University, Temple University, University of Arizona, Illinois Institute of Technology, University of Illinois Urbana-Champaign, Royal Holloway University of London, Rutgers University, Louisiana State University, University of Minnesota, National Physical Laboratory, NYU Langone, University of Waterloo IQC, and the University of Pisa
Quantum Systems Accelerator (QSA) [68]	Lawrence Berkeley National Laboratory,* Sandia National Laboratories, and MIT Lincoln Laboratory		University of Colorado Boulder, Caltech, Duke University, Harvard University, MIT, Tufts, University of California-Berkeley, University of Maryland, University of New Mexico, University of Southern California, University of Texas Austin, and the Université de Sherbrooke
The Quantum Science Center (QSC) [69]	Oak Ridge National Laboratory,* Fermilab, Los Alamos National Laboratory, and Pacific Northwest National Laboratory	ColdQuanta, IBM, and Microsoft	Caltech, Harvard University, Princeton University, Purdue University, University of California-Berkeley, University of California-Santa Barbara, University of California-Los Angeles, University of Tennessee-Knoxville, and University of Washington

Asterisk (*) denotes lead managing National Laboratory. Partnership information is current as of January 27, 2023.

3.3.2.6. National Q-12 Education Partnership

To increase the diversity and number of students ready to enter the quantum workforce, OSTP and NSF initiated in 2020 the National Q-12 Education Partnership between the Federal Government, industry, academia, and professional societies to offer various training opportunities [70].[51] The partnership has developed resources for educators to teach quantum science including curriculum frameworks to incorporate QIS concepts into high school curricula [71]. The framework "encourages hands-on experiences with quantum tools in the classroom and through online venues and connecting students to public and private quantum career opportunities" [70]. Other resources include textbooks, lecture notes, and other various reference materials [72].

3.3.2.7. QIS Public-Private Partnerships in Other Regions and Nations

The United States is not alone in establishing national initiatives that include PPPs to support development of QIST, and especially QC. For example, the European Quantum Industry Consortium (QuIC) was created in 2019 [73]. Other national consortia have since been established, including Quantum Delta NL in the Netherlands [74] and Q-STAR in Japan [75]. These consortia are predominantly focused on helping to generate economic value from quantum innovation.[52]

For example, the United Kingdom established its National Quantum Technologies Programme in 2013 [76]. In 2014, it invested £214 million (approximately $350 million) in 2014 to establish four technology hubs, which were renewed with an additional £94 million (approximately $120 million) in 2020. The hubs are organized around application areas: quantum communications, sensors and timing, enhanced imaging, and QC. These PPPs apply government funding to spur collaboration across universities, National Laboratories, and industry partners toward achieving commercial goals that might underpin a domestic quantum industry. The University of Oxford leads the Quantum Computing and Simulation Hub. This hub now features 16 other academic institutions and 27 industry partners [77].

In another notable national investment, the Netherlands' National Growth Fund awarded €615 million (approximately $735 million) to Quantum Delta NL to fund its activities between 2021 and 2027 [74]. Quantum Delta NL has launched five urban research hubs—connecting universities, startups, and other companies—with the mandate to coordinate and execute the Netherlands' National Agenda for Quantum Technology. By 2027, the consortium has goals of attracting three corporate quantum R&D labs, incubating and accelerating 100 quantum startups, and training 2,000 doctoral students in quantum disciplines. Early accomplishments include demonstrating a multi-node quantum network, launching a €2 million (approximately $2.2 million) fund providing seed grants to quantum startups, designing a "House of Quantum" headquarters with shared laboratory space, and

[51] Industry partners include IBM, Boeing, AWS, Intel, Quantum for All, Optica, Qubit by Qubit, Microsoft, American Physical Society, Google, Zapata, Quantinuum, American Association of Physics Teachers. SPIE, Rigetti, Montana Instruments, and Lockheed Martin. Other partners include QuSTEAM, University of California Santa-Barbara, Joint Quantum Institute, and the Chicago Quantum Exchange.

[52] See Appendix J for broader lists of quantum consortia in the United States and in other countries. Given the dynamic nature of QIS and differences in definitions of public-private consortia, these lists may not be exhaustive.

providing childcare travel grants to women working in quantum disciplines. Appendix J provides a more comprehensive list of consortia established by foreign countries.

3.3.3. Industry-Based Bodies That Develop Mandatory or Voluntary Standards for Quantum Computing

The current state of QC standards development reflects the technology readiness of practical QC applications and interoperability: to date few technical standards have existed for QC. Nevertheless, standards-setting or related activities pertaining to quantum technologies in general are underway by private sector organizations (namely, SDOs) in collaboration with industry, governments, and technical experts;[53] a few groups are exploring topics specific to QC. De facto standards, benchmarks, and related practices are also under development by researchers, companies, and other entities; de facto standards are not necessarily adopted formally or widely used, but are often useful within the QC community as evolving, near-term tools.

3.3.3.1. SDO Entities Developing QC Standards

SDOs have been engaged on standards for quantum technologies since 2010, and for QC in particular since 2018. Activity has increased over time along with interest and progress in these fields. Table 3 provides a list of SDO working groups or subcommittees currently developing QC standards.[54] While only a subset of international SDOs have published or are developing quantum technology standards, SDOs are increasingly forming groups to focus on them. SDO activities require alignment with best antitrust practices to avoid abuses of process that, for example, could lead one or more industry participants to gain an unfair competitive advantage over other participants.

The two SDOs most active in developing standards for QC are the Institute of Electrical and Electronics Engineers Standards Association (IEEE SA), and the Joint Technical Committee on information technology (JTC 1) of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). IEEE is a global organization that undertakes activities related to electrical engineering, including supporting technology-based communities and publications, regional professional groups, education, and standards development [78]. IEEE Quantum, a focal point of IEEE's quantum technology activities, was launched in 2019 [79]. IEEE Standard Association (SA) is the IEEE affiliate that focuses on standards development. Several IEEE working groups are focused on various aspects of standards development, as indicated in Table 3. ISO and IEC are non-governmental SDOs that set standards in many areas of technology and business, forming JTC 1 in 1987 to address mutual interests and foster an environment for experts to develop worldwide ICT standards for business and consumer applications [80]. Under JTC 1, Working Group 14 focuses on QC and Subcommittee 27 focuses on information security, cybersecurity and privacy protection, including post-quantum cryptography, and QIS standards more generally [80]. In 2022, the British Standards Institution submitted a proposal

[53] We note that, while the legislation asks about industry-based bodies, standards development is generally a collaborative, multisector process.

[54] The groups and standards listed in this report are current as of July 2022, unless otherwise noted.

for a new field of technical activity—ISO/IEC/JTC Quantum technologies—that will be voted on by the member National Standards Bodies of ISO and IEC.

Table 3. SDO Groups Developing QC-related Standards. [a]

SDO	Group	Topical Area	Purpose
ISO/IEC JTC 1 [80]	WG 14 Quantum Computing	Quantum computing	Identify gaps/opportunities for QC standardization; track and develop new QC standards
ISO/IEC JTC 1 [80]	SC 27 Information security, cybersecurity and privacy collection	Information communications technology security management systems	Development of standards for the protection of information and ICT
IEEE SA [81]	QuSIM/WG-Programmable Quantum Simulator Working Group	Quantum simulation	
IEEE SA [82]	QuADD/WG – Quantum Algorithm Design and Development WG	Quantum algorithms	Developing standards to help enable the design and development of new quantum algorithms
IEEE SA [83]	QCN-WG – Quantum Computing Nomenclature Working Group	Quantum computing	
CENELEC [84]	FGQT – Focus Group on Quantum Technologies	Quantum technology	Connects stakeholders interested in identifying standardization needs; developing a standardization roadmap

[a] Details of some working group activities are not publicly available.

The European Committee for Electrotechnical Standardization (CENELEC) set up a Focus Group on Quantum Technologies (FGQT) in mid-2020. CENELEC is one of three European

SDOs, together with the European Committee for Standardization (CEN) and the European Telecommunications Standards Institute (ETSI), that the European Union and the European Free Trade Association have officially recognized as responsible for developing and defining voluntary standards at the European level [85].

The Internet Engineering Task Force (IETF), the leading internet standards body, formed the Quantum Internet Research Group in mid-2021. The group is led by the IETF's parallel organization, the Internet Research Task Force (IRTF), which focuses on longer-term research issues related to the internet. The charter for the group includes working toward remote computation capabilities and distributed QC, including enabling classical connectivity for control and management of quantum computers [86]. IETF is also working to integrate PQC algorithms into several of its internet standards; the effort is anticipated to conclude after the completion of NIST's PQC standardization activity [87; 88].

The activities of national SDOs outside of the United States are also, at present, limited in QC. The British Standards Institution (BSI) formed a quantum technology panel in early 2021 [89]. Numerous other national SDOs (including in France, the Netherlands, South Korea, China, and Japan) have representation and participate in the ISO/IEC JTC1 quantum standards workgroup, though these national bodies have yet to designate their own quantum technology groups.[55] No published standards related to quantum technologies were identified from among the Standardization Administration of China's hundreds of thousands of mandatory or voluntary national standards. While China has in the past relied on technology standards developed in the West, it has engaged more substantially in recent years—particularly in areas such as cryptography. Its October 2021 standardization strategy, combined with the prioritization of high technology in its latest Five-Year Plan, suggests that China intends to engage in quantum standards-setting activity [90].

3.3.3.2. Informal or De Facto Standards

Standardization activities also occur outside the formalized structure of SDOs in the form of informal or de facto standards. Progress in QC is difficult to track in the absence of clear reporting conventions and metrics [3]. Toward that end, researchers and companies have developed a wide range performance metrics, tools, or benchmarks for use in characterizing system of performance in a consistent manner that permits direct comparisons, or for the purpose of tracking improvements. For example, IBM introduced a convention of "quantum volume" that accounts for multiple aspects of quantum processor performance in a single numerical value [91–93]. Alternative approaches proposed for tracking the performance of quantum processors include tracking the number of qubits on a quantum processor for a constant error rate in the near term, and tracking the number of logical qubits on an error-corrected processor in the longer-term (at such time that logical qubits are implemented in quantum systems) [3]. In 2021, QED-C released an open-source suite of application-oriented performance benchmark programs for characterizing QC hardware performance [94]. While these methods make it easier to track progress in quantum processor performance, direct

[55] Of the 176-member countries represented in ISO, 20 are on ISO/IEC JTC1 WG 14 "Quantum Computing:" Australia, Austria, Canada, China, Denmark, Finland, France, Germany, India, Ireland, Italy, Japan, Kazakhstan, Korea, Luxembourg, the Netherlands, Portugal, the Russian Federation, Spain, and the United States.

comparisons—especially across different hardware platforms—remain challenging at this time.

Also in 2021, DARPA established its Quantum Benchmarking program, dedicated to creating rigorous, quantitative benchmarks of progress toward specific quantum computational achievements, and to developing estimates of hardware requirements necessary to achieve them [95]. DARPA awarded several contracts in 2022 to performers for this program, including to Raytheon BBN, the University of Southern California, and a team including researchers from Aalto University, IonQ, University of Technology Sydney, University of Texas at Dallas, and Zapata Computing [96; 97]. Such benchmarks would make it easier to track progress in QC.

Another activity is to define common ways of simplifying discussion of QC systems at different levels of detail or operation (so-called abstraction layers) to improve the interoperability and portability of software across different quantum hardware platforms. QED-C members from across the QC industry are collaborating to conduct an architecture study and develop reference implementations for this abstraction, called intermediate representation [98]. At least two similar efforts are focused on QC intermediate representation. In the United States, the Quantum Intermediate Representation (QIR) Alliance was established under the Linux Foundation's Joint Development Foundation [99]. In the United Kingdom, the quantum software company Riverlane and the National Physical Laboratory released a preliminary specification for a multi-level QC hardware abstraction layer for quantum computers ("QHAL") of potential use to QC users [100; 101]. The existence of disparate activities in this area suggests a need for greater collaboration across the QC R&D community.

3.3.3.3. Status of Industry-based Mandatory or Voluntary Standards

The number of QC standards released or in development remains low—especially in comparison to more advanced technology areas such as artificial intelligence. The small number may reflect a consensus among sector participants that further technology maturation is required before undertaking meaningful efforts toward interoperability. QC currently has few interoperability requirements with other technologies; it may be analogous to classical computing's graphical processing units (GPU), which principally interface with a single component, the central processing unit (CPU). Today, even as CPU-GPU interoperability has matured, in the classical computing industry there are no SDO standards for this interaction. The interface is customized according to the designs of the GPU manufacturer. It is possible that QC technologies could follow a similar path.

Quantum computer providers generally offer their current-stage, experimental systems to the public through the cloud; many industry experts anticipate that fully mature quantum computers will also be accessed through cloud platforms, rather being owned by and sited with the end-user [7]. While the utilization of quantum computers is expected to have great impact, the actual number of units and users may not trigger a need for extensive standardization. This is akin to classical, high-performance supercomputers today—relatively few units and users as compared to other computers.

The standards currently under development for QC, listed in Table 4, generally focus on terms, definitions, early metrics and benchmarking, early architecture standards, and forward-looking roadmapping.

Table 4. Quantum Computing Standards Under Development by SDOs.

Standard	SDO (Group)	Status	Start	End
P3155 – Standard for Programmable Quantum Simulator [81]	IEEE SA/QuSIM/WG	Under development	2022-02	–
P3120 - Standard for Quantum Computing Architecture [102]	IEEE	Under development	2021-11	–
P2995 - Trial-Use Standard for a Quantum Algorithm Design and Development [103]	IEEE	Under development	2021-06	–
ISO/IEC AWI TR 18157: Information technology — Introduction to Quantum Computing [104]	ISO/IEC JTC1	Under development	2021-06	–
NP 4879 Quantum computing – Terminology and vocabulary [105]	ISO/IEC JTC1	Under development	2020-09	–
N149a: Quantum technologies standardization roadmap [106]	CEN/CENELEC FGQT	Under development	2020-06	–
P7131 - Standard for Quantum Computing Performance Metrics and Performance Benchmarking [107]	IEEE	Under development	2019-06	–
P7130 - Standard for Quantum Technologies Definitions [83]	IEEE	Under development	2018-02	–

3.3.4. Federal Agencies with Jurisdiction

Today, there is no regulatory framework explicitly targeting QC technologies. However, many Federal agencies have authority to regulate industrial activities that could eventually leverage QC technologies, depending on how existing authorities are applied. In addition, many agencies have missions that strongly overlap with different industrial sectors that could one day adopt QC technologies. Table 5 indicates which agencies have general jurisdiction over each industry sector, using the North American Industry Classification System (NAICS) and sector codes.

Table 5. Agencies with General Jurisdiction over a Sector That Could Adopt QC.

Department/Agency	Sector (NAICS)
CFPB	Finance and Insurance (52)
CFTC	Finance and Insurance (52)
CPSC	Retail Trade (44-45)
DHS	Utilities (22), Manufacturing (31–33), Wholesale Trade (42), Transportation and Warehousing (48–49), Information (51), Public Administration (92)
DOC-BIS	All Sectors
DOC-NIST	All Sectors
DOC-USPTO	All Sectors
DoD	Manufacturing (31–33), Wholesale Trade (42), Public Administration (92)
DoD-DARPA	Public Administration (92)
DOE	Mining, Quarrying, and Oil and Gas Extraction (21), Utilities (22)
DOI-USGS	Mining, Quarrying, and Oil and Gas Extraction (21)
DOJ	All Sectors
DOJ-ATF	Manufacturing (31–33)
DOL	All Sectors
DOT	Transportation and Warehousing (48–49)
ED	Educational Services (61)
EPA	Administrative and Support and Waste Management and Remediation Services (56); Mining, Quarrying, and Oil and Gas Extraction (21); Construction (23); Transportation and Warehousing (48–49); Utilities (22)
FCC	Information (51)

Department/Agency	Sector (NAICS)
FDIC	Finance and Insurance (52)
FFIEC	Finance and Insurance (52)
FRB	Finance and Insurance (52)
FTC	Information (51)
GSA	Public Administration (92)
HHS	Agriculture, Forestry, Fishing and Hunting (11), Health Care and Social Assistance (62)
HHS-FDA	Manufacturing (31–33)
HHS	Health Care and Social Assistance (62)
NASA	Public Administration (92)
ODNI-IARPA	Public Administration (92)
OPM	Public Administration (92)
SEC	Finance and Insurance (52)
Treasury	Finance and Insurance (52)
Treasury-OCC	Finance and Insurance (52)
Treasury-OFAC	Finance and Insurance (52)
Treasury-OIS	Public Administration (92)
U.S. Access Board	All Sectors
USDA	Agriculture, Forestry, Fishing, and Hunting (11)
VA	Health Care and Social Assistance (62)

In addition to the agencies listed in Table 5, the Department of Justice's Antitrust Division and the Federal Trade Commission enforce laws that prevent firms from creating or exploiting market power that would distort the allocation of resources or reduce innovation and, thereby, harm consumers. This mandate applies broadly across industries including those associated with QC technologies.

3.3.5. Interaction of Federal Agencies with Industry Sectors

Table 6 lists the agencies that have significant interactions with each industry sector (a reorganization of the information in Table 5), any of which could adopt QC should a compelling use case emerge. In many cases, this is because the agency has general jurisdiction over that sector. In addition, the science agencies (including DoD, DOE, NSF, NIST, and others) play an important role in funding QC R&D [11].

Table 6. Agencies That Have Significant Interactions with Industry Sectors That Could Use QC.

Sector	Name	Department/Agency
11	Agriculture, Forestry, Fishing, and Hunting	DOC-BIS, DOC-NIST, DOC-USPTO, HHS, USDA, EPA
21	Mining, Quarrying, and Oil and Gas Extraction	DOC-BIS, DOC-NIST, DOC-USPTO DOE, EPA, DOI
22	Utilities	DOC-BIS, DOC-NIST, DOC-USPTO DHS, DOE
23	Construction	DOC-BIS, DOC-NIST, DOC-USPTO
31–33	Manufacturing	DOC-BIS, DOC-NIST, DOC-USPTO, DHS, DoD, DOJ-ATF, HHS-FDA
42	Wholesale Trade	DOC-BIS, DOC-NIST, DOC-USPTO, DHS, DoD
44–45	Retail Trade	CPSC, DOC-BIS, DOC-NIST, DOC-USPTO
48–49	Transportation and Warehousing	DOC-BIS, DOC-NIST, DOC-USPTO, DHS, DoT
51	Information	DOC-BIS, DOC-NIST, DOC-USPTO, DHS, FCC, FTC
52	Finance and Insurance	CFPB, CFTC, DOC-BIS, DOC-NIST, DOC-USPTO, FDIC, FFIEC, FRB, SEC, Treasury-OCC, Treasury-OFAC, Treasury
53	Real Estate and Rental and Leasing	DOC-BIS, DOC-NIST, DOC-USPTO
54	Professional, Scientific, and Technical Services	DOC-BIS, DOC-NIST, DOC-USPTO
55	Management of Companies and Enterprises	DOC-BIS, DOC-NIST, DOC-USPTO
56	Administrative and Support and Waste Management and Remediation Services	DOC-BIS, DOC-NIST, DOC-USPTO, EPA
61	Educational Services	DOC-BIS, DOC-NIST, DOC-USPTO, ED
62	Health Care and Social Assistance	DOC-BIS, DOC-NIST, DOC-USPTO, HHS, VA
71	Arts, Entertainment, and Recreation	DOC-BIS, DOC-NIST, DOC-USPTO
72	Accommodation and Food Services	DOC-BIS, DOC-NIST, DOC-USPTO

Sector	Name	Department/Agency
81	Other Services (except Public Administration)	DOC-BIS, DOC-NIST, DOC-USPTO
92	Public Administration	DOC-BIS, DOC-NIST, DOC-USPTO, DoD, DoD-DARPA, DHS, EOP-OMB, GSA, NASA, ODNI-IARPA, OPM, Treasury-OIS

3.3.6. Interagency Activities

The NQIA, passed in 2018 (Pub. L. 115-368), authorized a number of Federal departments and agencies to coordinate Federal QIS efforts. One of these bodies is the National Quantum Coordination Office (NQCO), established within OSTP [8]. The NQCO is charged with overseeing the interagency coordination of the NQI Program.

As a part of the NQI Program, two committees within the NSTC host QIS-related subcommittees: the Committee on Science hosts SCQIS and the Committee on Homeland and National Security hosts ESIX. These subcommittees were formally authorized by the NQI Act and National Defense Authorization Act (NDAA) for FY2022, respectively, to support the NQCO. Table 7 provides a list and description of these subcommittees and the SCQIS-based Interagency Working Groups, which focus on Quantum Science, QIST End-Users, Workforce, and Quantum Networking. Other less formal interagency coordination mechanisms occur at the program manager level.

To coordinate interagency efforts and to advance the field of QIS writ large, the NQCO and NSTC subcommittees have published a number of documents on current and future Federal efforts in QC, including seven strategy documents. The 2018 National Strategic Overview for QIS identifies six major thematic areas of government effort: (1) Choosing a science-first approach to QIS, (2) Creating a quantum-smart workforce for tomorrow, (3) Deepening engagement with quantum industry, (4) Providing critical infrastructure, (5) Maintaining national security and economic growth, and (6) Advancing international cooperation. Other strategy documents focus on specific QIS sub-fields or thematic areas: quantum networking (two documents), quantum workforce (two documents), quantum sensors (one document); and frontiers of QIS research (one document). As of February 2022, there is no national strategy document focused on quantum computing.

The NQCO also provides a publication library containing 34 scientific and technical reports commissioned by or authored by researchers across the Federal Government—including from DOE, NSF, and AFRL. These reports span various topics including uses of QC for scientific research, creation of a nationwide quantum internet, and challenges posed by post-quantum cryptography. These documents, along with event summaries and the NQI Supplements to the President’s Budgets, are listed and available at NQI’s website (quantum.gov).

In addition to reports and publications, the NQCO and NSTC subcommittees have hosted and organized interagency QIS workshops and summits in collaboration with industry and academia. These events focused on coordination to build a robust quantum workforce and research networks, and include the Quantum Workforce: Q-12 Actions for Community Growth, held in February 2022 [108]; the White House Summit on Quantum Industry and Society in October 2021 [109]; the Workshop on Quantum Recruitment in the Federal Government in August 2021 [110]; and the National Quantum Initiative Centers Summit in December 2022 [48].

Table 7. Entities That Coordinate QC Activities Across U.S. Federal Agencies.

Activity/Entity	Participating Agencies	Description
National Quantum Coordination Office (NQCO) [111; 8]	EOP/OSTP	Authorized in §102 of the NQI Act, established within OSTP to oversee the interagency coordination of the National Quantum Initiative Program
Subcommittee on Quantum Information Science (SCQIS) [112; 113; 8]	EOP/NSTC, NIST, NSF, DOE, NASA, DoD, DHS, DOI, DOS, IARPA, NIH, ODNI, OMB, OSTP, USPTO	Authorized in §103 of the NQI Act, established to maintain and expand U.S. leadership in QIS and its applications.
Subcommittee on the Economic and Security Implications of Quantum Science (ESIX) [112; 114; 115]	EOP/NSTC, DOE, DoD, DOC, DHS, DARPA, ODNI, OMB, OSTP, DOJ, DOS, FBI, NASA, NSF, NIST, NSA, NRL, NSC, IARPA	Authorized in §6606 of the NDAA FY2022, established to ensure that economic and security implications of QIS are understood across agencies.
Working Group on Science [116; 117]	Multiple agencies; no official list	Focuses on needs for advancing fundamental QIS
End User Working Group [116; 117]	Multiple agencies; no official list	Focuses on use cases for quantum technologies
Working Group on Workforce [118]	Multiple agencies; no official list	Focuses on QIS workforce issues
Quantum Networking Working Group [119]	Multiple agencies; no official list	Focuses on quantum networking and communications
International Working Group	Multiple agencies; no official list	Focuses on issues related to international cooperation for QIS in alignment with the “Advancing international cooperation” thematic area of the National Strategic Overview for QIS [120]

3.3.7. Regulations, Guidelines, Mandatory Standards, Voluntary Standards, and Other Policies Implemented by Federal Agencies

At the time of this writing, Federal agencies have not issued mandatory or voluntary guidelines or regulations for QC technologies. Federal agency efforts concerning QC have focused on QC R&D rather than regulatory guidance or standards for QC, though Federal reports on QIS have highlighted that standards will be needed in the future. The Federal Government encourages Federal agencies to participate in SDOs, but agencies have not issued official guidance on QC-specific standards.

However, substantial activity is ongoing at NIST and other Federal agencies to address potential cybersecurity implications of QCs. NIST has focused on identification and standardization of classical cryptographic protocols expected to be resilient against cryptanalysis by a potential future quantum computer, should one of cryptographic relevance be developed; these approaches are referred to as "post-quantum cryptography." NIST has been soliciting and assessing quantum-resistant cryptographic algorithms from public stakeholders for eventual application in a government-wide post-quantum encryption standard [121].

In January 2022, the President issued National Security Memorandum-8, which ordered Federal departments to identify National Security Systems using algorithms that are not in compliance with NSA-approved Quantum Resistant Algorithms or commercial national security algorithms, and to create a timeline for transitioning those systems to quantum resistant encryption [122]. The President also issued Executive Order 14067 directing the OSTP Director, the Chief Technology Officer (CTO) of the United States, and relevant agencies to assess the technical risks of central bank digital currencies (CBDC) with respect to "emerging and future technological developments, such as quantum computing" [123]. Consistent with the nascent nature of QC, Federal agencies have yet to develop final regulations, guidelines, or standards related to digital currency, but are preparing for such an eventuality.

On May 4, 2022, the President issued National Security Memorandum-10 (NSM-10) on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems. This memorandum identifies key steps and Federal agency actions necessary to mitigate risks related to a potential CRQC, including in collaboration with industry, and critical infrastructure owners and operators [124]. On July 5, 2022, NIST announced the first four algorithms intended for standardization with four more under consideration [125]; publication of a final rule is expected in 2024 [126]. NSA has issued its views on the submitted algorithms [127]. In accordance with NSM-10, NSA issued notice to National Security System owners and operators about future requirements for quantum resistant cryptography and provided an approximate timetable for transition. Some of the algorithm selections are contingent on NIST finalizing its standardization process. DHS issued a memorandum providing a roadmap, created in collaboration with NIST, to each of its component heads to prepare for post-quantum cryptography [126].

Executive Order 14073 reestablished the National Quantum Initiative Advisory Committee under the current Administration as a Presidential advisory committee to evaluate the NQI and provide advice related to QIST [128]. The United States has also entered into bilateral agreements with eight nations as of February 2022 for cooperation in QIST [129]. Key policy documents described in this section are listed in Table 8.

Table 8. Executive Orders and Memoranda with Policy Related to QIST.

Document	Relevant Federal Agencies	Date	Description
National Security Memorandum (NSM-10) on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems [124]	EOP, State, Treasury, DoD, DOJ, DOC, DOE, DHS, OMB, ODNI, CIA, NSA, NEC, OSTP, FBI, NIST, CISA	May 4, 2022	Directs agencies involved with quantum computing development to participate in interagency coordination through the NQCO and to prepare for the adoption of quantum-resistant cryptography
Executive Order 14073: Enhancing the National Quantum Initiative Advisory Committee [128]	EOP	May 4, 2022	Establishes an enhanced National Quantum Initiative Advisory Committee to advise the President, the SCQIS, and the ESIX;
Executive Order 14067: Ensuring Responsible Development of Digital Assets [123]	EOP, State, Treasury, DoD, DOJ, DOC, DOE, DHS, OMB, ODNI, CIA, NSA, NEC, OSTP, FBI, NIST, CISA	March 9, 2022	Sets out U.S. policy objectives, coordination mechanisms, and government policies related to digital assets; one provision directs OSTP, the Chief Technology Officer (CTO), and relevant agencies to assess the technical risks of central bank digital currencies (CBDC) with respect to “emerging and future technological developments, such as quantum computing”
National Security Memorandum (NSM-8) on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems [122]	EOP, State, Treasury, DoD, DOJ, DOC, DOE, DHS, OMB, ODNI, CIA, NSA, FBI, CISA	January 19, 2022	Directs agencies to identify any instances of encryption not in compliance with NSA-approved Quantum Resistant Algorithms or CNSA following receival of Advisory Memorandum 01-7

Document	Relevant Federal Agencies	Date	Description
Executive Order 13885: Establishing the National Quantum Initiative Advisory Committee [130]	EOP	August 30, 2019	Established the National Quantum Initiative Advisory Committee to review the NQI

3.3.8. Federal Government Resources for Consumers and Small Businesses to Evaluate the Use of Quantum Computing

Because applications or end uses for QC for consumers or small businesses are currently nascent and a great many are being developed or evaluated, Federal resources to provide consumers or small businesses with information on using QC are limited. NQCO's online repository of technical reports related to QIS provide the public with information about the current state of quantum information science and technologies.

DARPA's Quantum Benchmarking program, described in Section 3.3.3.2, is supporting researchers from multiple sectors to develop quantitative benchmarks of QC performance intended to evaluate the utility of QC systems for specific tasks, along with associated hardware requirements. Other federally supported resources for evaluating the use of QC are targeted at researchers who wish to experiment with early-stage QC technologies, which could include individuals at small businesses or startups, such as those funded through SBIR/STTR programs. The Oak Ridge National Laboratory's Quantum Computing User Program (QCUP) enables researchers to apply for time on quantum computers at IBM, Quantinuum, or Rigetti, and access these commercial QC resources via the cloud [131]. NSF's DCL on supplemental funding for Cloud-Based Access to Quantum Computing also aimed to facilitate access to quantum systems (see Section 3.3.2.3 for more details) [43; 44].

DOE's Advanced Scientific Computing Research (ASCR) program funds Quantum Testbeds for Science, which provide the researchers with "novel, early-stage quantum computing resources" [132]. In 2017, two testbeds, facilities to enable researchers to experiment with different QC implementations, were funded at $56.3 million over 5 years at Lawrence Berkeley National Laboratory (the Advanced Quantum Testbed, with superconducting quantum circuits) [133] and Sandia National Laboratories (the Quantum Scientific Computing Open User Testbed, with trapped ions) [134]. The ASCR testbeds were recently renewed for a second five-year term. In 2021, LPS established a foundry service for gate-based superconducting quantum computing technologies to enable researchers to overcome the high barrier to entry associated with device fabrication. The CHIPS and Science Act of 2022 (P.L. 117–167) authorized the DOE Quantum User Expansion for Science and Technology (QUEST) program, at approximately $166 million over 5 years, to "encourage and facilitate access to United States quantum computing hardware and quantum computing clouds for research purposes" [35]. In coordination with NSF, NIST, SCQIS, and ESIX, the program is intended to provide U.S.-based researchers with access to quantum computing resources through a competitive, merit-reviewed process [135]. As of February 2022, QUEST has not received dedicated appropriations.

3.4. Marketplace and Supply Chain Risks

Today's nascent QC industry can be narrowly defined as companies that make QC systems, which are either sold to end-users or on which time is sold to end-users via cloud services—typically for R&D purposes. The QC supply chain consists of the entities that provide the materials, components, instrumentation, hardware, and software used by the QC industry to develop, manufacture, and operate quantum computers. The specific physical components required vary with the specific type of QC hardware in question, but generally fall into several categories: materials and components comprising the quantum processor itself/ components and instrumentation for performing operations and measurements on the quantum processors; software and other support technologies, for example, to control the environment around the quantum hardware. The QC supply chain currently overlaps that of quantum physics research, and largely depends on a small, disparate scientific research components industry. The early state of the QC industry and the considerable diversity of hardware and approaches to QC create several current and potential challenges to the industry and its upstream supply chain, and as the QC industry matures, a significant portion of its supply chain may need to evolve or be reinvented. As markets mature, a potential future source of supply chain risk could stem from the possibility of anticompetitive conduct or market consolidation; however, these behaviors have not been observed and the associated risk is largely speculative at this stage.

This section presents risks to the domestic QC supply chain identified through interviews with QC subject matter experts across multiple sectors, and using several QED-C research products:

1. A survey of commercial entities in the QC industry on perceived supply chain risks.
2. Recent case studies on two QC-related technologies: (1) superconducting quantum computers and (2) dilution refrigerators, required to reach milli-Kelvin temperatures, that are required for some QC systems.
3. An assessment of the use of critical minerals in QC.

Demand for QC components and systems is currently too low to build a robust QC supply chain or marketplace

At present, limited supplies or vendor options for some QC components create challenges for researchers, developers, and manufacturers to make progress, prolonging uncertainty about future demand for components and instrumentation by the QC industry. However, suppliers of QC components and support technologies are unlikely to ramp up production volumes while current demand is low and future growth remains uncertain. The industry is thus caught in a Catch-22 that inhibits growth in the QC supply chain and marketplace. While this is not an uncommon situation during the early stages of a new industry and tends to work itself out as end-user demand grows, special features of the QC industry create unique challenges to achieving a resilient supply chain.

First, many elements of the QC supply chain are also used by other technology sectors. Because QC-related demand is low, QC system developers usually represent a small share of overall demand in such cases and therefore exercise little buying power.

In addition, some elements of the supply chain for QC system developers are manufactured by a small number of suppliers. Dilution refrigerators, used to achieve the milli-Kelvin temperatures required for the operation of certain QC hardware implementations, are a key example. While there are pockets of expertise in making dilution refrigerators within the United States, effectively only two major commercial suppliers provide them. Both of these companies are located outside of the United States (namely, in the United Kingdom and Finland), and one represents 80 percent of the market share.[56]

Finally, some QC component suppliers are currently unable to meet the specifications QC manufacturers require, and small companies supplying QC components may lack the capacity to scale production. Given these limitations, QC developers often devote a large amount of time and money to managing supplier relationships relative to the financial value of those relationships.

Variations and uncertainty in the performance of commercial QC components can necessitate time-and resource-intensive in-house testing by QC developers

QC system developers often acquire components whose performance at cryogenic temperatures or whose provenance are uncertain. QC companies fear these components will perform sub-optimally because component manufacturers are not designing to QC industry specifications or because standards of production slip in the interest of increasing production volumes. In some cases, QC companies worry that bad actors may deliberately compromise the supply chain.

QC system developers currently assess component performance largely through in-house testing. This process is slow and uneconomical, but at the low volumes associated with R&D, the impact on company costs are not large. As QC system developers scale from R&D volumes to commercial volumes (even low-level commercial volumes), in-house testing could represent a significant cost and production bottleneck.

Half of all respondents to QED-C’s industry survey who anticipated critical materials or hardware-related QC supply chain problems over the next 3 years identified reliable access to key hardware subcomponents as the most critical manufacturing choke point. Of such respondents, 42% indicated that a supply chain problem in this area would slow them down for over a year, and 13% believed it would shut them down for more than a year.

QC R&D and systems require a variety of critical or hard-to-acquire materials

QC technology development uses a variety of specialized materials, including U.S. Government-designated critical minerals such as europium and niobium. In addition, specific isotopes or a high degree of isotopic purity may be needed to create qubits or support technologies (for example, helium-3 is used in the dilution refrigerators that help achieve the milli-Kelvin temperatures required by some QC systems). Given the range of different QC hardware types currently under development and the relatively early stages of QC technologies, a comprehensible list of materials that will prove vital cannot be assembled at this time. In the United States, the DOE Isotopes Program produces, distributes, and conducts R&D for improved production of isotopes needed for QIS R&D [136]. Currently, QC companies obtain some of their hard-to-acquire materials from U.S. Government sources, even when commercial intermediaries are available. The scarcity of these materials—whether due to limited natural abundance or effects of geopolitical conflict on production—is likely to remain a critical challenge to the development of the QC industry, especially if the industry begins to scale.

[56] As determined by a QED-C case study on dilution refrigerators in the QC supply chain.

The domestic supply of QC-trained scientists, engineers, and technical staff may restrict development of the U.S. QC industry

A skilled workforce is essential to the development and long-term success of any industry, even more so for a science-intensive one like QC. A growing QC industry will need staff with highly specialized QC skills and also a range of adjacent skills including engineering, computer science, physics, and business [137]. The QC workforce will need individuals with bachelor's, master's, and doctoral degrees. Graduate programs in several disciplines offer formal training in QC, but the pace at which quantum scientists and engineers graduate may impede progress in QC technology development [138].

A large percentage of recipients of U.S. doctoral degrees in QIS-related disciplines (46% in physics, 69% in electrical engineering, and 61% in computer and information science) are not U.S. citizens. While these graduates are an important part of the U.S. S&T and QIS ecosystems, the U.S. immigration system is often challenging to navigate, which may discourage top talent from joining the U.S. workforce—especially if competitive job opportunities are available elsewhere. A 2021 report from the NSTC Subcommittee on Economic and Security Implications of Quantum Science articulated the importance of foreign talent for QIS in the United States, and recommended general policies to their contributions that balance economic and scientific opportunity with security risks [139]. In January 2022, the White House announced several actions to address these issues for individuals in high-priority STEM fields, including through clarification of guidance for eligibility for and application of relevant programs and updates to associated DHS policy manuals [140].

QC curricula are primarily designed for graduate students; few programs are designed at the undergraduate level or below, or to retrain or upskill technicians for the quantum workforce [141], which may become increasingly important as the industry grows and matures. To help address this shortfall in training programs, several QED-C member companies are developing online training courses. In addition, NSF launched the Quantum Computing & Information Science Faculty Fellows program in 2018, which directly funds faculty lines to increase opportunities for education of the future QC workforce [142] and DOE included QIS topics in its Reaching a New Energy Sciences Workforce (RENEW) activity.[57] The multisector National Q-12 Education Partnership spearheaded by OSTP and NSF was launched in 2020 to nurture educational experiences and environments at the K-12 level to help increase the number and diversity of students with the interest and skills to go into QIS fields [143].

In QED-C's survey of 85 member companies with familiarity with the QC supply chain, more than half of the 47 respondents ranked "lack of skilled workforce" first among "potential external impacts on the QC supply chain." In 2022, the NSTC released the Quantum Information Science and Technology Workforce Development National Strategic Plan for a coordinated approach to building QIS workforce capacity [144].

[57] See https://science.osti.gov/Initiatives/RENEW

Concentration of investment in a subset of potential approaches to quantum computing may restrict investment in other areas

QC is somewhat unique in the number and technological diversity of approaches being pursued to develop commercial products and applications. As of the date of this writing, knowing which approaches will ultimately be successful is not possible. This necessitates a portfolio approach to QC R&D for both government and industry and tradeoffs between which approaches receive funding and investment. These decisions are informed by the current best collective understanding of where the industry and science stand and where the most productive paths are likely to be found. Given the uncertain path of research and innovation, near-term investments might shortchange areas that, in the long run, could prove to be more successful. To the extent that this happens, realization of a commercially viable domestic QC industry and marketplace will be delayed.

Private capital from venture capital firms and corporations may not be available in quantities sufficient to support small companies' participation in the industry

Substantial amounts of venture capital are currently being invested in QC. PitchBook reported estimates of more than $1 billion of venture capital invested in QC startups in 2021 compared to $684 million in 2020 [6]. Continued long-run risk capital investment in QC will require positive returns on the current portfolio of investments, which in turn will require finding commercially important use cases. Large companies can self-fund their QC research if they so choose, but startups rely on outside investment to continue research and develop their business prior to selling products commercially. Should private risk capital investment in QC decrease, U.S. startups would likely suffer, reducing technological diversity and the overall level of innovation in the industry. Despite the large amount of venture capital currently being invested in the QC industry, risk capital may be unavailable to certain segments of the industry, including some upstream QC supplier companies, in quantities sufficient for them to fund growth. Small companies that make the components and instrumentation used to develop and manufacture quantum computers may be particularly disadvantaged. They do not receive the same level of attention from venture capital investors as QC system integrators. These small components and instrumentation makers are an essential part of the QC supply chain.

The daunting challenge of finding commercial applications for QC may lead to a decline in funding for QC R&D necessary to sustain progress

Economically relevant QC use cases for which the technology offers clear, compelling technical advantages over classical approaches are needed for a sustainable QC industry. Although many potential use cases of QC have been identified, it is not yet possible to know when quantum hardware of sufficient scale and performance to support these applications will emerge or how commercially impactful these use cases will be. The longer it takes to identify and implement such uses cases, the more likely U.S. industry participants and the Federal Government will be to reduce investment and funding for QC R&D, which could slow the pace of QIS-related discovery and longer-term innovation.

Restricting the use, sale, or export of QC or support technologies for national security purposes could inhibit progress in open research needed to develop the QC industry

The Federal Government faces a perennial tradeoff between security and market development when enacting export controls and other regulatory restrictions on the business practices of domestic manufacturers. The U.S. National Strategic Overview for Quantum Information Science identifies “maintaining national security and economic growth” as a single policy goal, and explicitly acknowledges the relationship between and need for balance in achieving these two objectives by prioritizing consistent classification and export controls and providing as much information as possible to the research community, consistent with national security needs [145].

3.5. Risks to U.S. National Security, Including Economic Security

The preceding section describes several risks to the U.S. QC industry and its supply chain. In addition to constraining the development of the U.S. QC industry, they may provide the opportunity for foreign governments or third parties to exploit or otherwise interfere with the U.S. supply chain that raises risks to the national security, including economic security, of the United States.

Some QC supply chain components come from foreign suppliers; foreign companies or governments could prevent or otherwise interfere with the export of technology necessary to the QC industry

Companies that manufacture specialized components or instruments or that provide specialized materials to QC system integrators or to their suppliers may choose to limit or prioritize sales, for commercial or other reasons, to select customers within their own nations or regions. Similarly, foreign governments could choose to limit sales of domestically produced technology or materials to overseas entities—and may be more likely to do so reactively should the United States impose its own export controls on QC or related technologies. Where overseas suppliers provide a significant share of a technology or material needed for QC R&D, such restrictions may adversely affect the ability of the U.S. QC industry to obtain needed inputs.

Bad actors in the foreign or domestic QC supply chain could intentionally degrade the performance of components supplied to U.S. industry

Many U.S. QC industry participants spend substantial time and resources ensuring the quality of components they acquire for use in developing and manufacturing their systems. They fear components may perform at lower-than-expected levels of performance because they are selectively provided substandard components by their overseas suppliers, because suppliers intentionally trade off quality to meet market demand, and because some overseas suppliers or other bad actors in the supply chain may intentionally compromise component performance for commercial or strategic reasons, including in ways that could create security risks for the users of these components. Each of these scenarios can compromise the economic performance and security of the U.S. QC industry.

Formal or de facto QC standards may emerge that disadvantage the U.S. QC industry

Standards have a significant effect on what products and processes are viable and even permissible within an industry segment. Standards include those established by law or other government policy, standards set by recognized standards-setting bodies (typically with engagement across sectors and often across nations), and formal and de facto standards established by researchers, developers, practitioners, and industry consortia. When companies' processes or products are not compliant with established standards, they face a tradeoff between losing market share or the potentially high costs of product redesign and process modification. If technical standards are established that are inconsistent with how some or all U.S. QC industry participants conduct their current businesses, these U.S. companies will be forced to address this tradeoff. Foreign companies and foreign governments may attempt to influence standards setting that provides advantages to overseas industry participants at the cost of U.S. participants.

QC is an increasingly global field, and foreign governments can make public investments in developing their domestic quantum computing industries that disadvantage U.S. industry

The United States has long been a leader in QIS and QC R&D. As of 2021, the United States had more QIS startups than any other nation; U.S. companies accounted for nearly half of the patents granted by the U.S. Patent and Trademark Office between 2000 and 2021. However, these fields have become increasingly global. While U.S. researchers were the most productive of any nation in terms of number of peer-reviewed QC research papers published as of 2020, China was a close second; U.S. research papers are more highly cited than those of Chinese researchers, though several European countries' QC researchers are more highly cited than those in the United States.[58] Current leaders in the field come from around the world.

A 2021 report from CIFAR identified 17 countries with national QIS plans or strategies (Austria, China, France, Germany, Hungary, India, Iran, Israel, Japan, the Netherlands, Russia, Singapore, Slovakia, South Korea, Taiwan, the United Kingdom, and the United States) [146], and additional countries have initiated QIS planning activities. Of particular note, China has been developing a national flagship project for QIS R&D since 2016, and QIS is one of seven technology areas indicated as a focus area in China's 14th Five-Year Development Plan, released in 2021 [147].Governments in all countries with significant national capabilities in QC provide funding for QC R&D. This funding comes in a variety of forms and varying levels. One or more foreign governments may make significant public investments in QC that disadvantages the U.S. industry, including through funding research that leads to significant technical breakthroughs or subsidies that allow overseas firms to continue to participate in the quantum marketplace when it would otherwise be unprofitable for them (or U.S. participants) to do so.

Quantum computers are dual-use technologies

Perhaps the best-known potential application of a large-scale, gate-based quantum computer is cryptanalysis to defeat the asymmetric encryption algorithms historically used to protect data at rest and in motion. While new, quantum-resistant encryption standards are expected

[58] According to Scopus searches for the predefined research area of "quantum computing."

to be established by 2024, any adversary that has captured historically encrypted data could in theory read sensitive information if they had access to a large enough quantum computer. Should other security-sensitive use cases arise as QC technologies mature, access to QC systems or cloud services by bad actors could pose a substantial national security threat.

3.6. Recommendations

The American COMPETE Act requests policy recommendations for how the Federal Government can help achieve the following goals:

- Grow the U.S. economy through the secure development of QC.
- Strengthen U.S. global competitiveness through faster and broader adoption of QC.
- Mitigate current and emerging risks to the QC marketplace, supply chain, and workforce.
- Advance the adoption of QC where there are advantages and opportunities to be gained.

This section presents high-level recommendations to help address these goals, based on the industry landscape, risks, and ongoing Federal activities described in Sections 3.3–3.6 of this chapter. Most of these recommendations support more than one of the statutorily enumerated goals. The recommendations are organized around four key challenges that emerged from the research and information-gathering that informed this study. As noted in Section 3.2 of this chapter, information sources included: interviews with QC subject matter experts in industry, academia, and government; QED-C case studies of specific QC-related technologies (superconducting quantum computers and dilution refrigerators); and a review of government QC and related initiatives in the United States and overseas. The recommendations also reflect insights on establishing and implementing effective science and technology policies gained over several decades of economic and policy analysis.

Many Federal Government activities and investments, including those described in the preceding sections, are already addressing some of the challenges facing the QC industry. The government's ongoing support for R&D and infrastructure, national coordination, multisector partnerships, and risk mitigation should be sustained and strengthened in order to help support the development of QC technologies and industry, as described in the following.

Challenge 1: Despite much enthusiasm for the potentially transformative importance of QC, the technology is still in early stages due to the enormity of the science and engineering problems that must be tackled in order to make progress, as discussed in Sections 3.2 and 3.4 of this chapter; fundamental science is still of major importance for long-term progress.

Recommendation 1: The Federal Government should continue to support QC and QC-related R&D across the spectrum from fundamental to applied with a science-first approach in accord with the National Strategic Overview for QIS.

Recommendation 2: The Federal Government should continue its support for and develop strategies towards use-inspired QC R&D aligned with national priorities to work toward practical solutions and stimulate quantum technology development.

Challenge 2: Because of the early stages of the technology, a robust QC supply chain is not yet well established (as noted in Section 3.4 of this chapter), which in turn inhibits the development of use-cases, products, and applications.

Recommendation 3: The Federal Government should continue to support and evaluate the impact of efforts to make quantum computers available to researchers and students at all levels for experimentation, education, and training.

Recommendation 4: The Federal Government should identify additional QC equipment and facilities categories that are expensive, provide high value for research, and are sharable, and consider maintaining such equipment and facilities at central locations—for example, at Federal or National Laboratories.

Recommendation 5: The Federal Government should consider improvements to technology transfer practices at Federal facilities, such as training and incentives for government researchers to enhance the value of their QC patents, better tracking of available government inventions, and simplified and expedited licensing processes and agreements.

Recommendation 6: The Federal Government should consider a centralized certification service to help ensure that high-priority QC components meet user-desired performance standards, for example, through Federal or National Laboratories, or to promote risk-based assessment tools for these components.

Challenge 3: Many players in the QC R&D and innovation ecosystem landscape face difficulties in securing the talent necessary to drive their operations.

Recommendation 7: The Federal Government should continue to support QC-related education and training programs, including characterization of necessary QC-relevant knowledge and skills and associated curriculum development, to broaden the range of individuals positioned for opportunities in the QC industry.

Recommendation 8: The Federal Government should consider QIS and QC as priority fields in its efforts to make it easier for foreign-born individuals who wish to live and work in the United States to contribute to the U.S. innovation ecosystem.

Challenge 4: International competition and security risks that pose concerns to the QC industry and U.S. Government (as discussed in Section 3.5) are at odds with the importance of collaboration and open dissemination of research results for catalyzing progress needed to launch the industry.

Recommendation 9: The Federal Government should establish a mechanism for regularly assessing and stress-testing potential risks to the QC supply chain, to include characterization of key components and their available sources and suppliers, to inform potential decisions about use restrictions and domestic production or research and engineering for alternative technical approaches.

Recommendation 10: While acknowledging the place of technology protections, regulations and export controls, the Federal Government should consider the implications of such controls and regulations on the progress of QC R&D in its decision making.

Recommendation 11: The Federal Government should continue to support the development of PQC algorithms, protocols, and standards, and support and collaborate with industry and open-source developers to facilitate a smooth and timely transition to PQC deployment.

References

[1] Consolidated Appropriations Act, 2021. H.R.133. U.S. Congress. December 27, 2020. https://www.congress.gov/bill/116th-congress/house-bill/133/text.

[2] QED-C. “Home - QED-C.” Accessed July 8, 2022. https://quantumconsortium.org/.

[3] National Academies of Sciences, Engineering, and Medicine. *Quantum Computing: Progress and Prospects.* A consensus study report of the National Academies of Sciences, Engineering, Medicine. Washington, DC: The National Academies Press, 2019. https://doi.org/10.17226/25196.

[4] Subcommittee on Quantum Information Science. “National Quantum Initiative Supplement to the President's FY 2023 Budget.” January 2023. https://www.quantum.gov/wp-content/uploads/2023/01/NQI-Annual-Report-FY2023.pdf.

[5] Candelon, François, Jean-François Bobier, Maxime Courtaux, and Gabriel Nahas. “Can Europe Catch up with the US (And China) In Quantum Computing?,” Boston Consulting Group Henderson Institute, August 2022.

[6] Temkin, Marina. “Investors Bet on the Technologically Unproven Field of Quantum Computing.” Accessed May 12, 2022. https://pitchbook.com/news/articles/quantum-computing-venture-capital-funding.

[7] Bob Sorensen. “Sizing the Global Quantum Computing Market Landscape 2021.” Q2B 2021, December 07, 2021.

[8] National Quantum Initiative Act. NQI Act. U.S. Congress. December 21, 2018.

[9] NIST. “NIST Launches Consortium to Support Development of Quantum Industry.” Accessed June 16, 2022. https://www.nist.gov/news-events/news/2018/09/nist-launches-consortium-support-development-quantum-industry.

[10] QED-C. “QED-C Members | QED-C.” Accessed February 2, 2023. https://quantumconsortium.org/members/.

[11] National Quantum Coordination Office. “National Quantum Initiative Supplement to the President's FY 2022 Budget.” 2021. Accessed October 12, 2022. https://www.quantum.gov/wp-content/uploads/2021/12/NQI-Annual-Report-FY2022.pdf.

[12] JILA. “About JILA.” Accessed September 14, 2022. https://jila.colorado.edu/about/about-jila.

[13] JILA. “Quantum Information Science & Technology.” Accessed September 14, 2022. https://jila.colorado.edu/research/quantum-information-science-technology.

[14] JILA - The Anderson Group. “Neutral Atom Quantum Computing | JILA - Exploring the Frontiers of Physics.” Accessed September 15, 2022. https://jila.colorado.edu/dzanderson/research/neutral-atom-quantum-computing.

[15] JILA - The Sun Group. “Optical Quantum Computing.” Accessed September 15, 2022. https://jila.colorado.edu/sun/research/optical-quantum-computing.

[16] JILA - The Lewandowski Group. “Quantum Workforce Development.” Accessed September 15, 2022. https://jila.colorado.edu/lewandowski/research/quantum-workforce-development.

[17] CUbit Quantum Initiative. “Boulder Cryogenic Quantum Testbed.” Accessed February 12, 2023. https://www.colorado.edu/initiative/cubit/.

[18] Strain, Daniel. “New Boulder Facility to Help Pave the Way for Quantum Computers.” *CU Boulder Today*, October 15, 2019. Accessed October 12, 2022. https://www.colorado.edu/today/2019/10/03/new-boulder-facility-help-pave-way-quantum-computers.

[19] University of Colorado Boulder. “Partnerships for Informal Science Education in the Community.” Accessed September 16, 2022. https://www.colorado.edu/outreach/pisec/.

[20] JILA. “Education & Outreach.” Accessed September 16, 2022. https://jila.colorado.edu/outreach/education-outreach.

[21] Joint Quantum Institute. “About the Joint Quantum Institute.” Accessed September 14, 2022. https://jqi.umd.edu/about.

[22] Joint Quantum Institute. “About the Joint Quantum Institute.” Accessed February 2, 2023. https://jqi.umd.edu/about.

[23] National Institute of Standards and Technology. “Joint Quantum Institute Created by University of Maryland, NIST and NSA.” News release. September 11, 2006. https://www.nist.gov/news-events/news/2006/09/joint-quantum-institute-created-university-maryland-nist-and-nsa.

[24] Emily Edwards. “JQI Scientists Monroe and Gorshkov Are Part of a New, $15 Million NSF Quantum Computing Project.” News release. August 8, 2018. Accessed September 15, 2022. https://jqi.umd.edu/news/jqi-scientists-monroe-and-gorshkov-are-part-new-15-million-nsf-quantum-computing-project.

[25] Emily Edwards. “Ions Clear Another Hurdle Toward Scaled-up Quantum Computing.” News release. August 16, 2019. Accessed September 15, 2022. https://jqi.umd.edu/news/ions-clear-another-hurdle-toward-scaled-quantum-computing.

[26] C. Zandonella. “Rice-Sized Laser, Powered One Electron at a Time, Bodes Well for Quantum Computing.” News release. May 14, 2015. Accessed September 15, 2022. https://jqi.umd.edu/news/rice-sized-laser-powered-one-electron-time-bodes-well-quantum-computing.

[27] Joint Quantum Institute. “Outreach.” Accessed September 16, 2022. https://jqi.umd.edu/outreach-education.

[28] NIST. “UMD and NIST Announce the Creation of the Joint Center for Quantum Information and Computer Science | NIST.” 2014. Accessed October 13, 2022. https://www.nist.gov/news-events/news/2014/10/umd-and-nist-announce-creation-joint-center-quantum-information-and.

[29] University of Maryland. “Research | QuICS.” Accessed October 13, 2022. https://quics.umd.edu/research.

[30] National Science Foundation. “Bringing You the Quantum Future-Faster.” Accessed February 2, 2023. https://beta.nsf.gov/science-matters/bringing-you-quantum-future-faster.

[31] Ambrose, Mitch. “NSF Budget: FY22 Outcomes and FY2023 Request.” Accessed February 2, 2023. https://www.aip.org/fyi/2022/nsf-budget-fy22-outcomes-and-fy23-request#:~:text=workforce%20diversity%20initiatives.-,Congress%20increased%20the%20National%20Science%20Foundation's%20budget%20by%204%25%20to,20%25%20increase%20to%20%2410.5%20billion.

[32] National Science Foundation. “NSF Announces Quantum Leap Challenge Institutes for Biological Sensing and Quantum Simulation.” News release. June 16, 2022. Accessed June 16, 2022. https://www.nsf.gov/news/special_reports/announcements/090221.jsp.

[33] National Science Foundation. “NSF Establishes 3 New Institutes to Address Critical Challenges in Quantum Information Science.” News release. June 16, 2022. Accessed June 16, 2022. https://www.nsf.gov/news/special_reports/announcements/072120.jsp.

[34] Challenge Institute for Quantum Computation. “Research - Overview.” Accessed February 2, 2023. https://ciqc.berkeley.edu/overview.

[35] Challenge Institute for Quantum Computation. “Workforce Development.” Accessed February 2, 2023. https://ciqc.berkeley.edu/workforce-development.

[36] Challenge Institute for Quantum Computation. “CIQC Research Exchange Program.” Accessed February 2, 2023. https://ciqc.berkeley.edu/researchexchange.

[37] University of Maryland. “The NSF Quantum Leap Challenge Institute for Robust Quantum Simulation.” Accessed February 2, 2023. https://rqs.umd.edu/.

[38] University of Maryland. “About the Institute for Robust Quantum Simulation.” Accessed February 2, 2023. https://rqs.umd.edu/about/.

[39] University of Illinois Urbana-Champaign - The Grainger College of Engineering. “About.” Accessed February 2, 2023. https://hqan.illinois.edu/about.

[40] University of Illinois Urbana-Champaign - The Grainger College of Engineering. “HQAN Exchange Program.” Accessed February 2, 2023. https://hqan.illinois.edu/education-and-workforce/exchanges.

[41] University of Illinois Urbana-Champaign - The Grainger College of Engineering. “HQAN Internship Program.” Accessed February 2, 2023. https://hqan.illinois.edu/education-and-workforce/internship.

[42] University of Illinois Urbana-Champaign - The Grainger College of Engineering. “TeachQuantum.” Accessed February 2, 2023. https://hqan.illinois.edu/education-and-workforce/TeachQuantum.

[43] Martonosi, Margaret, Sean Jones, Susan Marguiles, and Erwin Gianchandani. “Enabling Quantum Computing Platform Access for National Science Foundation Researchers with Amazon Web Services, IBM, and Microsoft Quantum.” News release. October 12, 2022. Accessed October 12, 2022. https://beta.nsf.gov/funding/opportunities/enabling-quantum-computing-platform-access-0.

[44] National Science Foundation. “Dear Colleague Letter: Enabling Quantum Computing Platform Access for National Science Foundation Researchers with Amazon Web Services, IBM, and Microsoft Quantum (Nsf22092) | NSF - National Science Foundation.” Accessed February 6, 2023. https://www.nsf.gov/pubs/2022/nsf22092/nsf22092.jsp.

[45] Department of Energy. “Department of Energy Announces $625 Million for New Quantum Centers.” News release. January 10, 2020. Accessed June 16, 2022. https://www.energy.gov/articles/department-energy-announces-625-million-new-quantum-centers.

[46] Department of Energy. “White House Office of Technology Policy, National Science Foundation and Department of Energy Announce over $1 Billion in Awards

for Artificial Intelligence and Quantum Information Science Research Institutes." News release. August 26, 2020. Accessed June 16, 2022. https://www.energy.gov/articles/white-house-office-technology-policy-national-science-foundation-and-department-energy.

[47] National Defense Authorization Act for Fiscal Year 2020. Public Law 116-92. U.S. Congress. 2019. Accessed July 5, 2022. https://www.congress.gov/116/plaws/publ92/PLAW-116publ92.pdf.

[48] The White House. "Readout: National Quantum Initiative Centers Summit." News release. December 5, 2022. Accessed January 27, 2023. https://www.whitehouse.gov/ostp/news-updates/2022/12/05/readout-national-quantum-initiative-centers-summit/.

[49] Heck, Leslie. "Air Force Research Laboratory Designated as Quantum Information Science Research Center for U.S. Air Force and U.S. Space Force." News release. August 9, 2021. Accessed January 27, 2023. https://www.afrl.af.mil/News/Article/2724770/air-force-research-laboratory-designated-as-quantum-information-science-researc/.

[50] Cage, Paul. "NRL Designated Navy's Quantum Information Research Center." News release. September 28, 2020. Accessed January 27, 2023. https://www.nrl.navy.mil/Media/News/Article/2368962/nrl-designated-navys-quantum-information-research-center/.

[51] Laboratory for Physical Science Qubit Collaboratory. "LPS Announces First-Ever Qubit Collaboratory." News release. October 29, 2020. Accessed January 23, 2023. https://www.qubitcollaboratory.org/lps-announces-1st-qubit-collaboratory/?preview_id=2015&et_fb=1&PageSpeed=off.

[52] Griffiss Institute. "Innovare Advancement Center Launches '$1M International Quantum U Tech Accelerator' | Griffiss Institute." Accessed July 6, 2022. https://www.griffissinstitute.org/about-us/gi-news/news-story/innovare-advancement-center-led-by-air-force-research-laboratory-info-launches-1m-international-quantum-u-tech-accelerator.

[53] Innovare. "About Innovare." Accessed July 6, 2022. https://www.innovare.org/about-innovare.

[54] Innovare. "Facility." Accessed July 6, 2022. https://www.innovare.org/facility.

[55] Innovare. "Partnerships." Accessed July 6, 2022. https://www.innovare.org/partnerships.

[56] National Security Agency/Central Security Service. "NSA Launches LPS Qubit Collaboratory." Accessed February 7, 2023. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/2570949/nsa-launches-lps-qubit-collaboratory/.

[57] Laboratory for Physical Science Qubit Collaboratory. "LQC Research Thrusts." Accessed February 2, 2023. https://www.qubitcollaboratory.org/lqc-open-baa/.

[58] Laboratory for Physical Science Qubit Collaboratory. "2022 Short Course OVerview." Accessed February 2, 2023. https://www.qubitcollaboratory.org/soq-recap/?et_fb=1&PageSpeed=off.

[59] NSF Challenge Institute for Quantum Computation. "NSF Challenge Institute for Quantum Computation." https://ciqc.berkeley.edu/.

[60] NSF Challenge Institute for Quantum Computation. “Partnerships — NSF Challenge Institute for Quantum Computation.” Accessed February 6, 2023. https://ciqc.berkeley.edu/com-partnerships.

[61] University of Maryland. “The NSF Quantum Leap Challenge Institute for Robust Quantum Simulation.” https://rqs.umd.edu/.

[62] University of Illinois Urbana-Champaign - The Grainger College of Engineering. “Hybrid Quantum Architectures and Networks.” https://hqan.illinois.edu/.

[63] University of Colorado Boulder. “Q-Sense: Quantum Systems Through Entangled Science and Engineering: Partners.” https://www.colorado.edu/research/qsense/partners.

[64] University of Chicago. “NSF Quantum Sensing for Biophysics and Bioengineering.” https://qubbe.uchicago.edu/.

[65] Q-Next. “Partners.” https://q-next.org/partners/.

[66] Co-design Center for Quantum Advantage. “Team Leaders and Partner Institutions.” https://www.bnl.gov/quantumcenter/team.php.

[67] Fermilab. “Superconducting Quantum Materials and Systems Center - Partners.” https://sqmscenter.fnal.gov/about/our-partners/.

[68] Quantum Systems Accelerator. “Quantum Systems Accelerator.” https://quantumsystemsaccelerator.org/.

[69] Quantum Science Center. “Quantum Science Center.” https://qscience.org/.

[70] National Q-12 Education Partnership. “About.” Accessed October 12, 2022. https://q12education.org/about.

[71] National Q-12 Education Partnership. “QIS Key Concepts for Early Learners: K-12 Framework.” Accessed October 12, 2022. https://q12education.org/learning-materials-framework.

[72] National Q-12 Education Partnership. “Learning and Teaching Quantum Information Science and Engineering (QISE) - Resources.” Accessed October 12, 2022. https://q12education.org/learning-materials.

[73] HPCwire. “Launching of the European Quantum Industry Consortium.” News release. April 19, 2021. Accessed June 16, 2022. https://www.hpcwire.com/off-the-wire/launching-of-the-european-quantum-industry-consortium/.

[74] Från, Nyheter. “The Netherlands Invests 615 Million Euros in Quantum Delta NL, Bringing Quantum Technology to the Next Level in Europe.” April 12, 2021. Accessed June 16, 2022. https://www.prnewswire.com/sv/pressmeddelanden/the-netherlands-invests-615-million-euros-in-quantum-delta-nl-bringing-quantum-technology-to-the-next-level-in-europe-871329561.html.

[75] Barbaschow, Asha. “25-Member Q-STAR Quantum Alliance to Boost Japan's Competitive Advantage.” *ZDNet*, September 1, 2021. Accessed June 16, 2022. https://www.zdnet.com/article/25-member-q-star-quantum-alliance-to-boost-japans-competitive-advantage/.

[76] UK National Quantum Technologies Programme. “Our Programme.” Accessed June 16, 2022. https://uknqt.ukri.org/our-programme/.

[77] Quantum Computing & Simulation Hub. “About the Hub.” Accessed June 16, 2022. https://www.qcshub.org/the-hub.

[78] Institute of Electrical and Electronics Engineers. “IEEE at a Glance.” Accessed June 16, 2022. https://www.ieee.org/about/at-a-

glance.html?utm_source=linkslist_text&utm_medium=lp-about&utm_campaign=at-a-glance.

[79] IEEE Quantum. “Standards - IEEE Quantum.” Accessed June 16, 2022. https://quantum.ieee.org/standards.

[80] International Electrotechnical Commission. “ISO/IEC JTC 1 Subcommittee(S) And/or Working Group(S).” Accessed June 16, 2022. https://www.iec.ch/ords/f?p=103:29:201886398367410::::FSP_ORG_ID,FSP_LANG_ID:3387,25#1.

[81] IEEE SA. “IEEE P3155 - Programmable Quantum Simulator Working Group.” Accessed June 16, 2022. https://sagroups.ieee.org/3155/.

[82] IEEE SA. “IEEE P2995 - Quantum Algorithm Design and Development Working Group.” Accessed June 16, 2022. https://sagroups.ieee.org/quadd/.

[83] Institute of Electrical and Electronics Engineers Standards Association. “P7130 Standard for Quantum Technologies Definitions.” Accessed May 5, 2022. https://standards.ieee.org/ieee/7130/10680/.

[84] CENELEC FGQT. “Quantum Technologies.” Accessed July 7, 2022. https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/quantum-technologies.

[85] CEN-CENELEC. “Quantum Technologies.” Accessed June 16, 2022. https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/quantum-technologies/.

[86] Internet Engineering Task Force. “Quantum Internet Research Group (Qirg).” Accessed June 16, 2022. https://datatracker.ietf.org/rg/qirg/about/.

[87] IETF. “Hybrid Key Exchange in TLS 1.3.” Accessed November 8, 2022. https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/05/.

[88] IETF. “Internet X.509 Public Key Infrastructure: Algorithm Identifiers for Dilithium.” Accessed November 8, 2022. https://datatracker.ietf.org/doc/draft-ietf-lamps-dilithium-certificates/.

[89] British Standards Institution. “New ICT/1/1/2 Quantum Technology Panel.” Accessed June 16, 2022. https://www.bsigroup.com/en-GB/industries-and-sectors/quantum-technology/.

[90] DigiChina. “Translation: 14th Five-Year Plan for National Informatization.” Accessed June 16, 2022. https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national-informatization-dec-2021/.

[91] Cross, Andrew W., Lev S. Bishop, Sarah Sheldon, Paul D. Nation, and Jay M. Gambetta. “Validating Quantum Computers Using Randomized Model Circuits.” *Physical Review A* 100, no. 3 (2019). https://doi.org/10.1103/PhysRevA.100.032328. https://arxiv.org/pdf/1811.12926.

[92] IBM Research Blog. “Pushing Quantum Performance Forward with Our Highest Quantum Volume yet.” Accessed May 23, 2022. https://research.ibm.com/blog/quantum-volume-256.

[93] The Qiskit. “Measuring Quantum Volume.” Accessed May 23, 2022. https://qiskit.org/textbook/ch-quantum-hardware/measuring-quantum-volume.html.

[94] Lubinski, Thomas, Sonika Johri, Paul Varosy, Jeremiah Coleman, Luning Zhao, Jason Necaise, Charles H. Baldwin, Karl Mayer, and Timothy Proctor. “Application-Oriented Performance Benchmarks for Quantum Computing.” October 6, 2021. https://arxiv.org/pdf/2110.03137.

[95] Defense Advanced Research Projects Agency. "Quantum Benchmarking." Accessed February 7, 2023. https://www.darpa.mil/program/quantum-benchmarking.

[96] BusinessWire. "Zapata Computing Earns DARPA Award for Quantum Benchmarking." Accessed February 7, 2023. https://www.businesswire.com/news/home/20220329005302/en/.

[97] Keller, John. "DARPA Asks Raytheon BBN and USC Researchers to Test Limits of Quantum Computing for Military Applications." *Military Aerospace*, March 3, 2022. Accessed February 7, 2023. https://www.militaryaerospace.com/computers/article/14234944/quantum-computing-military-applications-test.

[98] QED-C. "Practical Intermediate Representation for Quantum (PIRQ): Requirements and Near-Term Recommendations." February 28, 2022. https://quantumconsortium.org/pirq22/.

[99] QIR Alliance. "QIR Alliance | Github." https://github.com/qir-alliance.

[100] GitHub. "GitHub - Riverlane/QHAL: [DEPRECATED] A Quantum Hardware Abstraction Layer Developed in the Context of UK ISCF Consortium." Accessed July 7, 2022. https://github.com/riverlane/QHAL/blob/main/README.md.

[101] Riverlane, and National Physical Laboratory. "Riverlane/QHAL: A Quantum Hardware Abstraction Layer." Accessed May 20, 2022. https://github.com/riverlane/QHAL.

[102] IEEE Standards Association. "IEEE SA - Standard for Quantum Computing Architecture." Accessed June 16, 2022. https://standards.ieee.org/ieee/3120/10751/.

[103] Institute of Electrical and Electronics Engineers Standards Association. "IEEE P2995 Trial-Use Standard for a Quantum Algorithm Design and Development." Accessed May 5, 2022. https://standards.ieee.org/ieee/2995/10633/.

[104] International Organization for Standardization. "ISO/IEC AWI TR 18157." Accessed July 7, 2022. https://www.iso.org/standard/85203.html.

[105] International Organization for Standardization. "ISO/IEC CD 4879." Accessed July 7, 2022. https://www.iso.org/standard/80432.html.

[106] CENELEC FGQT. "FGQT Q03: Towards Standardization for Quantum Technologies." CENELEC FGQT, 2022. https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/quantum-technologies/#:~:text=The%20Focus%20Group%20ensures%20the,of%20such%20technologies%20in%20industry.

[107] IEEE SA. "IEEE SA - Standard for Quantum Computing Performance Metrics & Performance Benchmarking." Accessed July 7, 2022. https://standards.ieee.org/ieee/7131/10681/.

[108] The White House. "White House Office of Science & Technology Policy and U.S. National Science Foundation Host "Quantum Workforce: Q-12 Actions for Community Growth" Event, Release Quantum Workforce Development Plan." News release. February 1, 2022. Accessed April 12, 2022. https://www.whitehouse.gov/ostp/news-updates/2021/10/07/readout-of-white-house-summit-on-quantum-industry-and-society/.

[109] The White House. "Readout of White House Summit on Quantum Industry and Society." News release. October 8, 2021. Accessed April 12, 2022.

https://www.whitehouse.gov/ostp/news-updates/2021/10/07/readout-of-white-house-summit-on-quantum-industry-and-society/.

[110] National Quantum Coordination Office. “Summary of Workshop on Quantum Recruitment in the Federal Government.” January 2022. https://www.nasa.gov/directorates/heo/scan/engineering/technology/quantum_communications_workshop_proceedings.

[111] National Quantum Initiative. “The National Quantum Coordination Office.” Accessed April 18, 2022. https://www.quantum.gov/nqco/.

[112] National Quantum Initiative. “About.” Accessed April 18, 2022. https://www.quantum.gov/about/.

[113] Subcommittee on Quantum Information Science Committee on Science of the National Science & Technology Council. “Bringing Quantum Sensors to Fruition.” March 2022.

[114] Subcommittee on the Economic and Security Implications of Quantum Science. “THE ROLE of INTERNATIONAL TALENT in QUANTUM INFORMATION SCIENCE.” 2021. https://www.quantum.gov/wp-content/uploads/2021/10/2021_NSTC_ESIX_INTL_TALENT_QIS.pdf.

[115] National Defense Authorization Act for Fiscal Year 2022. NDAA FY2022. U.S. Congress. December 27, 2021.

[116] Charles Tahan. “National Strategy for Quantum Information Science.” Office of Science and Technology Policy, October 27, 2020.

[117] National Quantum Coordination Office. Interview by Science and Technology Policy Institute (STPI). April 22, 2022.

[118] Subcommittee on Quantum Information Science Committee on Science of the National Science & Technology Council. “Quantum Information Science and Technology Workforce Development National Strategic Plan.” February 2022.

[119] Subcommittee on Quantum Information Science Committee on Science of the National Science & Technology Council. “A Coordinated Approach to Quantum Networking Research.” January 2021.

[120] Subcommittee on Quantum Information Science under the Committee on Science of the National Science & Technology Council. “National Strategic Overview for Quantum Information Science.” https://www.quantum.gov/wp-content/uploads/2020/10/2018_NSTC_National_Strategic_Overview_QIS.pdf.

[121] National Institute of Standards and Technology. “Post-Quantum Cryptography Standardization - Post-Quantum Cryptography | CSRC.” Accessed May 12, 2022. https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization.

[122] Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems. Executive Office of the President The White House. January 19, 2022. Accessed April 18, 2022. https://www.govinfo.gov/app/details/DCPD-202200025.

[123] Executive Order on Ensuring Responsible Development of Digital Assets. EO 14067. Executive Office of the President The White House. March 9, 2022. Accessed April 18, 2022. https://www.federalregister.gov/documents/2022/03/14/2022-05471/ensuring-responsible-development-of-digital-assets.

[124] Executive Office of the President. “National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems.” May 4, 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/.

[125] National Institute of Standards and Technology. “Announcing PQC Candidates to Be Standardized, Plus Fourth Round Candidates | CSRC.” Accessed July 7, 2022. https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4.

[126] Preparing for Post-Quantum Cryptography Memorandum. U.S. Department of Homeland Security. September 17, 2021. Accessed April 22, 2022. https://www.dhs.gov/sites/default/files/publications/usm_quantum_memo_0.pdf.

[127] National Security Agency, and Central Security Service. “Post-Quantum Cybersecurity Resources.” Accessed January 10, 2023. https://www.nsa.gov/Cybersecurity/Post-Quantum-Cybersecurity-Resources/#g.

[128] House, The White. “Executive Order on Enhancing the National Quantum Initiative Advisory Committee.” *The White House*, May 4, 2022. Accessed February 7, 2023. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/05/04/executive-order-on-enhancing-the-national-quantum-initiative-advisory-committee/.

[129] National Quantum Initiative. “Enhancing Competitiveness.” Accessed February 7, 2023. https://www.quantum.gov/competitiveness/#INTERNATIONAL-COOPERATION.

[130] Executive Order on Establishing the National Quantum Initiative Advisory Committee. EO 13885. Executive Office of the President. August 30, 2019. Accessed April 20, 2022. https://www.federalregister.gov/documents/2019/09/05/2019-19367/establishing-the-national-quantum-initiative-advisory-committee.

[131] Oak Ridge National Laboratory. “Quantum Computing User Support Documentation.” Accessed May 19, 2022. https://www.olcf.ornl.gov/olcf-resources/compute-systems/quantum-computing-user-program/quantum-computing-user-support-documentation.

[132] Department of Energy. “Advanced Scientific Computing Research (About).” Accessed May 19, 2022. https://science.osti.gov/ascr/About.

[133] Lawrence Berkeley National Lab. “Advanced Quantum Computing Testbed.” Accessed July 7, 2022. https://aqt.lbl.gov/.

[134] Claire Cramer. “Quantum Testbeds Update.” January 13, 2020. Accessed May 19, 2022. https://science.osti.gov/-/media/ascr/ascac/pdf/meetings/202001/QuantumTestbedUpdate_ASCAC_202001.pdf?la=en&hash=40A96E993B74EB75720B98F5EEEABE0BD2C93349.

[135] “CHIPS and Science Act.” In *Public Law.* 15 U.S.C. 8854. Accessed February 6, 2023. https://www.congress.gov/bill/117th-congress/house-bill/4346/text.

[136] Department of Energy. “ISOTOPE RESEARCH DEVELOPMENT and… | U.S. DOE Office of Science(SC).” Accessed July 4, 2022.

https://science.osti.gov/Isotope-Research-Development-and-Production/Research/Quantum-Information-Science.

[137] Hughes, Ciaran, Doug Finke, Dan-Adrian German, Celia Merzbacher, Patrick M. Vora, and H. J. Lewandowski. "Assessing the Needs of the Quantum Industry." August 25, 2021. https://arxiv.org/pdf/2109.03601.

[138] Chuck Leddy. "Q&A: The Talent Shortage in Quantum Computing." *MIT Department of Physics*, January 23, 2019. Accessed May 20, 2022. https://physics.mit.edu/news/qa-the-talent-shortage-in-quantum-computing/.

[139] Subcommittee on Economic and Security Implications of Quantum Science, Committee on Homeland and National Security, National Science & Technology Council. "The Role of International Talent in Quantum Information Science." October 2021.

[140] The White House. "Fact Sheet: Biden-Harris Administration Actions to Attract STEM Talent and Strengthen Our Economy and Competitiveness." *The White House*, January 21, 2022. Accessed November 21, 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/21/fact-sheet-biden-harris-administration-actions-to-attract-stem-talent-and-strengthen-our-economy-and-competitiveness/.

[141] Hasanovic, Mo, Chrys Panayiotou, Donn Silberman, Paul Stimers, and Celia Merzbacher. "Quantum Technician Skills and Competencies for the Emerging Quantum 2.0 Industry." *Optical Engineering* 61, no. 08 (2022). https://doi.org/10.1117/1.OE.61.8.081803.

[142] National Science Foundation. "NSF Quantum Computing & Information Science Faculty Fellows (QCIS-FF) (Nsf19507) | NSF – National Science Foundation." Accessed February 7, 2023. https://www.nsf.gov/pubs/2019/nsf19507/nsf19507.htm.

[143] "National Q-12 Education Partnership." Accessed July 4, 2022. https://q12education.org/.

[144] NSTC Subcommittee on Quantum Information Science. "QIST Workforce Development." Washington, DC, February 2022. https://www.quantum.gov/wp-content/uploads/2022/02/QIST-Natl-Workforce-Plan.pdf.

[145] Subcommittee on Quantum Information Science under the Committee on Science of the National Science & Technology Council. "National Strategic Overview for Quantum Information Science." September 2018. https://www.quantum.gov/wp-content/uploads/2020/10/2018_NSTC_National_Strategic_Overview_QIS.pdf.

[146] Johnny Kung, PhD, and and Muriam Fancy. "A Quantum Revolution - Report on Global Policies for Quantum Technology." Accessed October 13, 2022. https://cifar.ca/wp-content/uploads/2021/05/QuantumReport-EN-May2021.pdf.

[147] Zhang, Qiang, Feihu Xu, Li Li, Nai-Le Liu, and Jian-Wei Pan. "Quantum Information Research in China." *Quantum Science and Technology* 4, no. 4 (2019): 40503. Accessed October 13, 2022. https://doi.org/10.1088/2058-9565/ab4bea. https://iopscience.iop.org/article/10.1088/2058-9565/ab4bea/pdf.

Appendix H. Abbreviations

ACT	Agreements for Commercializing Technology
ADA	Americans with Disabilities Act
ASCR	Advanced Scientific Computing Research
BSI	British Standards Institution
CBDC	central Bank Digital Currencies
CEN	Committee for Standardization
CENELEC	Committee for Electrotechnical Standardization
CIQC	Challenge Institute for Quantum Computation
CPU	Central Processing Unit
CQE	Chicago Quantum Exchange
CRADA	Cooperative Research and Development Agreement
CRQC	Cryptographically-Relevant Quantum Computing
CTO	Chief Technology Officer
DARPA	Defense Advanced Research Projects Agency
DCL	Dear Colleague Letter
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
ETSI	European Telecommunications Standards Institute
GPU	Graphical Processing Units
HQAN	Hybrid Quantum Architectures and Networks
IARPA	Intelligence Advanced Research Projects Agency
IEC	International Electrotechnical Commission
IEEE SA	Institute of Electrical and Electronics Engineers Standards Association
IETF	Internet Engineering Task Force
IRTF	Internet Research Task Force
JQI	Joint Quantum Institute
JTC-1	Joint Technical Committee on information technology
LQC	Laboratory for Physical Science Qubit Collaboratory
NAICS	North American Industry Classification System
NDAA	National Defense Authorization Act
NIST	National Institute of Standards and Technology
NQCO	National Quantum Coordination Office
NQI	National Quantum Initiative
NQIA	National Quantum Initiative Act
NSA	National Security Agency
NSF	National Science Foundation
NSTC	National Science and Technology Council
OPT	Optional Practical Training
OSTP	White House Office of Science and Technology Policy
OTA	Other Transaction Agreement

PISEC	Partnerships for Informal Science Education in the Community
PPP	Public-Private Partnerships
PQC	Post-Quantum Cryptography
QC	Quantum Computing
QCUP	Quantum Computing User Program
QECC	Quantum Error Correction Codes
QED-C	Quantum Economic Development Consortium
QHAL	QC hardware abstraction layer for quantum computers
QIS	Quantum Information Science
QISRC	QIS Research Center
QIST	Quantum Information Science and Technology
QLCI	Quantum Leap Challenge Institute
QUEST	Quantum User Expansion for Science and Technology
QuIC	Quantum Industry Consortium
QuICS	Joint Center for Quantum Information and Computer Science
R&D	Research and Development
SCQIS	Subcommittees on Quantum Information Science
SDO	Standards Development Organization
SPP	Strategic Partnership Project
STAQ	Software-Tailored Architecture for Quantum co-design
TAC	Technical Advisory Committee

Appendix I. *American COMPETE Act* Quantum Computing Text

(d) STUDY TO ADVANCE QUANTUM COMPUTING.—

(1) IN GENERAL.—

(A) STUDY REQUIRED.—Not later than 1 year after the date of enactment of this Act, the Secretary of Commerce and the Federal Trade Commission shall complete a study on the state of the quantum computing industry and the impact of such industry on the United States economy.

(B) REQUIREMENTS FOR STUDY.—In conducting the study, the Secretary and the Commission shall—

(i) develop and conduct a survey of the quantum computing industry through outreach to participating entities as appropriate to—

(I) establish a list of industry sectors that implement and promote the use of quantum computing;

(II) establish a list of public-private partnerships focused on promoting the adoption and use of quantum computing, as well as industry-based bodies, including international bodies, which have developed, or are developing, mandatory or voluntary standards for quantum computing;

(III) the status of such industry-based mandatory or voluntary standards; and

(IV) provide a description of the ways entities or industry sectors implement and promote the use of quantum computing;

(ii) develop a comprehensive list of Federal agencies with jurisdiction over the entities and industry sectors identified under clause (i);

(iii) identify which Federal agency or agencies listed under clause (ii) each entity or industry sector interacts with;

(iv) identify all interagency activities that are taking place among the Federal agencies listed under clause (ii), such as working groups or other coordinated efforts;

(v) develop a brief description of the jurisdiction and expertise of the Federal agencies listed under clause (ii) with regard to such entities and industry sectors;

(vi) identify all regulations, guidelines, mandatory standards, voluntary standards, and other policies implemented by each of the Federal agencies identified under clause (ii), as well as all guidelines, mandatory standards, voluntary standards, and other policies implemented by industry-based bodies;

(vii) identify Federal Government resources that exist for consumers and small businesses to evaluate the use of quantum computing; and

(viii) consult with the Office of Science and Technology Policy and interagency efforts on quantum authorized by sections 102 and 103 of the National Quantum Initiative Act (Public Law 115–368) to minimize duplication of activities in this subparagraph among the Federal agencies listed under clause (ii).

(2) MARKETPLACE AND SUPPLY CHAIN SURVEY.—The Secretary and Commission shall conduct a survey of the marketplace and supply chain of quantum computing to—

(A) assess the severity of risks posed to such marketplace and supply chain;

(B) review the ability of foreign governments or third parties to exploit the supply chain in a manner that raises risks to the economic and national security of the United States; and

(C) identify emerging risks and long-term trends in such marketplace and supply chain.

(3) REPORT TO CONGRESS.—Not later than 6 months after the completion of the study required pursuant to paragraph (1), the Secretary and the Commission shall submit to the Committee on Energy and Commerce and the Committee on Science, Space, and Technology of the House of Representatives, and the Committee on Commerce, Science, and Transportation of the Senate, and make publicly available on their respective websites, a report that contains—

(A) the results of the study conducted pursuant to paragraph (1) and the survey conducted pursuant to paragraph (2); and

(B) recommendations to—

(i) grow the United States economy through the secure advancement of quantum computing;

(ii) develop a national strategy to advance the United States business sectors' position in the world on the adoption of quantum computing;

(iii) develop strategies to mitigate current and emerging risks to the marketplace and supply chain of quantum computing; and

(iv) develop legislation that may advance the expeditious adoption of quantum computing.

Appendix J. Quantum Consortia

Tables 9 and 10 list quantum consortia in the United States and in other countries, respectively. These tables were generated by QED-C based on its institutional knowledge of the quantum ecosystem, including its partner organizations and similar consortia. Additional organizations were identified through internet searches for quantum-related consortia, alliances, public-private partnerships, interest groups, and communities. Although a public partner is not acknowledged by every organization, these consortia are generally considered to have at least implicit support from governments or State-funded institutions.

Table 9. Quantum Consortia in the United States.

Name	Region	Mission	Founded	Computing	Sensing	Comms
CUbit Quantum Initiative	United States (Colorado)	Reinforce Colorado's prominence in quantum information science and technology, partner with regional universities and laboratories, link closely with quantum-intensive companies, and serve a spectrum of local, regional and national interests, including workforce development.	2019	✓	✓	✓
Institute of Electrical and Electronics Engineers (IEEE) Quantum	United States	Tackle challenges related to quantum computing, engineering, algorithms, and related technologies.	2019	✓		
Mid-Atlantic Quantum Alliance	United States	Accelerate moving quantum science and engineering to use and further enhance the region's primacy in a field that promises to revolutionize society.	2020	✓	✓	✓
Northwest Quantum Nexus (NQN)	United States	Accelerate discovery and innovation in the rapidly developing areas of quantum technologies, and to attract and retain talent, funding, and industrial investment in the Pacific Northwest region.	2019	✓	✓	✓

Name	Region	Mission	Founded	Computing	Sensing	Comms
Pistoia Alliance–QED-C Quantum Computing Community of Interest	Led by the United States and the United Kingdom, international participation	Maximize the positive effect of quantum computing on life sciences and healthcare research and development as quantum computing is the next frontier in the field of information technology, and one industry that is set to benefit significantly from the development of these impressive next-generation computers is pharma.	2021	✓		
QuPharm	United States	Provide a unique opportunity for member companies to work together on quantum computing technology for real-world life science problems.	2020	✓		
Duality	United States (Chicago)	The first accelerator program in the United States exclusively dedicated to startup companies focused on quantum science and technology.	2021	✓	✓	✓
Chicago Quantum Exchange	United States (Midwest)	Connect leading academic talent, top scientific facilities, and prominent members and partners to advance the science and engineering of quantum information, train the quantum workforce of tomorrow, and drive the local and national quantum economy.	2017	✓	✓	✓
Quantum Economic Development Consortium (QED-C)	United States (expanding internationally)	Enable and grow a robust commercial quantum-based industry and associated supply chain.	2018	✓	✓	✓

Table 10. Quantum Consortia in Other Countries.

Name	Region	Mission	Founded	Computing	Sensing	Comms[a]
Quantum Algorithms Institute (QAI)	Canada	Help secure British Columbia’s position as a global leader in the application of quantum computing technology to real-world problems.	2020	✓		
Quantum Industry Canada (QIC)	Canada	Ensure that Canadian quantum innovation and talent is translated into Canadian business success and economic prosperity.	2020	✓	✓	✓
Danish Quantum Community (DQC)	Denmark	Build a stronger Danish ecosystem, which can help to leverage the business potential of quantum technology by securing an optimal framework for innovation, research, education, and external investments.	2021	✓	✓	✓
European Quantum Industry Consortium (QuIC)	European Union	Boost the European quantum-technology industry's competitiveness and economic growth and bolster value creation across the continent.	2021	✓	✓	✓
Q-Exa Consortium	European Union	Accelerate European quantum computing technologies with the assistance of traditional high-performance computing.	2021	✓		
Quantum Technology and Application Consortium (QUTAC)	Germany	Quantum computing must find its way into practice and into commercially successful applications. This requires technical expertise, innovative spirit, economic resources and, above all, cooperation to pool findings from members’ distinct development projects, promote their further development, and effectively advance them for practical use.	2021	✓		
Quantum Ecosystems Technology Council of India (QETCI)	India	Accelerate the quantum computing ecosystem in India.	2021	✓		

Name	Region	Mission	Founded	Computing	Sensing	Comms[a]
Quantum Strategic Industry Alliance for Revolution (Q-STAR)	Japan	Provide global leadership in the promotion of activities that advance science and technology in this new era, and by promoting Japanese industry and strengthening international competitiveness.	2021	✓	✓	✓
Quantum Delta NL	Netherlands	Create a fully functional national ecosystem for excellence in quantum innovation for highly talented professionals to bring quantum computers, quantum networks, and quantum sensors to the market.	2020	✓	✓	✓
UKQuantum	United Kingdom (UK)	Unite the UK quantum industry with one voice; champion within government and internationally, advising on interventions and policies that will advance the UK quantum industry; promote the adoption and benefits of quantum technologies across the UK economy.	2021	✓	✓	
Federated Quantum System (FQS)	UK, United States, Japan, Canada, Italy, Belgium, and Austria	Develop a satellite-based quantum technology encryption network.	2021	✓		✓

Source: SRI International. [a]Communications.

Appendix K. Quantum Computing Marketplace and Supply Chain Survey Results

In March 2022, QED-C commissioned Hyperion Research to conduct a web-based survey of quantum computing system integrators, software developers, and component suppliers. QED-C staff selected 85 commercial entities to survey from among its members and other QC stakeholders based on their ability to answer questions related to the QC supply chain. The survey consisted of 27 questions and resulted in 47 responses. Given this relatively small number of responses, the representativeness of the sample with respect to the industry overall cannot be guaranteed.

Respondent characteristics

Respondents were fairly evenly split between firms that market directly to end-users and those that are suppliers to the QC sector (45 and 38%, respectively). The majority of respondents whose firms market directly to end-users have QC sales accounting for 90 to 100 % of their annual revenue (Table 11).

Table 11. Respondent participation in quantum computing.

n=47	Count	%
A QC firm that markets directly to end-users	21	45%
A QC-related supplier to the QC sector (includes materials, components, or sub-assemblies)	18	38%
Both of the above	5	11%
None of the above	3	6%

Figure 1 highlights respondent views of the likelihood and cause of supply chain disruptions. Of those who believed a QC supply chain disruption was likely to occur during the next 3 years, the three most cited causes were disruptions to access to manufacturing equipment, raw materials, and technical expertise to design or manufacture goods.

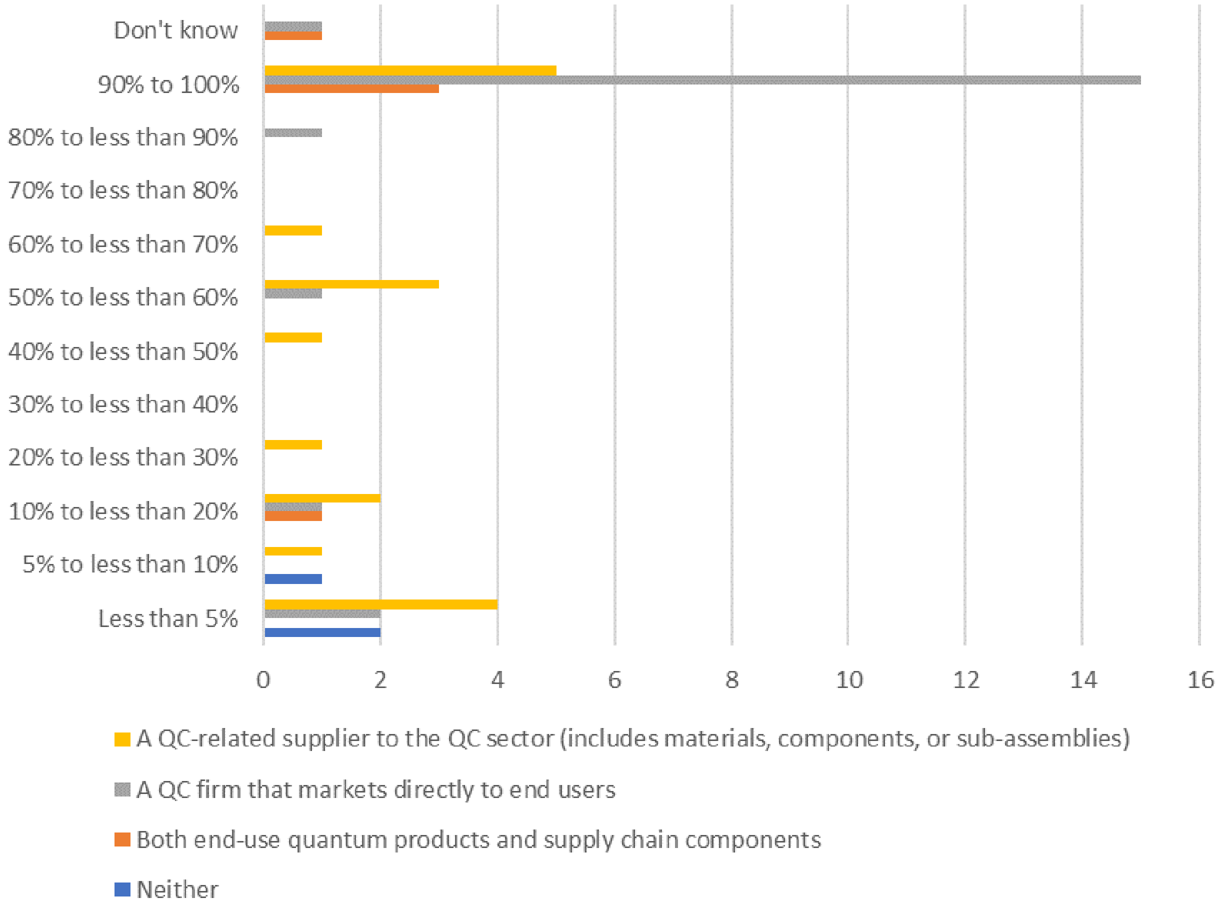


Figure 1. Respondent annual revenue from quantum computing.

Note: The sample size is 47 respondents.

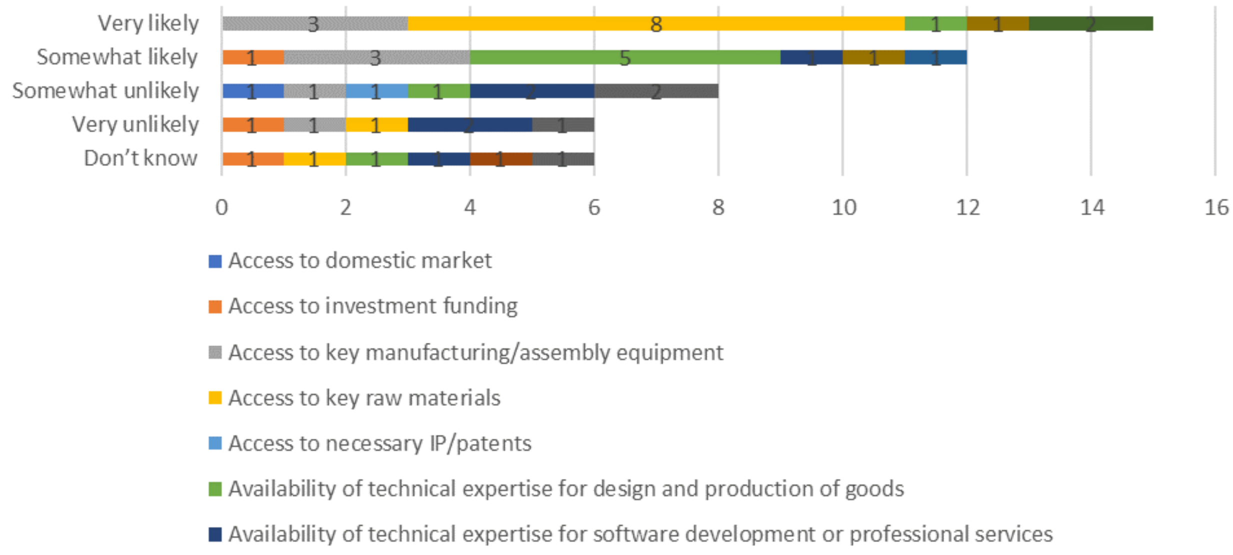


Figure 2. Views of supply chain disruption likelihood.

Note: The sample size is 47 respondents.

Materials and hardware supply risk

Respondents were asked to independently address risks related to QC materials and hardware (including materials, components, subassemblies, and finished QC systems) in terms of the severity of risks posed to the QC marketplace and supply chain and to risks related to QC software and services. Table 12 shows that half of all respondents who foresee critical materials- or hardware-related QC supply chain problems over the next 3 years identified reliable access to key hardware subcomponents as the most critical manufacturing choke point. Of such respondents, 42% indicated that a supply chain problem in this area would slow them down for over a year, and 13% believed it would shut them down for more than a year (Table 13). One-quarter of respondents believed it would take longer than a year to find an alternative supplier, and none believed lost supply could be replaced in less than a month (Table 14). The potentially lengthy delays raise the question of how feasible it would be to come up with a technical replacement solution. Most respondents believed it to be somewhat feasible or not very feasible (Table 15).

Table 12. Most critical manufacturing choke points.

n=24	Count	%
Reliable access to key hardware subcomponents	12	50%
Reliable access to key skilled workforce	3	13%
Reliable access to skilled scientific/engineering/technical workforce	3	13%
Reliable access to key raw materials	2	8%
Reliable access to key manufacturing equipment	2	8%
Reliable access to key processed materials	1	4%
Reliable access to a material or goods distribution channel alternative	1	4%
Reliable access to a material or goods distribution channel	0	0%
Reliable access to necessary compute/design/test equipment and related software	0	0%
Reliable access to critical IP and patents	0	0%
Don't know/Not sure	0	0%

Table 13. Consequences of loss of hardware supply chain capability.

n=24	Count	%
Would shut down our operations for more than one year	3	13%
Would shut down our operations for between six to twelve months	3	13%
Would shut down our operations for less than six months	0	0%
Would slow our operations for more than one year	10	42%
Would slow our operations for between six to twelve months	4	17%
Would slow our operations for less than six months	1	4%
Would not significantly affect our operations	1	4%
Don’t know/Not sure	2	8%

Table 14. Timeframe to find alternative hardware supplier.

n=24	Count	%
Less than a month	0	0%
More than one month, less than three months	3	13%
More than three months, less than six months	2	8%
More than six months, less than nine months	3	13%
More than nine months, less than one year	4	17%
More than one year	6	25%
Don't know/Not sure	6	25%

Table 15. Feasibility of technical alternative to lost hardware supply chain capability.

n=24	Count	%
Very feasible	1	4%
Somewhat feasible	11	46%
Not very feasible	8	33%
Not feasible at all	4	17%
Don't know	0	0%

Software and services supply risk

Regarding the severity of risks posed to the software and services components of the QC marketplace and supply chain, only seven respondents identified supply chain concern in this area (Table 16). With so few respondents highlighting supply chain concerns in this area, no meaningful trends are identified regarding their form or consequence beyond Table 16.

Table 16. Likelihood of critical software supply chain issue within 3 years.

n=47	Count	%
Yes	7	15%
No	19	40%
We do not market QC-related software and/or services	15	32%
Don't know	6	13%

Respondent views of the role of policy in securing the QC supply chain

Figure 3 shows respondent views on the favorability of government actions; listed are those potential domestic government actions that at least 50% of respondents thought would be beneficial. Also shown is the share of respondents who believe the same action on the part of foreign governments would be beneficial. Many of these potential actions revolve around funding. The potential domestic government action with the greatest appeal was to increase and strengthen government R&D incentives. Of respondents, 97.8% believed this government action would provide their organization some form of benefit.

In terms of external forces that could affect the QC supply chain, the main area of concern among respondents is the labor force. When asked to identify the external forces with the greatest potential to affect the QC supply chain, the top three chosen were lack of skilled workforce (100%), rising labor costs (64%), and lack of appropriate domestic educational system (48%) (Table 17).

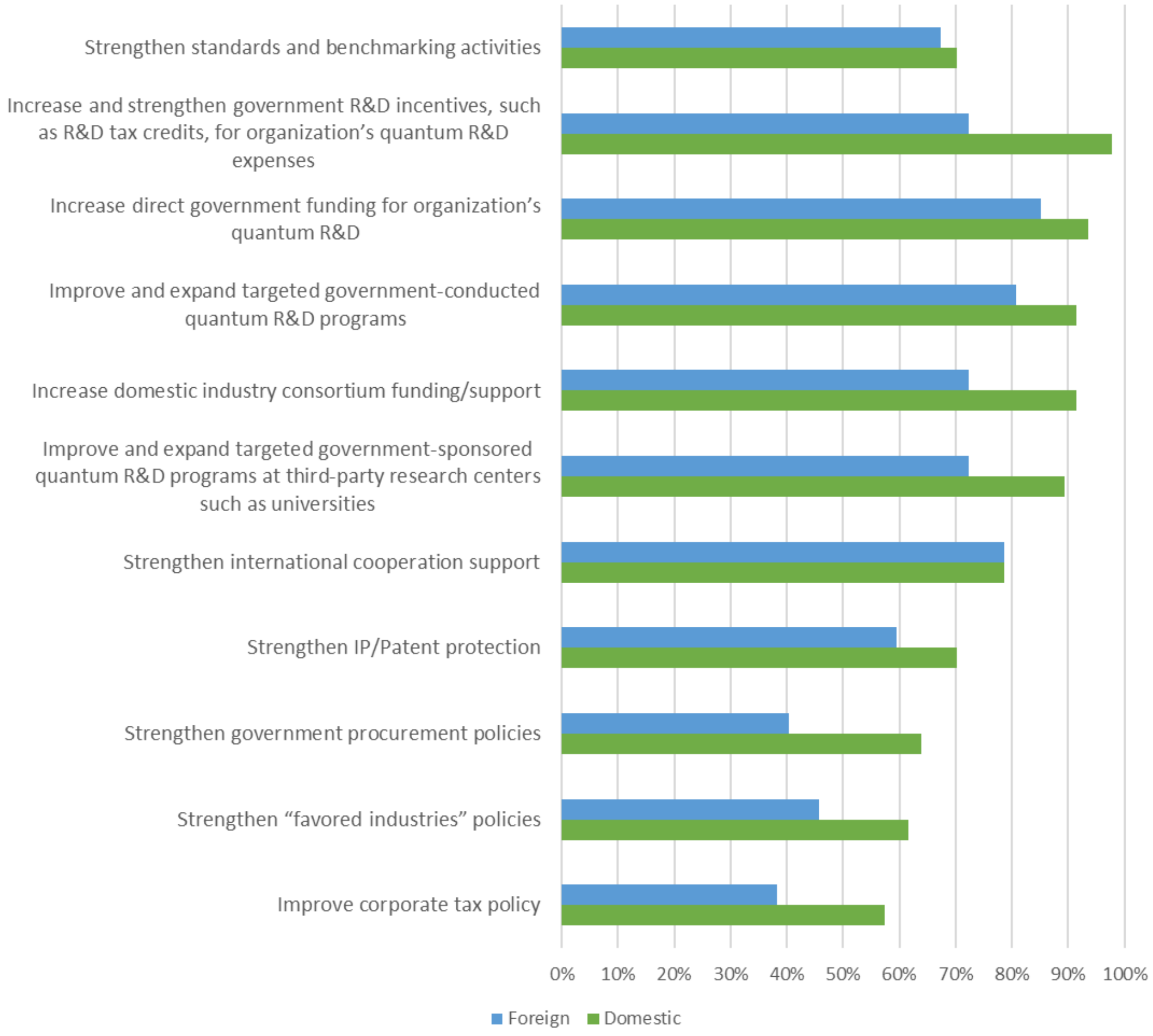


Figure 3. Beneficial government actions

Note: This figure includes all actions for which at least 50% of respondents view a domestic government action as favorable; the sample size is 47 respondents.

Table 17. Greatest potential external impacts on QC supply chain (rounded to the closest 1%).

n=47	First choice	Second choice	Third choice	Total
Lack of skilled workforce	51%	21%	29%	100%
Rising labor costs	13%	23%	29%	64%
Lack of appropriate domestic educational system	13%	26%	10%	48%
Other (Specify)	4%	8%	5%	17%
Poor telecommunications infrastructure (voice, data, internet)	2%	5%	5%	12%
Impacts of natural disasters	2%	0%	10%	12%
Sustainability concerns	2%	0%	10%	12%
Cost of construction/buildings	2%	3%	5%	9%
Climate/weather changes	2%	5%	0%	7%
Rising energy costs	2%	5%	0%	7%
Cost of real estate	0%	5%	0%	5%
Don't know/Not sure	4%	0%	0%	4%
Stricter environmental regulations	2%	0%	0%	2%
Poor physical infrastructure (roads, bridges, etc.)	0%	0%	0%	0%

Hyperion Research presented a complementary analysis of the survey data for QED-C members and other survey participants.[59]

[59] Hyperion Research, *Challenges and Opportunities for Securing a Robust U.S. Quantum Computing Supply Chain* (2022).

Blockchain

Chapter Contents

List of Tables

List of Figures

4. Blockchain

Summary

In the Consolidated Appropriations Act of 2021 (Public Law 116-260), Congress tasked the National Institute of Standards and Technology (NIST) to prepare a series of studies on critical and emerging technologies, including blockchain technology, and their impact on the U.S. economy. NIST is the lead author of this chapter. The Federal Trade Commission has reviewed this chapter in full to identify interactions with consumer protection and competition concerns. In accordance with the language of the Act, this chapter addresses:[60]

- identify key industry sectors that develop, implement, and promote blockchain;
- explore Federal agencies' roles with respect to particular implementations of blockchain technology, including their interaction with the private sector, and other activities;
- assess current regulations, standards, and guidelines in place surrounding these technologies;
- assess how blockchain affects markets and supply chains; and
- provide key policy recommendations for developing and regulating blockchain such that it promotes U.S. national security interests, including economic interests.[61]

In the information age, data storage and access are central concerns surrounding the development and implementation of new technologies. Developing recordkeeping systems that ensure data fidelity, while also preserving privacy and transparency, are crucial. One approach to protecting data in this way is blockchain technology, which is a type of distributed ledger technology (DLT): a means to maintain multiple copies of a ledger, each copy being updated in near real time to reflect changes in other copies. A blockchain can be conceptualized as a database in which information is incorporated in a ledger that marks all events and transactions shared among parties communicating through some network. These transactions are stored in a list of blocks, linked together to form a chain [1]. Blockchain can be beneficially employed in many contexts that require recordkeeping, while also posing risks (see Section 4.2.4).

One use of blockchains has recently drawn a great deal of concern: cryptocurrencies [2]. This chapter focuses on the broad application of blockchain technology, while acknowledging that the applications of blockchain-based technology in specific domains, such as the financial markets, may call for greater sector-specific reflection.

Challenge 1: The diverse application space for blockchain, coupled with the fact that the technology is still relatively new, means that there is a large degree of uncertainty over its

[60] Blockchain technologies, uses, markets, and policies are developing at a rapid rate. While this chapter aims to provide complete information, it is likely that some of its content will be out of date by the time it is completed and submitted.

[61] The Consolidated Appropriations Act of 2021 refers to "economic and national security," and economic security is understood to be part of national security for the purposes of authorities such as the Consolidated Appropriations Act of 2021 and Section 232 of the Trade Expansion Act of 1962 (Public Law 87-794).

future application. Regulations should help blockchain developers and companies ensure that their technology can provide value while mitigating harms and risks.

Recommendation 1: The U.S. Government should support the development of standards and promulgate regulations for blockchain technology that are inclusive of the diverse range of applications that currently exist and that consider potential future applications. It should ensure that these standards and regulations fully account for the varied range of potential risks and harms that blockchain technologies have already introduced and might continue to introduce. Following the lead of the relatively new DevSecOps approach to software development, the U.S. Government should consider security and privacy implications in all its standards and regulations [3]. The ISO documents in **Table 5** would be a good starting point. They provide PII standards and define terms.

The U.S. Government should also promote further study and foster innovation in next generation technologies that are designed to achieve the advantages of blockchain technology while avoiding fundamental weaknesses of blockchain design.

Challenge 2: The network effect of blockchain utility and value incentivizes the creation of proprietary architectures. The business models that underpin the development of blockchain platforms tend to disincentivize interoperability. Interoperability, however, increases the chances that the best blockchain technologies provide the most value for consumers, investors, and businesses.

Recommendation 2: The U.S. Government should encourage and participate with the private sector in developing standards and security best practices for interoperability among the various open-source blockchain consortia. Some industry standards have already been developed in this regard, which can be used as a guide for further standards.

Challenge 3: Blockchain-enabled cryptocurrencies allow individuals to make transactions outside the authority of a central bank. Blockchain technology has accelerated a number of innovations in payments, such as transaction programmability and cheaper cross-border payments. These innovations could help improve traditional payment infrastructure operated by central banks and large financial institutions. However, more work is needed to assess whether these features would provide benefits while mitigating risks to consumers, to financial stability, and other objectives.

Recommendation 3: In support of the Federal Reserve’s ongoing work on a possible U.S. Central Bank Digital Currency (CBDC), the U.S. Government should continue to assess whether a U.S. CBDC issued would advance the Administration's policy objectives for a U.S. CBDC System.

This assessment should include further study for how blockchain-related innovations in payments could help support a potential U.S. CBDC, and also consider approaches other than blockchain technology. Security-related aspects of CBDCs, and the potential AML/CFT requirements needed for CBDCs, should be factored into the assessment. Finally, this assessment should include the security and propriety of the data generated and/or stored on a connected or interconnected DLT.

Challenge 4: The decentralized nature of many blockchain implementations, particularly permissionless or mostly permissionless, means that data can be recorded on a blockchain in many ways, ranging from humans using a keyboard to data received from automated sensors.

Sensors may be crucial for supply chains that rely on blockchains, where the amount of information that must be recorded is too large and time-consuming to enter manually. This variety can decrease opportunities for standardization and increase the difficulty of ensuring the accuracy of data entry. Additionally, this decentralized infrastructure also opens these systems for security gaps – affecting both the blockchain as well as the data transferred and generated by the blockchain.

Recommendation 4: To ensure that blockchain technology is able to continue to grow, investments should be made such that networked devices are available and properly vetted for use in blockchain technology (see Section 4.3.1.2).

Challenge 5: There is no well-accepted model to calculate the costs and benefits of switching to blockchain. An organization whose current infrastructure supports company operations may have difficulty justifying a switch, even if the support is adequate but not optimal.

Recommendation 5: U.S. Government departments and agencies should identify opportunities for blockchain investments and to establish pathways to blockchain technology adoption, where the benefits of blockchain technology become concretely established.

Challenge 6: The open-source nature of blockchain technologies make them susceptible to the same cybersecurity risks in centralized technologies, such as Log4j, Heartbleed, and Solar Winds, as well as additional vectors of intrusion, such as "Bridge" or alt-chain exploitation. Issues of fraud, trust, and illicit use are relevant to blockchain applications, as they are to any cyber system.

Recommendation 6: The U.S. Government should work closely to carry over recommendations from Federal open source software security initiatives, namely ensuring that blockchain programming languages are memory safe.

Challenge 7: The United States currently has a lack of qualified candidates to fill positions working on blockchain technologies given the traditional undergraduate curriculum in the United States. Specifically, there is a lack of potential candidates that have both issue area expertise (e.g., contract law) and the requisite technical skills.

Recommendation 7: The U.S. Government should work collaboratively with universities and other institutions to develop a pool of people with the needed computational skill related to memory safe programming languages, data storage, quantum resistant cryptography, and network communication to create new data management systems (i.e., Blockchain technology).

Challenge 8: There may be undesirable consequences of widespread blockchain implementation. Currently, the best understood of these consequences is the considerable energy consumed by proof-of-work consensus models. Bitcoin miners have advocated shifting to using renewable energy sources, but as of April 2022 it was estimated that only 1% of Bitcoin mining used renewable energy [4; 5].

Recommendation 8: The U.S. Government should promote blockchain technologies that use models other than proof of work to add blocks to a blockchain. The U.S. Government should establish consensus model standards that do not rely on proof of work, and should fund academic sources and industries to develop a supporting open-source infrastructure.

Challenge 9: The possibility of implementing blockchain in mission-critical systems means human lives may depend on their expected behavior. Their widespread use in financial systems poses stability risks in markets.

Recommendation 9: The U.S. Government should establish vetting protocols and certification standards, similar to the FedRAMP authorization process.[62] The U.S. Government should require every system that uses blockchain technology to be certified to the degree appropriate for its intended purpose.

[62] https://www.fedramp.gov/

4.1. Overview

4.1.1. Definition of “Blockchain” and Related Concepts

In the literature, “blockchain” has different meanings. It can refer to a set of technologies that constitute a digital recordkeeping approach. Blockchain can also refer to a specific use case or application. Sometimes even within a single document, blockchain has different meanings depending on the context. Most often, blockchain refers broadly to an approach to digital recordkeeping with distributed ledgers that use lists linked using cryptographic hashes to ensure data fidelity; this definition is adopted in this chapter when blockchain is used as a noun. When used as an adjective, this chapter adopts the following definitions:

Blockchain technology—the combination of several computational techniques involving data storage, cryptography, and network communication to create a new data management system that uses distributed ledgers and lists linked using cryptographic hashes to ensure data fidelity.

Blockchain protocols—the rules that govern how a blockchain is implemented and how devices participating in that implementation interact. There are several categories of protocols. The most important ones, called the consensus mechanisms, specify how data are added to a blockchain [6], thereby allowing the task of recordkeeping to be shared among participants. Protocols also dictate whether the way in which a blockchain is implemented is:

- Public or permissionless: open to all users on a network, with all users participating as equals;
- Private or permissioned: accessible to select users, with a single individual or organization controlling access and permissions; or
- Hybrid: accessibility and participation rights are limited; also known as a consortium blockchain [7].

Together, the different protocols implement a permission spectrum, with private at one end (least permissioned) and public at the other (most permissioned). In between are many variants of hybrid accessibility.

Blockchain implementation—the realization of a distributed ledger implemented using blockchain technology, running on a collection of nodes exchanging information according to an agreed-upon set of blockchain protocols. The terms “blockchain application” and “blockchain solution” are synonymous. Some authors use “blockchain technology” to mean the same thing, but the term has a different meaning here (see above).

Blockchain network—the collection of devices participating in a blockchain implementation.

Blockchain is often conflated with cryptocurrency and, in particular, Bitcoin. This is largely due to the fact that (1) Bitcoin was the first blockchain network implementation used widely, and (2) cryptocurrency has driven the rapid advancement of blockchain technology. But

Bitcoin is a single blockchain implementation and use case. Blockchain technology has numerous implementations and much broader applicability.

4.1.2. Properties of Blockchain Technology

Several characteristics of blockchain technology exist across all forms of implementation and all protocols. These properties are core to the technology as a means of keeping and preserving records.

1. Blockchain is intended to be distributed: duplicate copies of the data are stored across devices (also called "nodes"), which communicate with one another to ensure there is a common understanding of the information contained in the blockchain [1].
2. Blockchain data are intended to be immutable, tamper-resistant, and tamper-evident: once data are written to a blockchain, any change can be detected. Blocks of new data—typically containing what are referred to as transactions—are appended, but previous blocks cannot be edited without compromising the blockchain's integrity in such a way that the edits can be detected [8]. Every node can independently verify the authenticity of all data included in the blockchain.
3. Blockchain is intended to be transparent: the ledger provides a complete history of all blocks in the blockchain [9].
4. Blockchain can hide identity: a blockchain implementation may show that a transaction occurred (transparency), the date and time it occurred, and the amounts involved, but transactions need not include information that can identify a transaction participant to anyone besides themselves [10].[63]

4.2. Background

4.2.1. Key Technologies That Underpin Blockchain Technology

4.2.1.1. Public-Key Cryptography

The transactive nature of blockchain technology necessitates a method for ensuring the authenticity of interactions between users. The principal way to ensure data confidentiality and integrity is through encryption. Encryption is a widely used technique that allows confidential data to be securely and privately transmitted through open communication channels, such as the internet [11].

Public-key cryptography is one such method for ensuring security and privacy, and is a foundational element of blockchain technology [8]. With public-key cryptography, a user creates two keys, one of which is private and the other public. The two keys are paired; a message encrypted with the public key can be decrypted by the private key. As an example,

[63] In practice, keeping identities private on a blockchain has been harder than anticipated. Subsequent sections discuss this topic.

when sending a private message from Person A to Person B, Person A encrypts the message with Person B's public key and transmits the encrypted message using open communication channels. Once received, Person B decrypts the message using their private key.

Similarly, in a blockchain transaction[64], Person A can sign transaction data with their private key and transmit the transaction data along with the signature to a public site, e.g., a node in a blockchain network. The blockchain node can verify the signature using Person A's public key, thereby verifying that the transaction originated from Person A [12].

Both of these examples highlight the importance of protecting a private key. If a user's private key is stolen, their "digital identity" is compromised. In the first example, whoever possesses Person B's private key can decrypt their private messages. In the second example, whoever possesses Person A's private key can create a valid transaction without Person A's knowledge—such as removing all of Person A's cryptocurrency from their digital wallet.

4.2.1.2. Cryptographic Hash Algorithms

Each block of data that is added to the blockchain is made tamper-resistant (i.e., locked) through the use of a hash digest generated by a cryptographic hash algorithm. A hash digest is a transformation of an arbitrary sized piece of data into an output piece of data of predetermined length, irrespective of the amount of data in the input. Similar to the use of keys in public-key cryptography, a blockchain application computes the hash digest using cryptographic algorithms. Cryptographic hash algorithms work such that changing even a single bit of information in the newly added data block will compute a hash digest that, to an observer, appears entirely dissimilar. Importantly, given only a hash digest, it is computationally infeasible to find an input data that a cryptographic hash algorithm would map to that has digest. Two blockchain blocks are never identical (at the very least, they will have different timestamps) so hash digests will differ with extremely high likelihood. The cryptographic hash digest serves as a tamper-proof seal on the block of data.[65]

This hash digest is then included in the following block on the chain, which creates the linking between blocks of data. Because the hash digest is included in the ledger, each hash digest locks all data for all preceding blocks in the chain. Hash digests make blockchains tamper-resistant [8].

A hash digest is easy to verify. When provided with a blockchain ledger, an application can quickly and easily verify that the hash digest for the previous block matches the data included in the block. However, because of the length of a blockchain, it is not necessarily trivial to verify the integrity of an entire blockchain. As of this writing, the Bitcoin blockchain contains over 743,000 blocks. The time needed to verify every block is difficult to estimate. It depends on hardware, block size, and block content. It is typically not an operation that can be performed in real time.

[64] Not to be conflated with financial transactions, which are but one specific use of blockchain technologies for cryptocurrencies.

[65] It is more accurate to say that, given two hash digests computed from different inputs, the probability they will be identical is miniscule. Likewise, if the two inputs differ by even a single bit, the probability an observer will consider them similar is also miniscule. The probability is so miniscule that it is often spoken of as if it is nil, including in this chapter.

4.2.1.3. Distributed Systems

One of the principal characteristics of public (i.e., more permissioned) blockchain technology is its decentralized, distributed nature of governance. By maintaining numerous copies of a ledger on computers across the world, the ledger has a different, and sometimes smaller, attack surface. With traditional data storage techniques, a central authority is used as a reference for data integrity. All users engaging in transactions under this system must ensure that their data are aligned with those found in the central server. Under this system, the data are vulnerable to a central point of failure; should the central authority be compromised by a malicious actor, the data could be compromised with no way of ensuring verification.

In contrast, blockchain technology *can* be implemented in a manner that does not rely on a central authority and, instead, provides all nodes in the network with some level of access to the ledger. These nodes communicate with other nodes to verify the true state of the ledger. Differences between nodes arise when different nodes contain different blocks in the chain. In most public blockchain protocols, when the blockchains differ between nodes, the node with the "longest" blockchain (i.e., the blockchain containing more blocks or that required more work to create) is considered the true state [6; 9]. Blockchains are generally distributed across a wide variety of hardware and software systems and, as a result, reduce malicious actors' ability to attack and compromise the entire blockchain environment. When adopting more-permissioned protocols, blockchain technology can be both distributed and used by one or more trusted central authorities with special roles and responsibilities for maintaining the ledger [13].

4.2.1.4. Consensus Mechanisms

Consensus mechanisms maintain consistency across a blockchain. With multiple users appending information to the blockchain, it is necessary for blockchain technology to have some method for ensuring agreement on the most recent block in the blockchain, which implies agreement on all previous blocks. Consensus mechanisms work to ensure that every new block added to the blockchain is a singular block upon which all nodes can agree [8].

Consensus mechanisms also work to ensure that a particular node receives a reward to help validate a small number of additions to the blockchain. Under the proof-of-work consensus mechanism—the model underlying Bitcoin—nodes compete by expending computing resources to be the first to solve a computationally complex, intensive puzzle. The winner gains the opportunity to append the next block of data to the blockchain [10]. With the proof-of-stake model, nodes are able to publish new blocks based on the amount of "stake" they have in the blockchain implementation, generally measured by the amount of coins native to the blockchain a node possesses, sometimes involving how long the node has possessed the coins; this does not require the time-consuming computations required for proof of work [14]. Precisely quantifying the differences in energy consumption between proof of work and proof of stake is difficult, but some research estimates that proof of work requires three orders of magnitude more energy than proof of stake [15]. In September 2022, Ethereum—an open-source blockchain with support for smart contracts that also has its own cryptocurrency—driven by concerns over the high energy consumption required to achieve proof of work consensus [16], became the first major blockchain provider to transition from the proof-of-work model to the proof-of-stake model [17]. Some blockchain providers have never used proof of work. Solana, for example, combines proof of stake with another consensus mechanism: proof of history.[66]

4.2.2. Services Provided by Blockchain Technology

Blockchain technology provides services. These types of services are not new, but blockchain technology integrates them and can offer levels of integrity not previously achieved. The following lists some of the important services.

- ***Ledger updating:*** A blockchain is a way to maintain a distributed ledger that is updated in near real time. Distributed databases also offer this service, but blockchain lets nodes verify every block's integrity.
- ***Transaction recording:*** Ledger entries are cryptographically-signed transactions making them almost impossible to refute. A blockchain records those transactions.
- ***Smart contracts:*** Some blockchains allow "smart" contracts—expressed as code—to automatically execute and record transactions. Smart contracts attempt to ensure all aspects of a transaction are carried out in accordance with prespecified terms.

In all these cases, the ability to verify integrity is a feature of blockchains. Administrators of a distributed database management system can keep logs, but those logs can be corrupted. They might compute hash digests of data sets and logs, but that would be an extra step, not one fundamental to operating a blockchain implementation.

4.2.3. Application Areas of Blockchain Technology

Blockchain technology assists in data management in a variety of application areas. Several of these implementations are discussed briefly in this section. It is important to note that blockchain implementation is not fully mature and sparse outside of a few markets; the following examples vary widely in their degree of development and deployment.

4.2.3.1. Cryptocurrency

Cryptocurrency is a digital asset, which may be a medium of exchange, for which generation or ownership records are supported through a distributed ledger technology (DLT). Cryptocurrency usually relies on blockchain technology to ensure the security of the transactions and stores these transactions as a blockchain. The distributed nature of the technology allows cryptocurrencies to function without trusted entities (e.g., a central bank) that verify transactions. Cryptographic techniques, such as public-key cryptography, protect an individual's assets, while the blockchain protocols ensure that transactions are recorded on a single, verifiable version of a blockchain implementation. However, though the term is in general use by the public, a "cryptocurrency" does not have all the attributes of "real" currency, as defined in 31 C.F.R. § 1010.100(m), including legal tender status in the U.S. [18].

[66] https://solana.com/learn/blockchain-basics.

4.2.3.2. U.S. Central Bank Digital Currency

The United States is exploring the potential benefits and risks of creating a central bank digital currency (CBDC), which would become a digital form of currency that is a direct liability of the Federal Reserve Bank of the United States. Some of the design choices popularized by blockchain technology, such as ledger history and transaction programmability, are being discussed as potential options to help a U.S. CBDC system meet the Biden-Harris Administration's Policy Objectives for a U.S. CBDC System [19; 20]. Other countries have developed, are developing, or are considering CBDCs, which would be legal tender [21].

4.2.3.3. Decentralized Finance

Decentralized finance (DeFi) is a term too new to have a generally accepted meaning, but it is usually taken to refer to "digital asset protocols and platforms that allow for some form of automated peer-to-peer transactions." [22]. DeFi uses digital ledgers such as blockchain to provide financial products, services, arrangements, and activities without the need for traditional financial intermediaries such as banks. This can include investment opportunities and providing collateral loans. DeFi also presents opportunities for investing outside of traditional methods and the concurrent risks, such as investments in non-fungible tokens (NFTs) [23]. DeFi could potentially provide trading services with lower fees, improve the timeliness of finalizing transactions, and be accessible to a broader population. However, certain issues relating to transparency, pseudonymity, cybersecurity, and lack of compliance with regulation create risks within the DeFi sector that are less consequential or not present in traditional investment systems [24]. Smart contracts, which are often viewed as integral to DeFi, are also a potential way to ensure that transactions conform to applicable financial rules and regulations [25].

4.2.3.4. Transaction Data Management as Asset Management

With the increased digitization of asset management, blockchain is one potential avenue for managing and storing data. For example, blockchain is being explored by some State and local governments for recording land and real estate transactions.[67] Contractual elements related to the transactions, such as financial or legal documents, can be stored on a blockchain [26]. In fact, some companies have already placed instances of conventional financial instruments on a blockchain. For example, KKR & Co., a global investment company, has tokenized part of a healthcare fund offering.[68] Tokenization is the process by which existing rights, assets, debt, equity, or other assets and liabilities are brought to the blockchain.

4.2.3.5. Supply Chains

Blockchain may be able to assist in supply chain management by providing a potentially tamper-resistant, tamper-evident, and transparent record of all activities and parties related to

[67] https://www.mintz.com/insights-center/viewpoints/2176/2018-05-04-blockchains-and-land-title-records

[68] https://techcrunch.com/2022/09/13/kkr-dives-into-avalanche-blockchain-to-tokenize-and-democratize-financial-services/

a product through its lifecycle. Blockchain may also be able to support the digitization of supply chain processes that can in turn improve the efficiency of and visibility into the movement of goods through the supply chain. One example of blockchain use in supply chains is Walmart, which in 2018 began to implement blockchain to track vegetables and promote trust in greens that have been subject to food-borne illness outbreaks [13]. Similarly, these types of records can provide traceability when tracking compliance with reporting requirements, important for organizations such as U.S. Customs and Border Protection (CBP) [27]. As a result, blockchain can also potentially cut down on the time required for shipments to be processed through customs. Records entered at the time material is packed for shipping could be propagated through a distributed ledger, and available to customs for verification.

It must be noted, however, that there appear to be challenges with the example in the previous paragraph. A November 2022 article reports that IBM and Maersk are shutting down TradeLens,[69] the blockchain-based global supply chain tracking system that Walmart was using, forcing Walmart to halt its involvement [28; 29]. Walmart found that the potential advantages of blockchain were unrealized; for a blockchain-based supply chain to be advantageous, all participants must use the blockchain implementation. This was easy enough for companies the size of Walmart and Maersk, but smaller companies were unwilling to invest in the technology and infrastructure.

4.2.3.6. Auditing of Regulated Industries

Similar to its potential in assisting U.S. CBP, blockchain may be able to assist in auditing regulated industries, e.g., regulations of food quality or drug quality [30; 31]. Because information stored on a blockchain is nearly immutable, individual entities cannot easily tamper with records. This provides auditors with greater assurance of data fidelity when assessing regulatory compliance.

4.2.3.7. Provenance and Traceability of Natural Resources

Similar to the auditing of regulated industries, companies may employ a more permissioned blockchain to trace supply chains within a company, or a slightly more-permissioned blockchain to manage transactions with outside vendors and suppliers [27]. One such company engaged in this work is Everledger, which aims to increase the transparency of global supply chains through blockchain [32]. Another effort, led by IBM, is exploring blockchain technology to ensure that mined cobalt is sourced from organizations that do not violate human rights and environmental protections. The U.S. Government, recognizing the potential of this and other uses, has prepared a report that discusses the pros and cons of blockchain technology related to energy generation, distribution, and consumption [33].

4.2.3.8. Personal Data and Identity Management

Blockchain can also be used as a tool for personal data management and user privacy. One report outlined a system in which links to personal data are stored on a blockchain and both services and users can request access to these data [34]. The personal data are stored in a

[69] https://www.tradelens.com/

distributed hash table. Blocks in the blockchain contain keys to values in that table. Users can revoke access for a service at any point in time. Consistent with the White House's data privacy objectives,[70] this system may enable built-in protections from abusive data practices, as well as increased agency for individuals and communities about how their data is used.

4.2.4. Key Risks, Challenges, and Uncertainty Related to Blockchain Technology

Much uncertainty remains about the future design, development, implementation, and use of blockchain technology, principally because it is in such an early stage of development. As is discussed throughout this chapter, the technology is subject to limited regulation at both the industry and government levels. As popular implementations of blockchain become more widespread, the risks associated with this uncertainty will only magnify.

A blockchain implementation, especially one using permissionless protocols, can be susceptible to a "51% attack". As discussed in Section 4.2.1.3, if blockchains differ between nodes, the one that represents the most work is considered to be the true blockchain. However, this assumes that every node is operating independently. If more than 50% of nodes conspire, they can control what blocks are added to the ledger and create the longest chain, thereby nullifying transactions in existing blocks. The original Bitcoin paper discussed this kind of attack and presented an analysis that concluded that its probability was low [10]. Successful 51% attacks have been staged, however, particularly against smaller blockchain implementations.[71]

Sections 4.2.3.5 and 4.2.3.7 discuss the potential value blockchain technology adds to tracking and tracing material goods. Descriptions of such blockchain applications tend not to consider the possibility that bad actors could enter, or that Internet-of-Things devices involved in blockchain transactions (scanners, sensors, etc.) could be programmed to enter, fraudulent data. Blockchain technology helps verify that a ledger has not been altered. It does not guarantee that entities referenced by a ledger are of the expected quality.

Predicting the computing infrastructure and capacity needed to expand the use of blockchain technology is difficult. As is shown throughout this chapter, there are many predictions on the growth of blockchain and the potential for its use. All make assumptions with degrees of uncertainty. Nevertheless, analysts have noted that the current infrastructure is inadequate to support widespread blockchain. The White House Office of Science and Technology Policy (OSTP) issued a report on blockchain's implications for the U.S. Government [20].

In March 2022, President Biden signed Executive Order 14067, *Ensuring Responsible Development of Digital Assets*, outlining a whole-of-government strategy for protecting consumers, financial stability, national security, and the climate [35]. Federal agencies wrote a number of reports that analyzed the risks that digital assets, including those using blockchain technology, posed to U.S. national and economic security. Building on those analyses, in this chapter we discuss the implications of these blockchain-related risks for U.S.

[70] https://www.whitehouse.gov/ostp/ai-bill-of-rights/data-privacy-2/

[71] See https://medium.com/hackernoon/the-history-of-51-attacks-and-the-implications-for-bitcoin-ec1aa0f20b94. Also see https://www.crypto51.app/ for estimates of the cost to perform a 51% attack on various cryptocurrencies.

national security, including economic security, along with the central challenges for ensuring that the technology's development is aligned with U.S. values.

4.3. Observations

Section 4.2.4 discusses the risks and challenges of blockchain technology. This section provides additional examples of how blockchain technology has been used, is being used, and may be used. It bears emphasizing that much is still unknown or uncertain. The spectrum from permissionless to permissioned is wide, and the suitability of a given application area to a given set of permissions deserves study before applying blockchain technology to that area. The result of this study can address areas such as application speed (a decentralized, permissionless blockchain implementation can be slower than a centralized, permissioned blockchain implementation) and potential for illicit use (cryptocurrencies have often been used for money laundering). This section presents uses of blockchain technology (along with some failures), but it does not attempt to assess whether the technology has been used most effectively, or even what is meant by using blockchain technology most effectively.

4.3.1. Industry Sectors That Develop, Implement, and Promote the Use of Blockchain

Blockchain technology arose from the financial sector, specifically Bitcoin, which provided the initial impetus for the widespread implementation and adoption of blockchains [36]. Through the desire to use Bitcoin for financial transactions, DLT was implemented, disseminated, and executed in the early 2010s [37]. This led to the recognition of the potential benefits of blockchain technology in areas other than cryptocurrencies.

As the potential for broader applications of blockchain technology became apparent, organizations invested in maturing the technology and growing their customer base. Major organizations now promote and provide blockchain technology to customers who seek to use DLT. Some of these organizations are shown in **Table 1**. The table is not intended to be complete, but to give an idea of the range of products and services offered. The first two organizations, Ethereum and the Linux Foundation, have developed blockchain technology, which the other organizations are using. These other organizations provide applications, middleware, infrastructure, and services to customers. The customer, having decided to use distributed ledgers, can turn to one of these companies for a turnkey solution or application programming interface (API)-based blockchain access.[72]

[72] An API is a specification by an application of how other applications can communicate with it. It is the basis for fully automated exchanges of information between systems, and of one system's use of another's services.

Table 1. Major Industry Organizations that Promote Blockchain Technology

Organization	Blockchain Technology	Notes
Ethereum	Ethereum (developer)	Ethereum is an organization that has developed an open-source, permissionless blockchain infrastructure, with support for smart contracts.[73] Unlike the other organizations, Ethereum was founded and exists as an organization to promote the Ethereum blockchain technology. Ethereum's popularity arises from its support of smart contracts, which are important for ensuring that transactions are executed according to a prespecified set of terms.
The Linux Foundation	Hyperledger Fabric[74] (developer)	One of the Linux Foundation's popular open-source projects is Hyperledger Fabric [38]. Hyperledger Fabric is an open-source, modular, permissioned blockchain infrastructure. Hyperledger Fabric's developers recognized the need for scalability and reliability in enterprise applications.
IBM	Hyperledger Fabric	IBM offers a blockchain development platform and sells blockchain-based services. IBM has built a blockchain platform on top of Hyperledger Fabric [39]. IBM offers a platform for blockchain developers and users, and personalized services. These services include identity management services, supply chain management, support services, and training services.
Amazon Web Services (AWS)	Ethereum and Hyperledger Fabric	AWS provides blockchain solutions based on both the Ethereum and Hyperledger blockchain infrastructures. Its solutions include private, hybrid, and public blockchains, offering customers flexibility in data privacy needs [40].
Oracle	Hyperledger Fabric	Oracle offers both on-premise and cloud-based blockchain solutions, depending on customer requirements

[73] See https://ethereum.org/

[74] Hyperledger Fabric is only one of several Hyperledger variants: see https://www.hyperledger.org/use/distributed-ledgers

Organization	Blockchain Technology	Notes
		and data storage needs. The blockchain technology is based on Hyperledger Fabric. Oracle also offers the Oracle Blockchain Platform on its cloud blockchain; the platform provides API-based access to cloud servers [41].
Intel	Hyperledger Fabric	Intel is building a development platform and also developing specialized hardware for mining and proof of work. As a chip manufacturer, Intel is developing energy-efficient chipsets intended to reduce the environmental costs of mining cryptocurrencies and promoting its Blockscale Application-Specific Integrated Circuit (ASIC) hardware accelerator for proof-of-work consensus applications [42]. Intel is also building a platform around Hyperledger Fabric, making use of select Intel technologies (Xenon scalable processors, solid state drives) to provide a scalable blockchain architecture tailorable to enterprise needs [43].
Microsoft	Quorum	Microsoft has shifted from developing blockchain-based solutions to providing infrastructure for executing them. Microsoft offers blockchain as a service (BaaS), the third-party creation and maintenance of the infrastructure a company needs to use a blockchain implementation. The service was originally built on top of its Azure cloud services and provided a workbench that developers could use to build and field blockchain applications. On May 10, 2021, Microsoft announced it would retire the Azure BaaS on September 10, 2021. It requested customers transition to ConsenSvs's Azure-based Quorum Blockchain Solution [44]. Quorum is based on Ethereum but uses different consensus mechanisms.
SAP	Hyperledger Fabric	SAP offers BaaS. Its services integrate with SAP’s enterprise software. SAP

Organization	Blockchain Technology	Notes
		offers BaaS in the cloud [45]. SAP has developed a Hyperledger Fabric-based blockchain, called SAP Blockchain, with tools that allow SAP Blockchain to be used for standalone application development, but also to integrate with the rest of SAP's enterprise application software infrastructure.[75]

With regard to Intel’s energy-efficient chipsets, it’s worth recalling Parkinson’s Law: work expands to fill the time available for its completion. An OSTP report [16] states that increases in energy efficiency have been counterbalanced by increases in the number of computations performed.

Most of the organizations in **Table 1** are large corporations seeking market dominance. They have no incentive to cooperate, which has led to some innovations but also to different architectures. Applications do not interoperate well across the architectures. An application that needs to transfer information from one distributed ledger to another would have to create a customized solution; there is no standardized approach.

Table 2 shows the industry sectors analyzed in this chapter and market sectors adapted from [46]. The first column names a sector. The second briefly describes it. The third lists some (but by no means all) of the applications for which blockchain technology is being used in the sector.

[75] The infrastructure includes SAP’s Leonardo, a service for integrating blockchains and capabilities.

Table 2. Industry Sectors Analyzed

Sector	Domain	Potential Applications of Blockchain
Agriculture and Food	Farming of crops, raising of livestock, and production of foods	Fraud reduction, regulatory compliance, contaminant tracing[76]
Banking and Financial Services	Holding and transfer of financial instruments between entities (organizations and individuals)	Transaction simplification, particularly international transactions
Education	Maintenance and transfer of student data and records of knowledge	Sharing student records between educational institutions, and with prospective employers
Energy and Utilities	Generation and distribution of energy	Reducing carbon emissions, supporting supply chain integrity and management, further enabling distributed energy resources, controlling integrity, reducing energy costs
Healthcare and Life Sciences	Diagnosis of patients, exchange of patient data, and acquisition, distribution, and use of medical tools and remedies	Clinical data exchange, claims payment, fraud reduction
IT and Telecom	Providing telecommunications infrastructure	Fraud reduction, international communications payment adjudication
Insurance	Providing risk management services	Fraud reduction, claims payment, regulatory compliance
Manufacturing	Generation of a product from raw materials or components	Material and component visibility, fault prediction
Media, Advertising, and Entertainment	Generation and distribution of content, both physical and digital	Asset storage, loyalty programs, advertising metrics
Mining	Extracting raw materials from the Earth	Visibility into products and practices, regulatory compliance
Real Estate and Construction	Transfer of property titles and construction of buildings upon properties	Deed visibility, transaction simplification, materials visibility

[76] USDA often refers to these three objectives as transparency, traceability, and trust.

Retail and E-commerce	Selling and distributing goods to consumers	Fraud reduction, regulatory compliance, shipment efficiency
Transportation and Logistics	Movement of (physical) materials, raw or processed; also concerned with warehousing and inventory management	Product visibility, efficiency, regulatory compliance
Travel and Hospitality	Transportation of persons and their possessions for business or personal reasons	Luggage tracking, loyalty programs, booking services

The technological areas listed in the summary for this chapter provide a framing device for the discussion because their adoption could potentially drive changes in business and operational practices. Some of the technological areas pervade all sectors and could affect practices similarly. Our analysis indicates that, irrespective of sector:

- ***Payment times for goods and services could decrease, and payment could become more efficient.*** The traditional payment model, involving an intermediary and an intermediary-approved method such as a check or credit card, could be disrupted by blockchain technology through potentially quicker settlement times, reduced fees and permanent, easily accessible, and verifiable records. This could occur for both domestic and cross-border payments. This would also come with challenges, such as potentially making remediation more difficult, new forms of fraud, and the speed with which money can be stolen. Additionally, newly developed services such as FedNow may change the relative benefits of blockchain systems in the financial space.
- ***Supply chain regulators could operate more effectively.*** Currently, regulation involves identifying the supply chain used to manufacture and distribute a product, gathering information from each organization involved in the supply chain, and using that information to determine whether the organization is complying with applicable regulations. By contrast, if each transaction in a supply chain is recorded using blockchain technology, the entire supply chain may be able to be discovered through analysis of a single blockchain implementation, although supply chain manipulations today are still possible on a blockchain, such as intentional mislabeling. This is just one example of the implications for regulatory oversight.
- ***Customers and other stakeholders could gain visibility into the supply chain.*** This effect is not dissimilar to the benefits for regulators. "Customers" in this case means any buyer at any point along the supply chain: manufacturers' buyers as well as end users (consumers). Manufacturers' buyers are typically concerned with price, materials quality, delivery schedule, and conformance to regulations. Consumers who wish to factor social considerations, e.g., personal health and ethics, into their purchases may be able to discover sources of raw materials. At present, a consumer's ability to discover this kind of information is largely based on trusting a brand or certifying organization.[77] Blockchain technology allows consumers to verify a brand's choices in sourcing raw materials. In a more-permissioned distributed ledger, the records at each step of a supply chain are open and accessible.
- ***Fraud, theft, smuggling, and other criminal behaviors could be easier to detect and trace.*** Scenarios for using blockchain technology in supply chains include

[77] An example of a certifying organization is Fairtrade International (https://www.fairtrade.net), which gives consumers assurance that farmers and workers are paid fair prices and wages. But here too, the consumer trusts that Fairtrade International conducts thorough and accurate research.

recording as transactions the insertion of goods into a container, the sealing of that container, the transport of that container, the unsealing of that container, and the unloading of the container. This additional data on the time-history of assets and recorded using DLT provides additional safeguards against fraud.

- ***Industries could need to invest in Internet of Things (IoT) technology.*** Making blockchain technology effective requires recording transactions. Digital devices, such as scanners and sensors, may simplify tracking and monitoring the creation and delivery of goods and services, thereby making blockchain technology more effective compared to manual record entry. The recent failure, discussed above, of the TradeLens system was blamed in part on the difficulty of participating in a blockchain implementation without having adequate infrastructure.[78]

Agriculture and Food: Agricultural products are delivered to consumers through a complex supply chain. Recording each step of a supply chain on a blockchain implementation provides the power to trace any food item to its source—for example, the farms that grew the plants, the ranches that raised the cattle, the seas that were fished, and the conditions of food items during transport (e.g., temperature).

In 2018, IBM started the IBM Food Trust, a blockchain-based network that empowers organizations and individuals to view the history of any food item and any ingredient of a processed food item, starting from where an item or ingredient originated (farm, ocean, etc.), the course of its journey, and (as appropriate) preparation into an edible product [47; 48]. The information includes not only locations, but also applicable certificates on fair trade practices, organic farming practices, pesticides used, etc. [13]. The original members included such major companies as Walmart, Dole, Kroger, Tyson Foods, Nestlé, and Unilever. The members as of 2020 include producers, intermediaries, and vendors [49]. However, the reports from 2020 indicated the members still regarded using blockchain technology as an experiment, not something integral to their models of operations. The Food Trust was based on IBM's TradeLens system which, as discussed above, was canceled in 2022.

Smaller organizations in specialized agricultural areas have sought their own niche applications of blockchain technology. Cargill has been piloting a blockchain that allows consumers to trace a turkey's origin [50], though we found no updates on this project since 2018.

In the context of agriculture and food, blockchain technology has the potential to offer several important opportunities to reduce fraud, detect sources of foodborne illness, establish provenance, and automate regulatory compliance. The Food Trust blockchain system expedites the process of linking foodborne illness outbreaks to an agricultural source [13]. If made accessible to consumers and regulators, this same blockchain system would support food provenance and regulatory compliance.

This sector illustrates a limitation of blockchain technology. Expecting ranchers to tag every head of cattle they ship to market so it can be entered into a distributed ledger seems

[78] Edwin Lopez, "Maersk, IBM to shut down blockchain joint venture TradeLens", https://www.supplychaindive.com/news/Maersk-IBM-shut-down-TradeLens/637580/, Nov 30, 2022.

practical. Expecting farmers to do the same for every raspberry is impractical; what, then, is the minimum viable unit? One farmer's grain shipment, mixed into a silo with other farmers', cannot be isolated without changing the entire agricultural supply chain; what benefits would a blockchain then provide? The use of blockchain in this sector raises issues such as its usability by consumers, challenges of ensuring the integrity of the mapping between blockchain entries and physical items, and the cost overhead of running these systems. These kinds of issues will have to be studied as blockchain technology and implementations move forward.

Banking and Financial Services: Finance was the original application of blockchain technology. Cryptocurrencies arose from a desire to create a store of value and complete financial transactions without the need for an intermediary, such as a bank. One estimate claims that $1.14 trillion worth of cryptocurrency trades occurred in 2021 [51]. Another placed the value of the trades at over $14 trillion.[79] Yet another says cryptocurrencies account for about 7 percent of the world's "money" [52]. Cryptocurrencies have become a large asset class.

There is debate over whether cryptocurrency is truly a form of money. One definition of money is that it must serve as a store of value.[80]Some argue that cryptocurrency's wildly fluctuating price makes it an unreliable store of value; witness Bitcoin dropping almost 65% in 2022,[81] and the view of many experts that cryptocurrency investments are speculative [53].[82] Nakamoto's original Bitcoin paper makes clear that cryptocurrency was intended to be a form of money. This paper does not take sides on whether cryptocurrency is *money*.

Many organizations implement blockchain wallets, which give users a way to store their cryptocurrency holdings, and exchange holdings for other forms of currency—other cryptocurrencies (e.g., Bitcoin to Ethereum) or fiat currencies. Two well-known examples are Blockchain.com and Coinbase, although there are many others [54–56].

Many activities involving digital assets are within the scope of existing domestic laws and regulations, an area where the United States has been a global leader. The United States has nonetheless acknowledged that the growing development and adoption of digital assets and related innovations, as well as the risks they present, necessitate an evolution and alignment of the U.S. Government's approach to digital assets. Through Executive Order 14067, *Ensuring Responsible Development of Digital Assets,* the Biden-Harris Administration tasked agencies to deliver reports on digital assets to the President in 2022 and into 2023 [35]. **Table 3** lists the reports, the party responsible for preparing them, their planned delivery dates, and the section of Executive Order 14067 that requires each report [35]. As of February 2023, all planned dates have been met, although items 3 and 8 have not been formally published, item 8 was not expected to be a deliverable report.

[79] https://www.theblock.co/linked/128526/centralized-crypto-exchanges-14-trillion-trading-volume-2021

[80] https://home.treasury.gov/system/files/136/Future-of-Money-and-Payments.pdf

[81] https://www.forbes.com/advisor/investing/cryptocurrency/crypto-market-outlook-forecast/

[82] For example, https://www.santander.com/en/press-room/insights/bitcoin-store-of-value-or-speculative-investment, https://www.schwab.com/learn/story/cryptocurrencies-should-you-invest-them

Table 3. Reports Required by Executive Order 14067

	Report	Responsible Party	Delivery Date	Section
1	Report on how to strengthen international law enforcement cooperation related to digital assets	Attorney General	June 2022	8(b)(iv)
2	Report on the future of money and payment systems	Secretary of the Treasury	September 2022	4(b)
3	Assessment of whether legislative changes would be necessary to issue a United States CBDC	Attorney General	September 2022	4(d)(i)
4	Report on the implications of development and adoption of digital assets for consumers, businesses, and investors	Secretary of the Treasury	September 2022	5(b)(i)
5	Report providing a technical evaluation for a United States CBDC	Director, OSTP and Chief Technology Officer of the United States	September 2022	5(b)(ii)
6	Report on the role of law enforcement agencies with regard to digital assets	Attorney General	September 2022	5(b)(iii)
7	Report on connections between DLT and climate and energy transition consequences	Director, OSTP	September 2022	5(b)(vii)
8	Competitiveness framework for digital assets	Commerce Department	September 2022	8(b)(i)
9	Legislative proposal to achieve #3, based on consideration of #2	Attorney General	October 2022	4(d)(ii)
10	Report outlining financial stability risks and regulatory gaps posed by digital assets, and recommendations	Financial Stability Oversight Council	October 2022	6(b)
11	Update to #7	Director, OSTP	March 2023	5(b)(vii)
12	Report on priority actions taken under established framework for engagement with foreign counterparts on using digital assets	Secretary of the Treasury	March 2023	8(b)(ii)

Organizations are also pursuing the use of blockchain to facilitate cross-border payments, thereby bypassing the process of using intermediaries for clearing and settlement. IBM developed IBM Blockchain World Wire for this purpose [57], although much of IBM's blockchain work has been scaled back[83]. Major banks have entered into this arena: JPMorgan, for example, piloted *Liink* in 2017 and started accepting live transactions in 2019 [58]. However, these solutions tend to be siloed. See the section on the Information Technology and Telecom sector for references.

Regulators and law enforcement are also using blockchain tools in their work. Financial regulatory agencies are using multiple complementary third-party tools to identify, trace, and attribute digital asset transactions on all major and many minor cryptocurrency and stablecoin blockchains. Currently, these tools support hundreds of tokens and use methods such as clustering algorithms, web scraping, and scam database monitoring that enable an investigator to link and attribute a wide range of transactions to real-world individuals and entities. Other regulators and law enforcement agencies use similar products from the private sector to help enhance the government's investigations and enforcement capabilities. Section 4.2.3.2 mentions that the U.S. Government is investigating a variety of technologies, including blockchain technology, as part of CBDC design experiments. It is not unique among governments. As of February 2023, 114 countries are exploring a CBDC: 17 are in the pilot stage and 11 have implemented actual currencies [59], though not all of these leverage blockchain. The European Central Bank (ECB) claimed in 2020 that CBDCs do not need blockchain technology. The purpose of blockchain technology for cryptocurrencies, the ECB said, is to provide trust in the absence of a central authority. But, according to Thomas Moser, an alternate member of the Swiss National Bank's governing board:

> … if you have a central bank, then this is the central party. And if you trust that central party, I think then it's not really straightforward to reason that you need a blockchain [60].

The White House has also noted that various characteristics of commercial blockchain applications may not make sense for a U.S. CBDC System. For example, OSTP noted in a September 2022 report that discusses the permissionless design choice that is common in blockchain implementations [20]:

> While a U.S. CBDC system could, in theory, be mostly "permissionless" from a governance standpoint, this design choice introduces a large number of technical complexities and practical limitations that strongly suggest that a permissionless approach does not make sense for a system that has at least one trusted entity (i.e., the central bank).

Education: The education sector maintains educational records. Among other reasons, an institution preserves a student's history to help other educational institutions and potential employers verify a potential student or employee's credentials. Blockchain technology could be useful to the education sector by reducing the need for educational institutions to maintain their own records of student transcripts, and to provide students with agency over their learning records [61]. Economies of scale would then reduce the overall cost of record maintenance. At the same time, accelerating access to records could increase efficiency in admissions, transfer, and hiring processes. Blockchain technology could also increase

[83] https://www.coindesk.com/business/2021/02/01/ibm-blockchain-is-a-shell-of-its-former-self-after-revenue-misses-job-cuts-sources

confidence in the accuracy of records. Furthermore, sharing of education data is subject to strict privacy rules and regulations. Blockchain technology may help maintain compliance with legal requirements, while also posing challenges for the privacy of student data [62].

Sony Global Education launched a platform to store and access transcripts in 2017 [63]. The system is built on IBM's blockchain, and is intended to be used throughout the world to record educational data from all of the schools a student attends [64].

The U.S. Department of Education launched the Education Blockchain Initiative (EBI) in 2020 [65]. Its purpose is to explore these kinds of distributed ledger applications in the educational sector. EBI's emphasis to date has been on "the secure, traceable, and verifiable exchange of educational data among institutions in the learning and employment ecosystem." [66]. Although EBI aims to use this information to help individuals in their career searches, the initial focus is on an infrastructure that supports institutions. EBI has produced a report to help identify and evaluate how blockchain technology can improve the sharing of data among individuals, educational institutions, and employers, and funded four pilot projects through the Blockchain Innovation Challenge [67].

The EBI report states that "consideration of a blockchain solution … was motivated by … privacy concerns" [65]. A student's record contains personally identifiable information (PII)—e.g., grades and government-issued identifiers—and deserves protection; having the information on a distributed ledger can be dangerous. The pilot project's guiding principles included aligning with pertinent laws and supporting policies and best practices of data privacy. In the report, the project leaders acknowledged, that ongoing development of an equity-centered, high-stakes-privacy, public-sector application is needed.

As part of the Education Blockchain Initiative, the U.S. Department of Education also developed a suite of materials to learn more about education blockchains, including privacy implications.[84]

Energy and Utilities: This sector encompasses the production of energy, including generation of electricity or extraction of fossil fuels, and the transportation of that energy to its destination. In all cases, the objective is to make sufficient energy available to consumers at the times it is needed. The energy supply chain differs from other supply chains. It is seasonal: the need for fossil fuels generally peaks during the winter heating season, whereas the need for electricity (even accounting for electricity generated using fossil fuels[85]) generally peaks during the summer cooling season with much lower demand in the spring and fall [68]. Regional patterns in electricity demand cause variations in seasonal peaks that are important due to limited ability to share resources between large regions of the United States [68]. The need for electricity varies depending on the time of day, usually falling at night, owing both to reduced need for cooling and heating and to reduced consumption for businesses and entertainment. Monitoring and maintaining the electric grid is complex.

Some energy sector interest in blockchain technology is driven by the objective to reduce energy costs and carbon emissions. Promoting clean energy on the grid through blockchain technology has attracted many companies, with some focused on energy generation and delivery, some specializing in blockchain technology, and some simply seeing a worthwhile opportunity [69]. Energy-generating companies record the energy they generate on a

[84] https://tech.ed.gov/blockchain/

[85] https://www.eia.gov/dnav/ng/hist/n3060us2m.htm, https://www.eia.gov/todayinenergy/detail.php?id=10211

blockchain, along with the technology used to produce it, whether clean energy or otherwise. Transmission companies or other entities can use this information to understand the overall amount of carbon dioxide generated. Consumers can choose whether to purchase only energy generated from "clean" sources. There have been pilots in which industrial consumers have exchanged carbon credits with producers [70]. Transparent data is needed on the electricity used, and carbon emissions generated from, U.S. crypto-asset and blockchain operations, in order to verify any potential savings and identify emerging challenges [33].

Most energy sector projects involving a blockchain focus on countries other than then United States. Forbes's 2019 top five list of companies using blockchain technology in service of renewable energy [71] includes only one U.S.-based company, Brooklyn Microgrid, which caters to U.S. residents in New York City [72]. Brooklyn Microgrid created a permissioned blockchain implementation called Exergy, the objective of which is to create local energy marketplaces within the existing energy grid. However, it is unclear whether Brooklyn Microgrid is still operating. A 2021 list of the top 20 blockchain energy start-ups [73] also included COI Energy Services, which is using blockchain technology to provide a service for monitoring, reducing, and repurposing energy waste in buildings [74].

Healthcare and Life Sciences: This sector includes patients; the medical professionals and institutions providing healthcare; the suppliers that support them (medical equipment manufacturers, pharmaceutical companies, and the researchers they employ); and the supply chains that keep hospitals, doctors' offices, and other medical facilities stocked. It also includes insurance companies, but the insurance sector is covered in a separate section.

FAIR principles—which call for information to be findable, accessible, interoperable, and reusable—guide work in this sector [75]. Accurate information on patients, tests and procedures, pharmaceuticals and their efficacy, and the availability of materials and facilities is vital to achieving the sector's objectives and ends. Individuals and organizations in the sector have shown interest in blockchain technology, with its promises of information distributed widely, quickly, and verifiably.

The pharmaceutical industry, for example, has shown much interest in blockchain technology [76]. Supply chain issues have long plagued the sector, but the problem became particularly acute during the COVID-19 pandemic, when temperature-controlled vaccines had to be shipped to pharmacies and doctors' offices [77]. Some hospitals within the United Kingdom's National Health Service have used blockchain technology to monitor the COVID-19 vaccine supply [78].

COVID-19 vaccines presented a use case for blockchain technology, but the pharmaceutical industry recognizes the technology's application elsewhere. The MediLedger Network is an organization established to help the entire industry use blockchain technology to monitor supply chains [21].

The healthcare and life sciences sector sees opportunities for blockchain technology in areas other than supply chains [79]. **Table 4** lists four such projects that were active when this chapter was drafted. The rapid pace of change in this domain means that these projects may well pivot, merge, change name, or simply disperse by the time of publication. Each project focuses on its own use case; all believe blockchain can help integrate information that currently exists on different networks. The Health Record Security project, for example, aims to integrate Estonia's KSI Blockchain with existing Oracle relational databases, thereby simplifying patient record maintenance while increasing “security, transparency, auditability, and governance.” [80; 81]. The Blockchain Claims Process project intends to connect payers directly with providers, and claims it can reduce healthcare expenses by up to $59 billion per year [67]. Hashed Health is providing services to payers, providers, pharmaceutical companies, and suppliers’ laboratories, with the objective of decreasing costs and administrative burdens.

Table 4. Sample Healthcare-Related Blockchain Projects

Project	Inception Date	Description
Change Healthcare Claims-Processing Network [82]	2018	A blockchain-based claims-processing network by Change Healthcare[86] to demonstrate the feasibility of switching from traditional centralized claims processing to distributed claims processing.
Guardtime Health’s HSX Record Security [83]	2020	A project by Guardtime that is using blockchain technology to store electronic patient records in Estonia.
Hashed Health Blockchain Consortium	2016	Described by CrunchBase as “a healthcare blockchain innovation firm creating an ecosystem of businesses that leverage blockchain and DLT” [84] and self-described as “a venture studio driving innovation and collaboration in healthcare” [85]

Information Technology (IT) and Telecom: This sector provides the infrastructure for operating computer networks. With respect to blockchain technology, it connects the nodes on which ledgers exist, and provides the services blockchain applications use to transmit information between distributed ledgers.

TBCASoft, which is promoting blockchain technology for telecommunications systems, participates in the Carrier Blockchain Study Group, a consortium comprising 19 carriers [86]. The consortium already implements blockchain-based cross-carrier purchases (using a mobile device app) that eliminate third-party billing [87]. Working groups are studying (and piloting) the use of blockchain technology in remittance, identity, 5G, telecommunications supply chain, and the IoT [86].

Telecom companies are studying how to use smart contracts to eliminate current costly business practices. One recent article highlights the problem of international voice

[86] https://www.changehealthcare.com/

settlements [88]. Telecom companies bill or pay each other according to pre-arranged agreements. All this data exchange can result in lengthy negotiations, sometimes involving court proceedings, to determine whether records are correct [89]. The article posits that smart contracts, making use of trustworthy blockchain-based records, could eliminate these disputes. However, this may only serve to shift the point of negotiation from the bills to the smart contracts themselves. The third-party clearinghouses currently used to resolve disputes and handle payments would be eliminated. However, another article notes that telecom companies tend to be creating solutions to this problem in silos. These solutions do not communicate with others, and have not progressed past the laboratory stage into the real world [89].

Insurance: The insurance sector manages risk by estimating the probability and consequences of events necessitating settlement.

The potential use of blockchain in this sector would leverage the properties and uses of blockchain described above to reduce risk and uncertainty: interoperable health records, smart contracts, fraud detection, and transaction accuracy [90]. As in other sectors, concerns over privacy and security are extent here, as well.

Guardtime had teamed with EY Global, shipping company Maersk, Microsoft, and four insurance companies to implement a blockchain-based maritime insurance platform, Insurwave [91; 92]. Launched in 2018, the platform has helped manage risk for over 1,000 commercial vessels [93].

Blockchain technology is not necessarily seen as applicable across the entire industry. One paper posits that transactions involving only a few parties, or using a known, trusted intermediary, may operate just as efficiently and effectively using their existing business models [94]. The paper does not provide statistics on the percentage of transactions that fall into these categories, so it is hard to evaluate the statement’s importance.

Media, Advertising, and Entertainment: As described below, blockchain technology is being employed to manage digital rights to media and to track access to digital entities.

Some companies have a business model that rewards active users with tokens. Sapien is a blockchain-based social news platform in which a post’s assumed truth is subject to consensus. If the community unanimously agrees a post is true, its creator earns a token, good for use in Sapien’s metaverse or exchangeable for other cryptocurrency tokens [95]. Vevue rewards video content creation with tokens, although it also rewards site interactions, such as answering fan questions and performing tutorials [96].

Ad metrics fraud is a constant problem in advertising. Ad buyers once hoped metrics would let them track the effectiveness of each advertisement. That quickly yielded to search engine optimization, and then to advanced click-fraud techniques involving botnets [97; 98]. Companies such as Kubient and Rebel AI [99; 100] (since acquired by Logiqlogia) [101] have experimented with blockchain technology to prevent fraudulent botnet traffic. Furthermore, distributed ledgers are a new approach to providing advertisers with immediate access to data; this is in contrast to the traditional model of collecting information in a central database and periodically using that information to create and distribute reports [102].

Mining: Increasingly, consumers are concerned with the environmental, social, and governance costs of the products they purchase. The RCS Global Group [103], a company dedicated to considering these issues in mining materials for batteries, has established a blockchain to provide visibility into material provenance (the mines from which minerals are extracted) and production methods (the degree to which the methods are environmentally and socially conscious).

Retail and E-commerce: This sector concerns the final step of a supply chain: the sale of products to consumers. E-commerce is the portion of retail in which the sale is conducted over the internet.

Many of the familiar names in the retail sector seem to be using or exploring blockchain technology. Examples include:

- French grocer Carrefour SA, which is using blockchain technology to track shipments of fresh meat and produce to its stores (and claims to have seen sales boosted as a result) [104].
- Nestlé, which is cooperating with The Rainforest Alliance to track the origin of coffee beans, their shipping routes, and where they are processed [105].
- De Beers, whose Tracr™ technology tracks the provenance of diamonds [106].
- Ikea, whose Chain of Traceability lets consumers use augmented reality to visualize a product's origins (down to the component level), where and how it is manufactured, and its carbon footprint [107].

Transportation and Logistics: The transportation and logistics sector ensures the movement of goods throughout supply chains. This involves warehouses, modes of transportation (maritime, trucking, rail, aviation, barge), infrastructure, labor, and the planning capability to coordinate these entities.

Major corporations in this sector understand the complexities of information flows in international trade. According to one estimate, mislabeled, misdirected, and stolen cargo account for losses of $50 billion per year [108].

DHL showed early interest in blockchain technology and identified important use cases [109]. As early as 2018, it had partnered with Accenture to develop a prototype system for shipping pharmaceuticals [110]. FedEx has partnered with Hyperledger and is developing a blockchain-based pilot project [111]. Its goals include exploring smart contracts in the industry to improve planning and analysis.

In 2018, IBM teamed with Maersk to develop TradeLens, a blockchain technology-based platform to support asset transparency in the shipping industry [112]. TradeLens involved blockchain access from shippers, ports, terminals, government authorities, and customs officials. It intended to provide a complete picture of an asset's journey from source to destination. In November 2022, IBM and Maresk announced they were ending TradeLens.[87]

Travel and Hospitality: This sector comprises industries that transport people (rather than goods) and provide for their necessities during trips and at destinations.

[87] https://www.supplychaindive.com/news/Maersk-IBM-shut-down-TradeLens/637580/

The World Economic Forum is attempting to simplify travel by providing the Known Traveler Digital Identity System [113]. The system that is being designed claims to be "the first global collaboration of its kind" and brings together governments, consumers (travelers), and the travel industry [113]. Travelers would be able to enter personally identifying information but have the right to determine what to share, and with whom. Travelers would collect "attestations": claims issued by a trusted entity, such as a government or authority. Travelers could then (selectively) present these attestations as necessary to obtain permissions. Accumulating attestations builds trust, simplifying the travel experience. The World Economic Forum partnered with Accenture in 2018 to implement the system, though the current status is unclear [114].

The travel and hospitality sector was perhaps the first commercial sector to implement smart contracts. Fizzy, launched in 2017 by insurance company AXA, used smart contracts to allow customers to automatically obtain flight delay payments. However, AXA ended Fizzy in 2020, citing insufficient demand [115].

A review of start-ups shows that the travel and hospitality industry is using blockchain technology in an attempt to wrest control from the industry's major agents, who charge commissions that end parties would prefer to eliminate or at least reduce [116]. This provides savings to both customers and providers as it can avoid commissions.

4.3.1.1. Public-Private Partnerships Focuses on Promoting the Adoption and Use of Blockchain

Because blockchain is a relatively new technology, there has been little in the way of public-private partnerships. Some government organizations are developing guidelines and standards, and have included representatives from academia, civil society, and industry in their standards and advisory committees. The following subsections briefly describe selected efforts. The first four are U.S. efforts. The last is organized by governments outside the United States.

National Science Foundation

As the Federal Government's leading investor in fundamental and translational research in science and engineering, the National Science Foundation (NSF) has a long history of investing in research and development (R&D) in a range of critical and emerging technologies that underpin blockchain and distributed ledger technology (DLTs) at the nation's universities, non-profit research institutions, and startups and small businesses. NSF's investments have supported a large number of researchers, students, and entrepreneurs who have pioneered seminal breakthroughs leading to today's capabilities.

For example, NSF has supported R&D efforts that have produced many related foundational technical elements (e.g., public-key cryptography, digital signatures, Merkle hash tree, zero knowledge proofs, etc.), alongside advances in sociotechnical innovations, including greater understanding of the commercial and economic value propositions of these capabilities. NSF has also extended the research of DLT and related technologies to other types of architectures and protocols such as directed acyclic graphs (DAGs), in addition to blockchain. Notably, distributed ledger ecosystems supporting digital finance and many broader sectors of the economy are critically dependent upon secure, privacy-preserving, and robust sociotechnical infrastructure that is integrated and interoperable – and NSF's investments have paved the way to foundational advances enabling such infrastructure.

NSF funding has focused on the need for use-inspired research in blockchain and DLT, that is, research that is inspired by potential use cases. Such use cases span the full range of economic sectors, such as health, finance, and energy. They intersect with brick-and-mortar companies, as well as the digital economy, including next-generation Internet architecture and Web 3.0. For example, in healthcare, NSF has funded DLT innovations enabling cross-institutional secure and privacy-preserving data sharing, public health data monitoring, pharmaceutical tracking, and enhanced transparency and cost reductions vis-à-vis claims processing. Similarly, in the energy sector, NSF has funded innovations in DLT that are inspired by the aggregation of distributed energy resources and energy storage, as well as complex utility management more generally.

Finally, NSF-funded translational research has matured the breakthroughs and technologies emerging from the fundamental research described above, while also catalyzing further fundamental research. For example, the NSF Small Business Innovation Research/Small Business Technology Transfer (SBIR/STTR) program, which specifically delineates DLT as a topic area of interest, has funded nearly 50 startups and small businesses to date, covering a wide range of areas including blockchains, DAGs, and related capabilities (cryptography, smart contracts, etc.). Applications of these technologies and approaches span a range of industries and commercial uses.

National Institute of Standards and Technology

The National Institute of Standards and Technology (NIST) has undertaken several blockchain-related projects. NIST, as its name implies, produces standards. When organizations follow standards, "technology work[s] seamlessly and business operate[s] smoothly."[88] NIST's results to date have been expressed as written reports, but not as what it calls standards. The projects conducted research on blockchain applications of interest to a broad community. Examples include:

- Blockchains for industrial applications: A community of interest to explore using blockchain in smart manufacturing.
- Enhanced DLT: A group concerned that blockchain inalterability conflicts with privacy requirements. In particular, Europe's General Data Protection Regulation (GDPR) guarantees European Union citizens the right to have personal data erased from public records. The Enhanced Distributed Ledger Technology group has created a new form of distributed ledger technology that still provides integrity assurance but allows for selected, controlled revision or deletion of data.
- Token Design and Management: A paper presenting a formal model of tokens and their management [117]. It defines a conceptual framework whose purpose is "to lower the barriers to study, prototype, and integrate token-related standards." The paper is intended to help in the design of systems, standards, and protocols by giving form to vaguely defined blockchain-related concepts.

[88] See https://www.nist.gov/standards/.

Each of these papers was prepared with the participation of individuals in the private sector.

Department of Energy

The Department of Energy has begun an effort named Blockchain for Optimized Security and Energy Management (BLOSEM) [118]. The project is attempting to identify features of blockchain that may be useful in creating a robust nationwide electricity grid, one that is capable of meeting the complex generation and transmission needs of the future, as well as withstanding cyberattacks.

BLOSEM aims to stand up a distributed laboratory environment to test the concepts its members propose. Five national laboratories are participating in the project: The National Energy Technology Laboratory, Ames Laboratory, the National Renewable Energy Laboratory, the Pacific Northwest National Laboratory, and SLAC National Accelerator Laboratory. Other participants include NIST, the United States Military Academy, Carnegie Mellon University, IBM, General Electric, the Institute of Electrical and Electronics Engineers (IEEE), and a range of other industry partners.

Department of Homeland Security

In 2016, DHS Science and Technology Directorate (S&T) initiated five distinct but separate R&D projects via its Small Business Innovation Research (SBIR) Program and its Silicon Valley Innovation Program (SVIP) to understand the value and utility of blockchain technologies to the DHS Enterprise. These projects explored various facets of blockchain technologies such as:

1. The format of data in blockchain systems and the utility of linked data structures to ensure interoperability and semantic understanding of that data
2. Use of decentralized registry and discovery services in a blockchain environment
3. The support for confidentiality, integrity, availability, non-repudiation, provenance and pseudo-anonymity in blockchain systems
4. The ability to establish and maintain trusted transactions between the public and private sector owned infrastructures
5. The applicability of blockchain technology to authenticate IoT devices and ensure the integrity and provenance of the data from such devices.

The R&D phase of this work was then followed by 3 separate proof-of-concept (POC) implementations in 2017-2018 to identify scalable integration architectures and to determine the gain/pain ratio of adopting and integrating blockchain technologies into existing DHS technical and business process environments:

1. POC: Authenticity and Integrity of IoT Device, Camera and Sensor Data

   Lesson Learned: Use of blockchain technology within an Enterprise is overkill as there exists existing and mature solutions that are better suited for this purpose.

2. POC: Enhancing the Entry Submission Process to Streamline International Trade Facilitation

   Lesson Learned: Use of common data models based on JSON-LD (Linked Data) is viable, critical and developer friendly. There exists a need to separate on-chain (ledger) data from off-chain (storage) data.

3. POC: Enhancing the Registration and Verification of Intellectual Property Assertions of Imported Goods

   Lesson Learned: There exists a need to standardize interfaces to off-chain confidential storage and authorization capabilities that allow for delegated access to information. In addition, use of standards to prevent vendor lock-in and ensure interoperability between systems is critical.

In May 2018, Douglas Maughan, DHS S&T, testified before the House Committee on Science, Space, and Technology in the U.S. House of Representatives [119]. He mentioned several capabilities that DHS is using public-private partnerships to pursue: on the results of both the R&D conducted by S&T as well as the POCs conducted by S&T in partnership with U.S. Customs and Border Protection.

The results of the R&D and POCs resulted in a clear realization by DHS that to ensure that blockchain technology remains useful, an approach to removing platform, technology, and vendor lock-in was necessary. In particular, the priority at DHS shifted from focusing on the specifics of a blockchain platform to ensuring and prioritizing standards-based interoperability between blockchain systems as well as between blockchain systems and existing Enterprise systems.

To that end, DHS has funded, contributed use cases to, and championed the development of the open, royalty free and free to use global standards at the World Wide Web Consortium (W3C), a global standards development organization, such as its W3C Verifiable Credentials Data Model Standard and W3C Decentralized Identifier standards that provide such wide-spread interoperability between blockchain, non-blockchain and existing systems i.e., These standards do not require blockchains but can support them if they are needed, thus ensuring DHS has choice and flexibility in how it implements solutions.

In late 2018, DHS issued an open solicitation thru its Silicon Valley Innovation Program (SVIP) that specifically required support for these global interoperability standards developed by the W3C to meet the operational needs of:

- U.S. Citizenship and Immigration Services in the digital issuance of high value immigration credentials such as the U.S. Permanent Resident Card and
- U.S. Customs and Border Protection in the digital issuance and verification of cross-border trade documents related to the import of oil, natural gas, steel, agriculture, and e-commerce products.

The seven companies that were competitively selected from an application pool of more than 200 are a mix of companies that use as their infrastructure both blockchain technologies and non-blockchain technologies, while supporting the W3C interoperability standards required by DHS to ensure global, multi-platform, multi-vendor interoperability.

The demonstration of standards based interoperability between these companies and others in the global identity and trade ecosystem has validated the DHS approach to support standards-based APIs and data representation standards when it comes to addressing blockchain technologies, which ensures vendor choice and prevents technology and platform lock-in.

Public-Private Partnerships Outside the United States

The European Union, together with Norway and Lichtenstein, launched the European Blockchain Partnership (EBP) in 2018. Its objective is to build what it calls the European Blockchain Services Infrastructure (ESBI). ESBI leverages open-source blockchain standards and aims to provide a set of standardized APIs. The APIs will allow organizations (government and otherwise) and citizens to develop applications that are compliant with ESBI and can interoperate with other ESBI-based applications. EBP is initially concentrating on four use cases: identity, education, social security, and document traceability [120].

Countries that have launched CBDCs have also formed public-private partnerships to implement the underlying technology. The Central Bank Digital Currency Tracker website[89] lists 21 firms working with governments. Most of these firms have partnered with a single government. Two, however, have partnered with many governments: Bitt Inc.[90] has partnered with 12 and Soramitsu[91] with 7. Bitt Inc.'s business is helping countries operationalize digital currencies, including CBDCs, whereas Soramitsu delivers blockchain-based solutions to customers, including CBDCs.

4.3.1.2. Industry-Based Bodies that Develop Voluntary Standards for Blockchain

Blockchain technology has few widely accepted standards. There are no internationally recognized bodies that deal specifically with standards across all blockchains. Instead, some traditional technology-focused organizations have—with participation from industry, government, and academia—worked on and published voluntary standards for the design, implementation, and use of blockchains. A paper from 2020 surveying the topic concluded:

> There are still no standards catering to the mass implementation of blockchain and the situation must change to ensure a sustained survival of the DLT ecosystem as a major part of modern technology [121].

Without standards that govern how to implement and use blockchains, the technology could fragment across applications: one set of standards for using blockchains in support of supply chains, another set for healthcare, etc.

The International Organization for Standardization (ISO) has established a technical committee to develop and promote standards for blockchain and distributed ledger technologies [122]. To date it has published seven documents, shown in **Table 5**. Of these documents, only Vocabulary (ISO 22739:2020) has undergone the ISO review process that results in an official, published standard. Also, only two are standards: Vocabulary and Reference Architecture. As for the others [123]:

- Those with "/TS" in their identifiers are technical specifications. A technical specification describes an area for which experts agree standards would be useful, but which is not yet ready to be standardized. The objective in writing a technical

[89] https://www.atlanticcouncil.org/cbdctracker
[90] https://www.bitt.com/
[91] https://soramitsu.co.jp/

specification is to document work that, after some use and review, appears likely to evolve into a standard.

- Those with "/TR" are technical reports. A technical report is informative rather than normative.

Table 5. ISO-Published Blockchain Documents

Standard	Publication Date	Identifier
Vocabulary	July 2020	ISO 22739:2020
Privacy and PII protection considerations	May 2020	ISO/TR 23244:2020
Reference architecture	February 2022	ISO 23257:2022
Taxonomy and ontology	November 2021	ISO/TS 23258:2021
Overview of and interactions between smart contracts in blockchain and DLT systems	September 2019	ISO/TR 23455:2019
Security management of digital asset custodians	December 2020	ISO/TR 23576:2020
Guidelines for governance	February 2022	ISO/TS 23635:2022

ISO is preparing 10 additional documents (**Table 6**). With two exceptions, ISO/PRF TR 23249 and ISO/PRF TR 23249, the documents are under preparation or not approved by the blockchain technical committee and do not yet have a publication date. As in **Table 5**, most documents are technical reports and technical specifications, not standards. Vocabulary (ISO/CD 22739) contains updates to the vocabulary published in July 2020.

Table 6. Unpublished ISO Blockchain Documents

Standard	Identifier
Use cases	ISO/DTR 3242
Identifiers of subjects and objects for the design of blockchain systems	ISO/WD TR 6039
Data flow model for blockchain and DLT use cases	ISO/WD TR 6277
Decentralized identity standard for the identification of subjects and objects	ISO/AWI 7603
Vocabulary	ISO/CD 22739
Overview of existing DLT systems for identity management	ISO/PRF TR 23249
Legally binding smart contracts	ISO/DTS 23259
Interoperability framework	ISO/AWI TS 23516
Overview of smart contract security good practice and issues	ISO/WD TR 23642
Overview of trust anchors for DLT-based identity management (TADIM)	ISO/DTR 23644

IEEE is actively working on blockchain-related standards [124]. IEEE has published 9 standards (**Table 7**) and lists 49 under development. As the titles indicate, five of these standards concern cryptocurrency, no doubt reflecting the first major application of blockchains. The standards under development cover other application areas (agriculture, autonomous vehicles, energy, healthcare, and telecommunications, among others). They also concern foundational blockchain technologies (blockchain architectures, smart contracts, testing) and their implementation.

Table 7. IEEE Published Blockchain Standards

Standard	Publication Date	Identifier
IEEE Standard for a Custodian Framework of Cryptocurrency	June 2020	2140.5-2020
IEEE Standard for General Process of Cryptocurrency Payment	June 2020	2143.1-2020
IEEE Standard for a Custodian Framework of Cryptocurrency	July 2020	2140.5-2020
IEEE Standard for General Requirements for Cryptocurrency Exchanges	November 2020	2140.1-2020
IEEE Approved Draft Standard Data Format for Blockchain Systems	December 2020	2418.2-2020
IEEE Standard for Framework of Blockchain-Based IoT Data Management	January 2021	2144.1-2020
IEEE Approved Draft Recommended Practice for E-Invoice Business Using Blockchain Technology	March 2021	2142.1-2021
IEEE Standard for the Use of Blockchain in Supply Chain Finance	September 2021	2418.7-2021
IEEE Standard for Security Management for Customer Cryptographic Assets on Cryptocurrency Exchanges	January 2022	2140.2-2021

The American National Standards Institute (ANSI) has published a risk assessment framework for blockchain [125]. The framework is specifically for permissioned blockchains.

The European community is also working to standardize aspects of blockchain. Examples of standards organizations include:

- The European Telecommunications Standards Institute (ETSI), which has published a standard on system architecture for smart contracts [126].

- The European Committee for Standardization (CEN), which formed a technical committee in 2019 to investigate blockchain and distributed ledger technologies (DLT) [127]. To date it has not published any standards.

Several industry-based consortiums have arisen from the desire to promote blockchains for purpose-based tasks. These consortiums are driving the adoption of voluntary standards.

Two significant organizations that promote industry-based standards are worth discussing at length. The Enterprise Ethereum Alliance (EEA), based on the public Ethereum blockchain, is an industry organization whose vision is "a world of collaboration built on a new foundation of trust," and whose mission is to "enable organizations to adopt and use Ethereum technology." [128]. EEA membership is open to industry, legal practitioners, government, non-governmental organizations, and academic institutions. However, of these categories, only industry and legal practitioners have voting rights [129]. EEA is not an ANSI accredited standards development organization (SDO), nor have its standards been approved as American National Standards (ANSs).[92]

The EEA has published five documents. These documents are shown in **Table 8**. The first three may be regarded as standards for implementing and using blockchains. The last two are guidelines and best practices.

Table 8. EEA Publications

Document	Version	Publication Date
Enterprise Ethereum Alliance Client Specification	6	November 2020
Enterprise Ethereum Alliance Permissioned Blockchains Specification	2	November 2020
Enterprise Ethereum Alliance Off-Chain Trusted Compliance Specification	1.1	October 2019
EEA Architecture Stack		December 2020
Crosschain Security Guidelines	1	September 2021

In 2015, The Linux Foundation started the Hyperledger Project, now generally referred to as Hyperledger [130]. The project's objective was to bring together parties interested in developing and using blockchain and related technologies. Its first members included companies, in particular IBM and Digital Asset, that had devoted resources to developing blockchains and supporting infrastructure.

Hyperledger has produced white papers, but has not yet produced any standards. Rather, its products provide de facto standards through their APIs. To use Hyperledger, a product requires accessing that product through defined APIs, thereby standardizing best practices. The Linux Foundation considers six of these products to be "graduated" (i.e., ready for

[92] See American National Standards Institute (ANSI) Accredited Standards Developers, last updated September 2, 2022, available at https://share.ansi.org/shared%20documents/forms/allitems.aspx?rootfolder=/shared+documents/standards+activities/american+national+standards/ansi+accredited+standards+developers&folderctid=0x01200019af95c796227a438566c464851845db. For a list of Approved ANSs, see https://ansi.org/american-national-standards/info-for-standards-developers/ans-complete-lists.

production use) [131]. Each addresses some aspect of the architecture of blockchain-based applications:

1. Aries, a library for working with verifiable digital credentials.
2. Besu, distributed ledger software implemented as an Ethereum client, and emphasizing flexible permissioning schemes.
3. Fabric, distributed ledger software providing foundational technology for blockchain-based application development. Fabric emphasizes modular architecture: components such as the consensus protocol can be switched as needed. This is one of Hyperledger's most popular products and is also discussed in Section 4.3.1.
4. Indy, distributed ledger software in the form of tools, libraries, and components in support of digital identities embedded in blockchains.
5. Iroha, distributed ledger software designed to fit into existing infrastructure and IoT projects.
6. Sawtooth, distributed ledger software whose modular architecture explicitly separates blockchain details from the application domain. Sawtooth is designed to support smart contracts, enabling business rules to be separated from underlying blockchain design issues.

Hyperledger also has nine "incubating" products. These support specific aspects of using blockchains, including cloud-based blockchains, integrating multiple blockchains, and creating blockchain dashboards.

Many other organizations have arisen, each generally promoting the use of blockchain in some sector. The following briefly describes a few:

- The Blockchain Association is a member-led trade association dedicated to promoting the potential of blockchain technology to advance the future of cryptocurrency.
- The Global Blockchain Business Council (GBBC) is an industry association working with regulators and business leaders [132].
- The Blockchain Collaborative Consortium is a Japanese consortium covering financial services, manufacturing, and retail [133].
- The Energy Blockchain Consortium promotes the use of blockchain technology in the energy sector [134].
- R3 is a consortium of commercial organizations working to use blockchain to promote trust in regulated markets [135].
- Bonifii (CULedger until recently) is developing a blockchain-based infrastructure for financial services [136].

- The Wall Street Blockchain Alliance is a non-profit trade association whose mission is to promote blockchain adoption in global markets [137].
- The Government Blockchain Association is an international association, incorporated as a U.S.-based nonprofit, promoting blockchain technology for solving government problems.[93]

These organizations have arisen independently and sometimes have overlapping objectives. The statement that the GBBC is working with regulators and business leaders comes from their website, and emphasizes their focus; but others make the same claim, if only in their particular area of interest.

4.3.1.3. Description of the Ways Entities or Industry Sectors Develop, Implement, and Promote the Use of Blockchain

Entities and industry sectors are developing, implementing, and promoting blockchain technology in three ways: developing business models, engaging in consortia for the development of open-source platform technologies, and participating in standard-setting activities. The commercial solutions provided by these companies are customized versions of open-source blockchain platforms, such as Hyperledger and Ethereum. These open-source platforms serve as both unsanctioned standards and as starting points for international standard-setting bodies, such as ISO, IEEE, and the ITU Telecommunication Standardization Sector (ITU-T) [138].

4.3.2. Federal Agency Roles

The roles of federal agencies are discussed from two perspectives: cross-cutting blockchain issues and select existing or emerging blockchain use cases.

4.3.2.1. Cross-Cutting Blockchain Issues

Within the set of foreseeable use cases of blockchain technology, a relatively small number of issues appear repeatedly. Each of these issues is discussed here.

Personal digital identity management: Many blockchain applications include a network of participants that must be identified. The challenge of personal digital identity management is to ensure security, i.e., proof of certain facts or conditions, while protecting privacy, i.e., restricting publicly visible information. The relative balance between security and privacy varies across applications. The need to protect PII is well understood, but determining who may legitimately access PII is challenging. In medical applications, for instance, it is theoretically desirable that medical professionals can share patient records easily, yet this does not mean that every medical professional should be able to access every patient's records. Then too, building a secure system has proven challenging. Bad actors have a long history of exploiting insecure code.

[93] See https://blockchainindustrygroup.org/influencers/government-blockchain-association/.

Public-key encryption allows blockchain participants to attest to certain facts, such as possessing a sufficient amount of cryptocurrency for a purchase without necessarily providing self-identifying information. For pseudonymous transactions, public-key encryption has proven sufficiently strong and secure [10]. For the large majority of digitally-based transactions (e.g., banking, securities trading, education, healthcare, and insurance), however, the connection of a digital identity to a specific person is necessary—and sometimes legally required. Federal agencies, the private sector, and Congress are all grappling with creating, protecting, and managing digital identities better [139–141]. Identity management responsibilities are distributed across the Federal, State, local, and Tribal governments. At present, responsibility for blockchain-based identity management would fall to the agency with regulatory oversight over the specific blockchain use-case. The Federal Information Security Management Act of 2002 (FISMA)[94] requires NIST to develop identity management guidelines and minimum standards for use by Federal agencies [142]. These standards would extend to include identity management needs to support blockchain applications.

Device identity management: High-speed communication networks have enabled billions of physical devices around the world to be connected to the internet to share data [143]. Many blockchain use cases—especially those related to healthcare, supply chains, energy, manufacturing, and provenance—are designed with the expectation that digital devices will contribute data to the blockchain. A recent report from the Department of Commerce states that government oversight of these connected digital devices—collectively referred to as the IoT—is a "qualitatively different challenge to government and society that has not been encountered before" [144]. Similar to people contributing to blockchains, these digital devices require unique digital identifiers to participate in a blockchain network. Furthermore, in blockchain applications with regulatory oversight, digital devices will likely require assigned ownership to a person or organization with legal responsibility for the veracity of the sensor function and data recorded on the blockchain.

Data compliance, privacy, and protection: Because blockchain applications create, access, modify, and delete digital information, they are subject to all data compliance, privacy, and protection laws. In the United States, data compliance and privacy laws have emerged sector-by-sector with health care,[95] banking,[96] and securities trading[97] operating under different regulations for the protection of non-public personal information [145]. Under FISMA, all Federal agencies are required to assess and reduce risk of data compromise. Permissioned blockchain applications or blockchain applications that link to "off-chain" encrypted data files could contain non-public personal information [146]. Similar to personal digital identity management, absent a government-wide policy on data privacy and protection, each Federal agency with data protection and privacy oversight responsibilities will be obligated to analyze blockchain data use on a sector-by-sector basis. The distributed nature of blockchain data storage means that a single blockchain application may exist on nodes that are physically located in many different countries and thus subject to data privacy laws beyond those set by the United States, like the EU's GDPR [147].

[94] FISMA was signed into law as part of the Electronic Government Act of 2002

[95] Health Insurance Portability and Accountability Act of 1996 (HIPPA)

[96] Gramm–Leach–Bliley Act (GLBA)

[97] Sarbanes-Oxley Act of 2002 (SOX)

Smart contracts: Smart contracts are computer protocols designed to automatically enforce agreements among multiple untrusted parties once required conditions are met [148; 145]. The untrusted parties could be people, digital devices, or both. All stages and elements of the smart contract are stored and recorded on the blockchain, including required conditions, the smart contract executable code, and the execution of the smart contract. Smart contracts could play a prominent role in nearly all blockchain applications. However, significant consumer harm and losses could arise from improper or flawed implementations. Recently, this has been demonstrated by exploits of decentralized finance (DeFi) services [149].

The legal standing of an automatic, code-executed agreement between potentially unknown parties is currently unclear [150; 151]. The Uniform Commercial Code (UCC) is a comprehensive set of State laws governing all commercial transactions in the United States [152]. State governments are considering new laws across all aspects of blockchain technology, including extending the UCC to include smart contracts [153].[98] Since parties involved in a smart contract may be unknown to one another, guaranteeing that all parties are legal participants (e.g., not minors) is challenging and links to the importance of personal identity management, discussed above.

Smart contracts may offer significant opportunities for Federal agencies with oversight over export controls,[99] counterfeit prevention,[100] and the enforcement of U.S. trade law, among other areas.[101] Exchanges of goods and materials through smart contracts recorded to a blockchain expedite the auditing and forensic activities associated with the regulatory obligations pertaining to export controls, counterfeit prevention, and adherence to trade law.

Smart contracts can also be used to grant data access and sharing privileges. The Cybersecurity and Infrastructure Security Agency (CISA) lists the management of decentralized data records as a primary strategic challenge [154]. CISA views blockchain technology as a potential solution to managing transactional records and considers smart contracts as a potential method for controlling who gets access to what data and for how long.

4.3.2.2. Existing or Emerging Blockchain Use Cases

Since blockchain technology is a method for recording information, and recording information permeates nearly every aspect of modern society, there are numerous potential applications of blockchain technology. The extent to which blockchain technology realizes this potential is unclear [4]: in some situations, other technologies may be more appropriate. Instead of an exhaustive summary of all possible applications, we restrict the discussion to certain existing or emerging use cases. The use cases were chosen to cover a range of Federal agencies that are being confronted with blockchain regulatory issues, or might be confronted with such issues in the near term.

[98] Indiana Senate Bill 351, for example, would "add a new chapter to the Uniform Commercial Code (UCC) that governs transactions involving controllable electronic records."

[99] Agencies involved in the administration or enforcement of export controls include: DOC, DOS, SEC, DOJ, USDA, DHS, DOE, and DOI.

[100] Agencies charged with counterfeit protection include: FDA, OIPR, USITC, FBI, and CBP.

[101] Including all U.S. Government Trade Agencies: USDA, DOC, DOE, DOL, DOS, Treasury, EPA, FDA, USAID, USITC, USTDA

Cryptocurrency: Blockchain technology is the foundation for supporting the more than 10,000 cryptocurrencies, which have had a total asset-class value of as much as approximately $1 trillion.[102] In 2017, the Securities and Exchange Commission (SEC) determined that cryptocurrency is a virtual currency for the purchase of goods and services, and that most cryptocurrencies act as a security and, as a result, are subject to the Securities Exchange Acts of 1933[103] and 1934 [155]. However, SEC Chair Gensler has questioned whether Bitcoin is "maybe" a commodity, not a security.[104] Practically anyone with access to a digital device has the ability to exchange fiat currency for cryptocurrency at numerous cryptocurrency exchanges, allowing cryptocurrency to be used as a store of value [156].

Many cryptocurrencies have proven volatile, so in response organizations have created stablecoins. A stablecoin is a cryptocurrency designed to provide stable value, typically by maintaining collateral in the form of reserves of some asset such as a country's currency, or by using algorithms that adjust supply to dampen value fluctuations, or both. Tether, begun in 2014 was the first stablecoin, and claims to have one U.S. dollar for each Tether "dollar".[105] In practice, stablecoins have not always lived up to their claims. The purported algorithmic stablecoin TerraUSD, launched in 2018, collapsed in May 2022 [157].

In 2021, the President's Working Group on Financial Markets found that cryptocurrency "poses illicit finance concerns and risks to financial integrity, including concerns related to compliance with rules governing anti-money laundering (AML) and countering the financing of terrorism (CFT) and proliferation" [158]. The dual use of cryptocurrency as both a currency and security creates jurisdictional oversight that spans the banking, securities, and broader financial sectors, including the SEC; Commodity Futures Trading Commission (CFTC); Department of the Treasury, including its Financial Crimes Enforcement Network; Office of the Comptroller of the Currency; and Internal Revenue Service. In addition, working with federal law enforcement agencies, the Department of Justice (DOJ), through a national network of prosecutors and DOJ's National Cryptocurrency Enforcement Team, investigates, prosecutes, and otherwise disrupts criminal offenses involving the theft of digital assets and the exploitation of digital assets to facilitate or conceal other criminal activity [159]. In terms of blockchain technology in the context of cryptocurrency, these regulatory and enforcement efforts span all four of the cross-cutting issues concerning blockchain discussed above.

Central Bank Digital Currency: The Federal Reserve is studying the possibility of creating a digital U.S. dollar to complement cash and electronic money transfers [160]. While printing and regulating U.S. dollars—both paper and those with only a digital representation—fall within the role of the Federal Reserve, the Federal Reserve has stated that specific authorizing language from Congress and support from the executive branch is needed before moving forward with the issuance of a CBDC [160]. Depending on the design of the CBDC, blockchain technology might play a central role or not be used at all. Eleven nations have launched a CDBC, and 103 others are considering creating, or are in the process of creating, a CDBC. Of these combined 114 nations, 18 are using blockchain technology exclusively, and a further 16 are using blockchain and existing technologies [161].

[102] As of January 18, 2023, the value was approximately $966 billion. See https://coinmarketcap.com/.
[103] https://www.govinfo.gov/content/pkg/COMPS-1884/pdf/COMPS-1884.pdf
[104] https://www.protocol.com/fintech/gensler-sec-bitcoin-commodity
[105] See https://tether.io/

Intellectual property: Across a wide range of sectors and applications, intellectual property (IP)—such as music, software, digital media, and artwork—is and may be exchanged in blockchain-enabled marketplaces. A blockchain-based IP management system could enhance the efficiency of IP rights management for individuals, companies, and government regulators, as well as improve detection of counterfeit products [162]. Article I, Section 8 of the U.S. Constitution gives Congress express authority to grant authors and inventors time-limited exclusive rights to their creations. Congress has delegated the responsibility of administering patent and trademark rights to the U.S. Patent and Trademark Office and copyrights to the U.S. Copyright Office. Opportunities exist for these agencies to explore blockchain-based solutions for internal recordkeeping, information exchange and dissemination, and customer interaction.

Food Quality Assurance: Food quality assurance requires oversight of complex, multi-actor, global supply chain networks [163]. Blockchain technology is being actively developed, tested, and piloted by industry and technology leaders as a solution to address quality assurance, food provenance, and traceability [164]. Blockchain solutions in the food sector depend on the IoT to continuously track and monitor environmental conditions during transport [165]. The transparency and real-time auditability of blockchain-based food quality assurance systems have the potential to reduce food contamination and associated health risks while, at the same time, forestalling the unnecessary recall of foods. Some blockchain food assurance projects provide a complete history of the food product to the consumer [166]. For example, by scanning a QR code attached to a seafood product, a consumer could find the date and region of harvest, along with the travel history from catch to market. Widespread adoption of blockchain technology by multinational food companies is possible. Such an outcome would pose challenges to the dozen departments or agencies implementing more than 35 statutes pertaining to food safety [12].

Many agencies with roles involving oversight of some aspect of food quality assurance are exploring blockchain technology. The Food and Drug Administration is developing a rule to establish additional traceability and recordkeeping requirements for food manufacturing, processing, packing, and storage [31]. While not final, this rule is expected to accommodate and possibly promote the use of automated digital recordkeeping, such as blockchain. The U.S. Department of Agriculture is exploring the use of blockchain technology within the National Organic Program [167]. NOAA is including blockchain technology as it tries to improve fisheries management and traceability [168].

4.3.3. Interaction of Federal Agencies with Industry Sectors

Federal agencies are interacting with industry sectors in two ways: 1) expanding sector-specific regulatory oversight to include blockchain or clarifying that existing oversight includes blockchain, and 2) supporting and partnering with industry on the development of sector-specific blockchain use-cases and pilot projects. As mentioned in 4.3.2.2, the use of blockchain technology to enable cryptocurrency, for example, resulted in the clarification and expansion of AML/CFT regulations, including know-your-customer (KYC) provisions to ensure their application to cryptocurrency exchanges. The SEC has promulgated guidelines on when U.S. securities laws are applicable to initial coin offerings (ICOs) [169]. Recent remarks by SEC Chair Gary Gensler made clear that the SEC, along with the CFTC, intends to significantly strengthen the government's interaction with and oversight of the cryptocurrency market in the near future [170]. Areas of increased oversight by the SEC and CFTC could include 1) registration of exchanges, 2) determination of when a token is a commodity and when it is a security, and 3) additional protections for custody of digital assets. Other agencies are similarly evaluating how to enhance oversight of this fast-evolving industry, as discussed further in the publications prepared by various government agencies under Executive Order 14067 listed in **Table 3**. Section 4.3.2.2 also discussed a few agency-led initiatives to explore and test the potential of blockchain technology. Additional examples include the use of blockchain technology for: managing the electricity grid, managing pharmaceutical supply chains, and operating exchanges of securities [171; 118; 30].

4.3.4. Interagency Activities

Signed on March 9, 2022, the President's Executive Order on *Ensuring Responsible Development of Digital Assets* created an interagency process for carrying out the Order's numerous directives [35]. The interagency process is coordinated by the National Economic Council and the National Security Council, under the direction of the economic policy advisor and the national security advisor. More than 20 departments, agencies, offices within the White House, and independent regulatory bodies are participating in the interagency process.

The interagency process is instructed to provide analyses in the following areas:

- The future of money and payment systems
- Legislative changes and a legislative proposal for issuing a CBDC
- Implications of a CBDC for consumers, investors, businesses, and equitable economic growth
- A technical evaluation of a CBDC
- The role of law enforcement in detecting, investigating, and prosecuting criminal activity related to digital assets
- The connection between blockchain technology and the energy transition; financial risks and regulatory gaps posed by adoption of digital assets
- Views on the risks of illicit finance
- A plan for mitigating digital asset-related illicit finance and national security risks
- A summary of pending, proposed, and prospective rulemaking to address digital asset illicit finance risks
- A framework for international engagement for the adoption of principles and standards related to digital assets
- A framework for enhancing U.S. economic competitiveness in developing digital assets, and

- How to strengthen international law enforcement to detect, investigate, and prosecute criminal activity related to digital assets.

See **Table 3** for a discussion of the reports required by Executive Order 14067 and their status. Blockchain technology is included, directly or indirectly, in most of the Executive Order reports. For example, blockchain technology could be adopted to support all or part of a CBDC issued by the Federal Reserve (see 4.3.2.2 for more information). Overall, blockchain technology features prominently as experts across the Federal Government conduct the analyses required by the Executive Order.

OSTP also coordinates various Federal activities and research and developments relating to a number of technologies underpinning digital assets, including blockchain, as mandated by law in 42 USC § 19271 [172]. This includes coordinating an interagency effort to develop a National Digital Assets Research and Development Agenda.

4.3.5. Regulations, Guidelines, Mandatory Standards, Voluntary Standards, and Other Policies Implemented by Federal Agencies

Numerous statutes regulate the use of blockchain technology in support of government-related activities. FISMA requires agencies to implement programs to protect all forms of digital information and tasks NIST with developing minimum standards for agency-developed information security programs [173]. In addition, FISMA requires DHS and the Office of Management and Budget (OMB) to issue and implement government-wide guidance and programs intended to improve agencies' information security. OMB Circular A-130 makes clear the information security requirements extend to all non-Federal entities that collect or maintain information on behalf of the Federal Government [174]. The Federal Information Technology Acquisition Reform Act (FITARA) governs all devices and data centers used to maintain or store blockchain information.

Core technologies used to create blockchain technology—such as cryptography, hashing, public-private keys, and data security—have applicable standards. As discussed in Section 4.3.3, Federal agencies are working to accommodate the application of blockchain technology within specific sectors on a case-by-case basis. Similarly, while blockchain technology—as a whole—is not export controlled, the underlying algorithms or computer hardware used to create blockchain solutions could be subject to export control regulations under the International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EAR). Enforcement of ITAR and EAR is carried out by the Department of State and the Department of Commerce, respectively, with criminal enforcement carried out by federal law enforcement agencies and the DOJ.

NIST maintains and develops an extensive suite of standards for operations that form the foundation of blockchain technology, such as hashing, digital keys, and data security (see Section 4.3.1.1). Developers of blockchain technology are encouraged to adopt these standards, such as the Secure Hash Algorithm-2 [175] and pseudorandom number generator algorithms [176]. Cryptographic tools used by popular blockchain technology platforms cannot always be validated against the suite of NIST cryptography standards [177].

In addition to data security, NIST develops and maintains standards on other key aspects of blockchain technology, such as personal digital identity management and digital device management. Guidelines for all aspects of personal identity management, ranging from enrollment to proofing to authentication, are detailed in a series of NIST Special Reports.[106]

There is also increased focus on blockchain technology by regulators. In May 2022, the Treasury Department sanctioned the virtual currency mixer Blender.io. The company uses blockchain technology to mask digital currency transactions that would normally be public. The company was used by Lazarus Group, the Democratic People's Republic of Korea's state-sponsored cyber hacking group, a sanctioned country and company, to move stolen cryptocurrency out of the United States. Under the sanctions, all property of Blender.io in possession of U.S. persons must be reported to the Treasury Department [178]. These sanctions, which are the first of their kind, represent a marked shift in the approach to blockchain companies. The sanctions demonstrate that the United States is serious about ensuring that blockchain companies are building and using technology aligned with democratic values.

4.3.6. Guidelines, Mandatory Standards, Voluntary Standards, and Other Policies Implemented by Industry-Based Bodies

Blockchain standards and guidelines across industry generally take two forms. The first is through formal standards such as those put in place by IEEE and ISO. These standards are generally created to reduce uncertainty when using a specific product (in this case, a blockchain implementation) and can also facilitate ease of use and, in some cases, lower costs [179]. The second form is through the blockchain networks themselves. Open-source blockchain platforms allow users to design and implement new applications on top of existing technology with specific design protocols, rather than build the technology from the ground up. The design choices implemented by the developers of these underlying platforms act as a de facto standard in blockchain development.

With respect to actual standards surrounding blockchain, standards generally focus on particular fields in which blockchain is implemented. IEEE has a number of blockchain standards, most of which focus specifically on cryptocurrency (see **Table 7**; also see Section 4.3.1.2). Standards in other areas focus on digital asset and data management. As of May 2022, there were nine published IEEE standards for blockchain. However, there are roughly 50 blockchain standards that are currently under development [124].

In addition to these standards, ISO has established a technical committee governing blockchain and distributed ledger technologies [180]. This committee has engaged in projects that include mapping the design and use cases of blockchain and establishing fundamental blockchain terminology [181], as well as developing standards across a range of focus areas [182]. See **Table 5**.

The development of many third-party applications, such as third-party coin wallets, that employ the same underlying blockchain technology has prompted some to propose a standard for tokens within smart contracts. One such example, an Ethereum Improvement Proposal (EIP), is the EIP-20: Token Standard by the Ethereum platform, which enables users to transfer tokens between multiple third-party apps [183]. In this case, these standards govern how developers write the format of the code. Specifically, this standard defines the function

[106] See NISTSP 800-63-3, NISTSP 800-63A, NISTSP 800-63B, and NISTSP 800-63D

names and parameters used when creating smart contracts [184]. This standard was updated by EIP-777, which is retrospectively compatible with the original standard [185]. Therefore, code compatible with EIP-777 is also compatible with EIP-20.

A 2020 report by the World Economic Forum on blockchain technical standards noted several gaps in the current blockchain standardization landscape. Specifically, the report found that despite several organizations having definitions for blockchain, inconsistent use of terminology has led to challenges in developing a common understanding. Furthermore, the complex nature of blockchain technologies makes establishing the scope of blockchain standards difficult. The document notes significant overlap in the standards landscape, with high activity concentrated in particular areas and relatively few standards in others [186].

Beyond the formal industry standards, open-source blockchain networks have gained prominence in the field, establishing themselves as de facto standards. One such example is the Ethereum Network [161]. The design choices that this platform uses govern the applications, smart contracts, and other tools built on the network. One such example is the consensus mechanism. Previously, Ethereum used the proof-of-work consensus mechanism, meaning that to add blocks onto a chain, users had to use computer power to engage in some *work* (usually computationally intensive math problems). In October 2022, Ethereum adopted proof-of-stake as the consensus mechanism, meaning that these same users had to, instead, stake Ether (see Section 4.2.1.4), the Ethereum cryptocurrency, in order to earn the right to append new transactions to the blockchain. This may lead to proof-of-stake becoming a de facto standard.

4.3.7. Federal Government Resources for Consumers and Small Businesses to Evaluate the Use of Blockchain

To date, the Federal Government has taken a few steps to provide resources for consumers and small businesses to evaluate the use of blockchain technology. The Federal Government has:

- Assembled documents relating to the regulation of cryptocurrencies and crypto assets. These can be found on the Library of Congress's website [187].
- Promoted research on blockchain applications through the Small Business Innovation Research (SBIR) program [188].

Although the Library of Congress exists to serve the U.S. Congress, many of its resources are freely available to the public, and therefore of use to consumers and small businesses. In this case, the assembled resources help consumers navigate the tax implications of cryptocurrencies and provide small businesses with the information they need to use cryptocurrencies in compliance with Federal and State laws.

The Library of Congress limits its blockchain technology resources to the legal area. It does not help consumers or small businesses set up a new blockchain implementation, connect to an existing one, or develop blockchain applications.

The SBIR program has issued many grants to small businesses conducting blockchain research.[107] The nature of these research efforts ranges from the theoretical to the practical. On the theoretical side, the NSF has provided small businesses with resources to conduct research on protocols, security, and fault tolerance [189]. Practical projects have considered the use of blockchain technology in specific application areas. Fig. 1 shows the distribution of 60 of the projects among government departments and agencies. The Department of Defense funds a plurality of the projects, followed by the NSF and DOE.

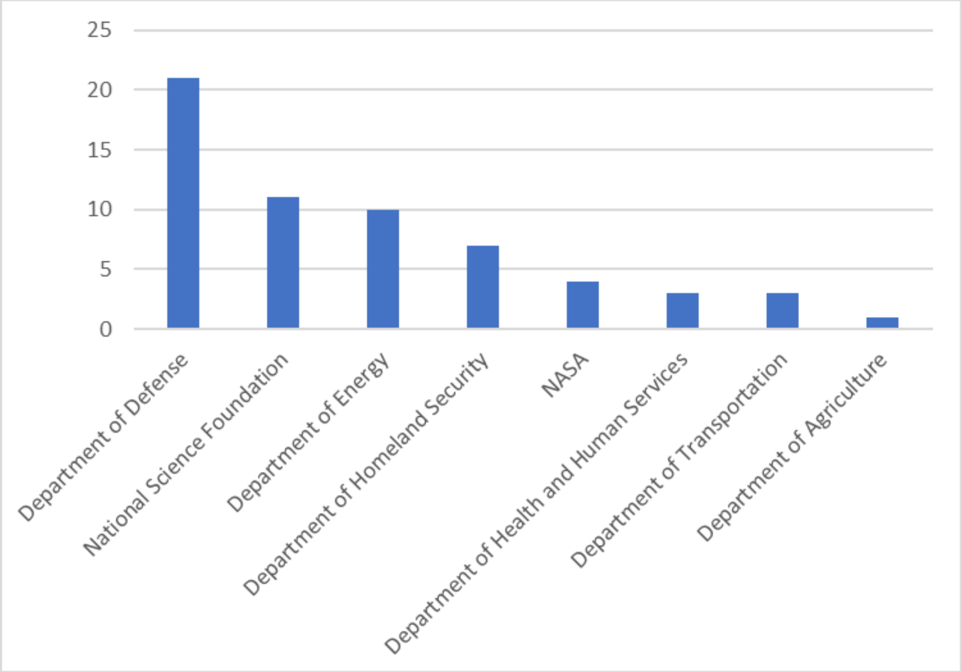


Figure 1. Blockchain-Related SBIR Projects Grouped by Federal Agency

4.3.8. Building a Blockchain Workforce

Blockchain is multidisciplinary. As Section 4.2.3 points out, the current applications of blockchain are many and diverse. Developing, operating, and maintaining blockchains requires a workforce with specific skills not taught in today's traditional university curricula. As blockchains grow and their use becomes more common, demand for individuals with specialized blockchain-related knowledge will grow. To mitigate blockchain's risks, a workforce with both technical and sociotechnical expertise will be necessary.[108]

Experts' opinions, course syllabi, and job listings all provide clues as to the skills blockchain developers and operators must possess. There is general agreement on the following subject areas [190–192; 23; 193]:

- Programming languages: Understanding how to write applications that use blockchains, how to query blockchains, and how to submit transactions. Judging

[107] As of this writing, a search on the SBIR's website lists 474 funded projects.
[108] See U.S. Department of Commerce's report *Responsible Advancement of U.S. Competitiveness in Digital Assets*. https://www.commerce.gov/sites/default/files/2022-09/Digital-Asset-Competitiveness-Report.pdf

from the sources surveyed, there is little interest in training individuals to develop blockchains from scratch.

- Data structures: This fundamental computer science concept is the key to thinking conceptually about a blockchain, blocks, and block components.
- Cryptography: Understanding the cryptographic principles that make a blockchain tamper-resistant, and that keep transactions pseudonymous.
- Blockchain architecture: Knowledge of fundamental concepts, such as that a blockchain is a kind of distributed ledger, that it is tamper-resistant, and that it maintains a permanent record of transactions.
- Smart contracts: The initial application of blockchain was cryptocurrency, and the only type of transaction was the transfer of Bitcoins. The realization that blockchains could be used for other kinds of transactions was an important step in blockchain maturation. Understanding how to write smart contracts is seen as vital to blockchain growth and broad application.

Computer science undergraduates all learn programming languages and data structures. Cryptography is increasingly offered to undergraduates, and in fact is part of the Association for Computing Machinery's (ACM's) latest computing curriculum recommendations [194]. The ACM lists blockchain as an emerging area worthy of consideration in developing curricula. Computer science graduates, then, will likely possess knowledge in four of the five areas (all but smart contracts). Computer science departments can be expected to take the lead in developing a blockchain-capable workforce by incorporating blockchain concepts into their courses.

Writing a smart contract also requires mastering a programming language. One source claims the top 5 languages are Solidity, Rust, JavaScript, Vyper, and Yul [195]. These specialized languages are not commonly taught in undergraduate programming classes, where students learn Python, C++, or Java. It is doubtful that many of today's computer science graduates would be able to begin writing smart contracts immediately upon being hired. More significantly, writing a smart contract can require knowledge of the contract's subject area: real estate, property, copyright, etc. If law schools taught blockchain concepts as they relate to smart contracts, the workforce would have individuals capable of participating in teams to ensure contracts are not only automatable but legal. This same principle applies to any area in which a smart contract can be useful, such as manufacturing.

Some of the sources expect blockchain developers and operators to have other skills, including distributed systems, peer-to-peer networking, and web development. The first two would be useful in setting up blockchain networks and ensuring their smooth operation, thereby establishing a network that is sufficiently connected to minimize latency in finalizing transactions. Knowledge of web development would come into play when developing blockchain application front ends.

4.4. Marketplace and Supply Chain

4.4.1. Risks Posed to the Marketplace and Supply Chain

By nature, more-permissioned (public) blockchains are both highly decentralized and transparent. The hardware underlying the technology must necessarily be available to intended participants in the network, which is often the general public. In this way, blockchain may not be subject to the same supply chain risks affecting technologies like artificial intelligence or advanced manufacturing, which require the most advanced hardware to operate at maximum efficiency.

As noted throughout this chapter, blockchain can also be a solution to supply chain risks facing other products. The immutable nature of the information stored on the blockchain allows for a higher degree of certainty when tracking products through the supply chain [27]. Product information can be stored on the blockchain to track location or identify where in the supply chain a product could be tampered with or otherwise altered.

4.4.2. Risks to the National Security, including the Economic Security, of the United States

With respect to the national security of the United States, blockchain technology brings with it significant risks and benefits. For example, DHS has identified 16 critical infrastructures "whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[109] Many of these 16 critical infrastructure sectors—such as financial services, information technology, transportation, food and agriculture, healthcare, and energy—are highlighted in Section 4.3 as areas where blockchain solutions are rapidly advancing. As a result, blockchain holds the potential to make these critical infrastructure sectors more secure and resilient. At the same time, blockchain's use is accompanied by the risks associated with adopting it.

With respect to the aspects of U.S. national security specifically concerning economic issues, financial applications of blockchain are prone to several risks. One is the lack of consumer protections apparent in cryptocurrency as well as decentralized finance. The decentralized nature of such financial systems is attractive to many as it prevents a single point of failure. However, this same system also obscures accountability when failure does occur, often leaving investors vulnerable and lacking recourse for technical failures, financial catastrophes, or crime and other malfeasance [9].

Blockchain technology has enabled the creation of cryptocurrencies. Since cryptocurrencies provide a means of exchanging goods and services with currencies other than those issued by central banks, cryptocurrencies are competitors to the U.S. dollar and, as a result, pose risks to the dominance of the U.S. dollar. If the total amount of cryptocurrency transactions becomes sufficiently large, this alternative to fiat currencies could increase the risk of instability in financial markets and call into question the assumption that fiat currencies are

[109] https://www.cisa.gov/critical-infrastructure-sectors

the only safe store of value that is readily available for the exchange of goods and services. Limited transaction rates (the number of transactions per unit of time), asset volatility, and limited retail adoption are all constraining the growth of cryptocurrency for retail transactions. Continued advances in blockchain technology could help overcome some of these constraints and support the further growth and acceptance of cryptocurrencies.

The pseudonymous nature of cryptocurrencies can also enable illicit activities. It can enable hackers and others engaged in digital ransom attacks to avoid detection. One such example is the Colonial Pipeline attack [196]. In 2021, Colonial Pipeline reported to the Federal Bureau of Investigation (FBI) that its computer network was accessed by an organization named DarkSide and that it had received and paid a ransom demand for approximately 75 bitcoins. Law enforcement was able to track multiple transfers of bitcoin and identify that approximately 63.7 bitcoins, representing the proceeds of the victim's ransom payment, had been transferred to a specific address, for which the FBI had the "private key." The DOJ seized the 63.7 bitcoins, valued at approximately $2.3 million.[110]

Since their creation in 2008, the majority of cryptocurrencies have used proof-of-work consensus algorithms to add transactions to the ledger.[111] The proof-of-work algorithms require the solution of a computationally intensive puzzle before a participant can add transactions to the blockchain and, as a result, be paid for helping to maintain the blockchain (see Section 4.2.1.4). Many thousands of participants compete to be the first to solve the puzzle. The electricity consumed by attempting to solve the proof-of-work puzzles is substantial. Bitcoin mining in 2022 was estimated to consume 0.16% of global energy production, which can locally drive up local retail electricity costs.[112] According to one estimate, Bitcoin mining consumed 150 terawatt-hours of electricity in 2021, which is more than the country of Argentina used [197]. Mining of cryptocurrency poses risks to the climate due to the release of greenhouse gases when fossil fuels are used to generate electricity. It also poses risks to local economies through increases in the cost of electricity. Newer cryptocurrencies, sensitive to these issues, often use less resource-intensive approaches to mining, such as the proof-of-stake consensus mechanism recently adopted by Ethereum. Alternative system and protocol designs can also reduce energy consumption.[113]

Competition with other countries also influences national security, including economic security, risks to the United States. Other countries and geopolitical organizations are investigating blockchain technology. The main organizations implementing this technology are multinational, with a presence in the United States. The Chinese government, however, has issued an opinion that it should invest heavily in blockchain technology research, development, and application [198]. It concluded that blockchain will continue to grow throughout the 2020s, and that China should be ready to leverage blockchain's advantages in the application areas described in this chapter. Moreover, it proposes that China should develop its own blockchain technology and blockchain implementations. If successful, these implementations could be competitive with existing blockchain technology, thereby decreasing market share of U.S. companies with an international presence in the blockchain

[110] See https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside
[111] https://www.coinbase.com/learn/crypto-basics/what-is-proof-of-work-or-proof-of-stake
[112] https://cointelegraph.com/news/btc-energy-use-jumps-41-in-12-months-increasing-regulatory-risks
[113] https://www.coinbase.com/learn/crypto-basics/what-is-proof-of-work-or-proof-of-stake

market. Also, the Russian Federal Service for Intellectual Property (Rospatent) intends to use blockchain technology to help manage IP rights, and plans to have an implementation by 2024.[114]

4.4.3. Emerging Risks and Long-Term Trends in the Marketplace and Supply Chain

A blockchain is shared within a network of participants. The utility and, thus, the value of the information stored and exchanged in the blockchain will grow, on average, as the size of the network grows. As networks grow in size, its value grows and creates a barrier to competitors (a basic principle of economies of scale). The consortia developing open-source blockchain platforms are motivated, in large part, by the strategic and financial value of winning widespread adoption. The consortia are competing to grow the biggest, most valuable network. Premature consolidation or winnowing of competing blockchain consortia could dramatically limit the opportunity for novel and potentially transformative elements of blockchain technology to be realized.

4.5. Recommendations

In preparing this chapter on blockchain technology, several challenges with implications for the United States emerged. Here, we discuss these challenges and recommendations for addressing them. At a high level, these recommendations address the immature nature of blockchain in the development timeline and how the U.S. Federal Government can ensure that the technology develops in the service of U.S. values.

Challenge 1: The diverse application space for blockchain, coupled with the fact that the technology is still relatively new, means that there is a large degree of uncertainty over its future application. Regulations should help blockchain developers and companies ensure that their technology can provide value while mitigating harms and risks.

Recommendation 1: The U.S. Government should support the development of standards and promulgate regulations for blockchain technology that are inclusive of the diverse range of applications that currently exist and that consider potential future applications. It should ensure that these standards and regulations fully account for the varied range of potential risks and harms that blockchain technologies have already introduced and might continue to introduce. Following the lead of the relatively new DevSecOps approach to software development, the U.S. Government should consider security and privacy implications in all its standards and regulations [3]. The ISO documents in **Table 5** would be a good starting point. They provide PII standards and define terms.

The U.S. Government should also promote further study and foster innovation in next generation technologies that are designed to achieve the advantages of blockchain technology while avoiding fundamental weaknesses of blockchain design.

Challenge 2: The network effect of blockchain utility and value incentivizes the creation of proprietary architectures. The business models that underpin the development of blockchain platforms tend to disincentivize interoperability. Interoperability, however, increases the

[114] https://www.iam-media.com/article/the-future-here-what-the-digital-economy-programme-means-rospatent

chances that the best blockchain technologies provide the most value for consumers, investors, and businesses.

Recommendation 2: The U.S. Government should encourage and participate with the private sector in developing standards and security best practices for interoperability among the various open-source blockchain consortia. Some industry standards have already been developed in this regard, which can be used as a guide for further standards.

Challenge 3: Blockchain-enabled cryptocurrencies allow individuals to make transactions outside the authority of a central bank. Blockchain technology has accelerated a number of innovations in payments, such as transaction programmability and cheaper cross-border payments. These innovations could help improve traditional payment infrastructure operated by central banks and large financial institutions. However, more work is needed to assess whether these features would provide benefits while mitigating risks to consumers, to financial stability, and to other objectives.

Recommendation 3: In support of the Federal Reserve's ongoing work on a possible U.S. Central Bank Digital Currency (CBDC), the U.S. Government should continue to assess whether a U.S. CBDC issued would advance the Administration's policy objectives for a U.S. CBDC System.

This assessment should include further study for how blockchain-related innovations in payments could help support a potential U.S. CBDC, and also consider approaches other than blockchain technology. Security-related aspects of CBDCs, and the potential AML/CFT requirements needed for CBDCs, should be factored into the assessment. Finally, this assessment should include the security and propriety of the data generated and/or stored on a connected or interconnected DLT.

Challenge 4: The decentralized nature of many blockchain implementations, particularly permissionless or mostly permissionless, means that data can be recorded on a blockchain in many ways, ranging from humans using a keyboard to data received from automated sensors. Sensors may be crucial for supply chains that rely on blockchains, where the amount of information that must be recorded is too large and time-consuming to enter manually. This variety can decrease opportunities for standardization and increase the difficulty of ensuring the accuracy of data entry. Additionally, this decentralized infrastructure also opens these systems for security gaps – affecting both the blockchain as well as the data transferred and generated by the blockchain.

Recommendation 4: To ensure that blockchain technology is able to continue to grow, investments should be made such that networked devices are available and properly vetted for use in blockchain technology (see Section 4.3.1.2).

Challenge 5: There is no well-accepted model to calculate the costs and benefits of switching to blockchain. An organization whose current infrastructure supports company operations may have difficulty justifying a switch, even if the support is adequate but not optimal.

Recommendation 5: U.S. Government departments and agencies should identify opportunities for blockchain investments and to establish pathways to blockchain technology adoption, where the benefits of blockchain technology become concretely established.

Challenge 6: The open-source nature of blockchain technologies make them susceptible to the same cybersecurity risks in centralized technologies, such as Log4j, Heartbleed, and

Solar Winds, as well as additional vectors of intrusion, such as "Bridge" or alt-chain exploitation. Issues of fraud, trust, and illicit use are relevant to blockchain applications, as they are to any cyber system.

Recommendation 6: The U.S. Government should work closely to carry over recommendations from Federal open source software security initiatives, namely ensuring that blockchain programming languages are memory safe.

Challenge 7: The United States currently has a lack of qualified candidates to fill positions working on blockchain technologies given the traditional undergraduate curriculum in the United States. Specifically, there is a lack of potential candidates that have both issue area expertise (e.g., contract law) and the requisite technical skills.

Recommendation 7: The U.S. Government should work collaboratively with universities and other institutions to develop a pool of people with the needed issue area expertise and computational skill related to memory safe programming languages, data storage, quantum resistant cryptography, and network communication to create new data management systems (i.e., Blockchain technology).

Challenge 8: There may be undesirable consequences of widespread blockchain implementation. Currently, the best understood of these consequences is the considerable energy consumed by proof-of-work consensus models. Bitcoin miners have advocated shifting to using renewable energy sources, but as of April 2022 it was estimated that only 1% of Bitcoin mining used renewable energy [4; 5].

Recommendation 8: The U.S. Government should promote blockchain technologies that use models other than proof of work to add blocks to a blockchain. The U.S. Government should establish consensus model standards that do not rely on proof of work, and should fund academic sources and industries to develop a supportive open-source infrastructure.

Challenge 9: The possibility of implementing blockchain in mission-critical systems means human lives may depend on their expected behavior. Their widespread use in financial systems poses stability risks in markets.

Recommendation 9: The U.S. Government should establish vetting protocols and certification standards, similar to the FedRAMP authorization process.[115] The U.S. Government should require every system that uses blockchain technology to be certified to the degree appropriate for its intended purpose.

[115] https://www.fedramp.gov/

References

[1] Priyadarshini, Ishaani. "Introduction to Blockchain Technology." In *Cyber Security in Parallel and Distributed Computing: Concepts, Techniques, Applications and Case Studies.* Vol. 2017. Edited by Dac-Nhuong Le et al. First edition, 91–107. Hoboken NJ: John Wiley & Sons Inc; Scrivener Publishing LLC, 2019. https://doi.org/10.1002/9781119488330.ch6.

[2] White House. "The Administration's Roadmap to Mitigate Cryptocurrencies' Risks." News release. January 27, 2023. Accessed March, 2023. https://www.whitehouse.gov/nec/briefing-room/2023/01/27/the-administrations-roadmap-to-mitigate-cryptocurrencies-risks/.

[3] de Naray, Rachel K, Lee G Kennedy, Ryan R Wagner, and Steven P Wartik. "Cybersecurity and DoD System Development: A Survey of DoD Adoption of Best DevSecOps Practice." P-22749, Institute for Defense Analyses, September 1, 2021.

[4] Newar, Brian. "Earth Day Analysts Say Bitcoin Mining Is Naturally Gravitating to Green Energy." *Cointelegraph*, April 21, 2022. Accessed February 22, 2023. https://cointelegraph.com/news/this-earth-day-analysts-say-bitcoin-mining-is-naturally-gravitating-to-green-energy.

[5] Usman, Jerry. "A Shift to Renewables Will Optimize Bitcoin Mining." *Bitcoin Magazine - Bitcoin News, Articles and Expert Insights*, October 9, 2022. Accessed February 22, 2023. https://bitcoinmagazine.com/culture/renewables-will-optimize-bitcoin-mining.

[6] Zhang, Shijie, and Jong-Hyouk Lee. "Analysis of the Main Consensus Protocols of Blockchain." *ICT Express* 6, no. 2 (2020): 93–97. https://doi.org/10.1016/j.icte.2019.08.001.

[7] Buterin, Vitalik. "On Public and Private Blockchains." https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/.

[8] Yaga, Dylan, Karen Scarfone, Nik Roby, and Peter Mell. "Blockchain Technology Overview." Gaithersburg, MD, 2018. https://nvlpubs.nist.gov/nistpubs/ir/2018/nist.ir.8202.pdf.

[9] U.S. Government Accountability Office. "GAO-22-104625 - Blockchain: Emerging Technology Offers Benefits for Some Applications but Faces Challenges." 2022. https://www.gao.gov/assets/gao-22-104625.pdf.

[10] Wright, Craig S. "Bitcoin: A Peer-to-Peer Electronic Cash System." *SSRN Electronic Journal*, 2008. https://doi.org/10.2139/ssrn.3440802. https://bitcoin.org/bitcoin.pdf.

[11] Nieles, Michael, Kelley Dempsey, and Victoria Yan Pillitteri. "An Introduction to Information Security." NIST SP 800-12, NIST, Gaithersburg, MD, 2017. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf.

[12] United State Nuclear Regulatory Commission. "Introduction to Cryptography." https://www.nrc.gov/site-help/e-submittals/intro-crypt.html.

[13] IBM. "About IBM Food Trust." 2019. https://www.ibm.com/downloads/cas/8QABQBDR.

[14] Ethereum. "Proof-of-Stake (PoS) | Ethereum.Org." Accessed October 11, 2022. https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/.

[15] Platt, Moritz, Johannes Sedlmeir, Daniel Platt, Jiahua Xu, Paolo Tasca, Nikhil Vadgama, and Juan Ignacio Ibañez. "Energy Footprint of Blockchain Concensus Mchanisms Beyond Proof-of-Work." Accessed February 21, 2023. http://blockchain.cs.ucl.ac.uk/wp-content/uploads/2021/11/UCL_CBT_DPS_Q32021_updated-2.pdf.

[16] Office of Science and Technology Policy. "Climate and Energy Implications of Crypto-Assets in the United States." https://www.whitehouse.gov/wp-content/uploads/2022/09/09-2022-Crypto-Assets-and-Climate-Report.pdf.

[17] Ethereum. "The Merge." https://ethereum.org/en/upgrades/merge/.

[18] U.S. Department of the Treasury. "Crypto-Assets: Implications for Consumers, Investors, and Businesses." Washington D.C., 2022. https://home.treasury.gov/system/files/136/CryptoAsset_EO5.pdf.

[19] Executive Office of the President. "Policy Objectives for a U.S. Central Bank Digital Currency System." Executive Office of the President, 2022. https://www.whitehouse.gov/wp-content/uploads/2022/09/09-2022-Policy-Objectives-US-CBDC-System.pdf.

[20] Executive Office of the President. "Technical Evaluation for a U.S. Central Bank Digital Currency System." Executive Office of the President, Washington, D.C., 2022. https://www.whitehouse.gov/wp-content/uploads/2022/09/09-2022-Technical-Evaluation-US-CBDC-System.pdf.

[21] MediLedger. "The MediLedger Project." Accessed October 11, 2022. https://www.mediledger.com/.

[22] U.S. Department of Justice. "The Role of Law Enforcement in Detecting, Investigating, and Prosecuting Criminal Activity Related to Digital Assets." The Report of the Attorney General Pursuant to Section 5(b)iii of Executive Order 14067, Department of Justice (DOJ), 2022. https://www.justice.gov/media/1245466/dl?inline.

[23] Sharma, Rakesh. "Non-Fungible Token (NFT): What Is a Non-Fungible Token (NFT)?." https://www.investopedia.com/non-fungible-tokens-nft-5115211.

[24] Crenshaw, Caroline A. "Statement on DeFi Risks, Regulations, and Opportunities." https://www.sec.gov/news/statement/crenshaw-defi-20211109.

[25] Lu, Kevin. "A Dive into Smart Contracts and DeFi." *CoinMarketCap*, January 12, 2021. https://coinmarketcap.com/alexandria/article/a-dive-into-smart-contracts-and-defi.

[26] Wouda, Hugo Pieter, and Raymond Opdenakker. "Blockchain Technology in Commercial Real Estate Transactions." *Journal of Property Investment & Finance* 37, no. 6 (2019): 570–79. https://doi.org/10.1108/JPIF-06-2019-0085.

[27] Fefer, Rachel F. "Blockchain and International Trade." *Congressional Research Service*, 2019. https://sgp.fas.org/crs/row/IF10810.pdf.

[28] Lopez, Edwin. "Maersk, IBM to Shut down Blockchain Joint Venture TradeLens." Accessed February 21, 2023. https://www.supplychaindive.com/news/Maersk-IBM-shut-down-TradeLens/637580/.

[29] PYMNTS. "Walmart Puts Pricey Blockchain Food Tracking Platform on Ice." *PYMNTS.com*, December 19, 2022. Accessed February 21, 2023. https://www.pymnts.com/blockchain/2022/walmart-puts-pricey-blockchain-food-tracking-platform-on-ice/.

[30] U.S. Food and Drug Administration. “DSCSA Pilot Project Program.” *FDA*, May 22, 2019. Accessed October 12, 2022. https://www.fda.gov/drugs/drug-supply-chain-security-act-dscsa/dscsa-pilot-project-program.

[31] U.S. Food and Drug Administration. “FSMA Proposed Rule for Food Traceability.” *FDA*, January 12, 2021. Accessed October 12, 2022. https://www.fda.gov/food/food-safety-modernization-act-fsma/fsma-proposed-rule-food-traceability.

[32] Everledger. “Main Home - Everledger.” Accessed October 11, 2022. https://everledger.io/.

[33] Executive Office of the President. “Climate and Energy Implications of Crypto-Assets in the United States.” Executive Office of the President, 2022. https://www.whitehouse.gov/wp-content/uploads/2022/09/09-2022-Crypto-Assets-and-Climate-Report.pdf.

[34] Zyskind, Guy, Oz Nathan, and Alex Pentland. “Decentralizing Privacy: Using Blockchain to Protect Personal Data.” In *2015 IEEE Security and Privacy Workshops*, 180–84. IEEE, 2015.

[35] Executive Order on Ensuring Responsible Development of Digital Assets. EO 14067. Executive Office of the President. March 9, 2022. https://www.federalregister.gov/documents/2022/03/14/2022-05471/ensuring-responsible-development-of-digital-assets.

[36] Gupta, V. “A Brief History of Blockchain.” https://hbr.org/2017/02/a-brief-history-of-blockchain.

[37] Davis, Joshua. “The Crypto-Currency: Bitcoin and Its Mysterious Inventor.” *The New Yorker*, October 3, 2011. https://www.newyorker.com/magazine/2011/10/10/the-crypto-currency.

[38] Hyperledger Foundation. “Hyperledger Fabric – Hyperledger Foundation.” Accessed October 11, 2022. https://www.hyperledger.org/use/fabric.

[39] IBM. “What Is Hyperledger Fabric? | IBM.” Accessed October 11, 2022. https://www.ibm.com/topics/hyperledger.

[40] Amazon Web Services. “Amazon Managed Blockchain.” Accessed April, 2023. https://aws.amazon.com/managed-blockchain/.

[41] Oracle. “Oracle Blockchain.” Accessed October 11, 2022. https://www.oracle.com/blockchain/.

[42] Intel. “Intel® Blockscale™ ASIC.” Accessed October 11, 2022. https://www.intel.com/content/www/us/en/products/docs/blockchain/custom-asic-product-brief.html?wapkw=blockchain.

[43] Intel. “Intel Select Solutions for Blockchain: Hyperledger Fabric.” Accessed October 11, 2022. https://www.intel.co.uk/content/www/uk/en/products/solutions/select-solutions/cloud/blockchain-hyperledger-fabric-ver-2.html.

[44] Foley, Mary Jo. “Microsoft Is Shutting down Its Azure Blockchain Service.” *ZDNet*, May 12, 2021. Accessed October 11, 2022. https://www.zdnet.com/finance/blockchain/microsoft-is-shutting-down-its-azure-blockchain-service/.

[45] Schuster, Andreas. “SAP HANA Blockchain: Technical Overview.” Accessed May 11, 2023. https://blogs.sap.com/2018/08/28/sap-hana-blockchain-technical-overview/.

[46] Adams, Kathie. "Blockchain AI Market Size, Share, and Global Market Forecast to 2025." Accessed April, 2023. https://www.datasciencecentral.com/blockchain-technology-the-future-of-the-manufacturing-industry/.

[47] Anzalone, Robert. "IBM Blockchain Is Growing in the Food Industry During Covid-19." *Forbes*, June 4, 2020. https://www.forbes.com/sites/robertanzalone/2020/06/04/ibm-blockchain-technology-is-growing-in-the-food-industry-during-covid-19/?sh=243151c27f07.

[48] IBM. "IBM Food Trust - Blockchain for the World's Food Supply." Accessed October 11, 2022. https://www.ibm.com/blockchain/solutions/food-trust.

[49] Murphy, Mike. "Who Is Buying into IBM's Blockchain Dreams?" *Protocol*, March 9, 2020. https://www.protocol.com/ibm-blockchain-supply-produce-coffee.

[50] Meat+Poultry. "Cargill Implements Traceable Turkey Solution." *MEAT+POULTRY*, October 25, 2017. https://www.meatpoultry.com/articles/17337-cargill-implements-traceable-turkey-solution.

[51] Lang, Hannah. "Does the Cryptocurrency Crash Pose a Threat to the Financial System?" *Reuters Media*, May 11, 2022. Accessed July 24, 2022. https://www.reuters.com/business/finance/does-cryptocurrency-crash-pose-threat-financial-system-2022-05-11/.

[52] Reiff, Nathan. "How Much of All Money Is in Bitcoin?." https://www.investopedia.com/tech/how-much-worlds-money-bitcoin/.

[53] Securities and Exchange Commission. "Remarks Before the Aspen Security Forum." Accessed February 22, 2023. https://www.sec.gov/news/speech/gensler-aspen-security-forum-2021-08-03.

[54] Blockchain.com. "Blockchain.Com - the Most Trusted Crypto Company." Accessed October 11, 2022. https://www.blockchain.com/.

[55] Coinbase. "Coinbase - Buy and Sell Bitcoin, Ethereum, and More with Trust." Accessed October 11, 2022. https://www.coinbase.com/.

[56] Rodriguez, Gabriel. "8 Best Crypto Wallets of October 2022." https://money.com/best-crypto-wallets/.

[57] IBM. "Transforming Insurance Management with IBM Blockchain." 2018. https://www.ibm.com/downloads/cas/OMJRXZAL.

[58] Finextra. "JPMorgan Builds on Blockchain-Based Payment Network." *Finextra*, October 28, 2020. https://www.finextra.com/newsarticle/36836/jpmorgan-builds-on-blockchain-based-payment-network.

[59] Kumar, Ananya, Nitya Biyani, Stefan de Villiers, and Matt Goodman. "Central Bank Digital Currency Tracker." https://www.atlanticcouncil.org/cbdctracker/.

[60] Obey, Comfort. "European Central Bank Claims Blockchain Is Useless to CBDCs." https://ledgerdemain.com/2020/09/22/european-central-bank/.

[61] Privacy Technical Assistance Center. "The Lifelong Learner: How Blockchain Solutions Can Facilitate Data Transfer and Protect Personal Information for a Lifetime." Accessed April, 2023. https://tech.ed.gov/files/2021/02/blockchain-lifelong-learner.pdf.

[62] Department of Education. "The Privacy Implications of Self-Sovereign Identity in Education." Accessed April, 2023. https://tech.ed.gov/files/2021/02/privacy-implications-self-sovereign-identity-education.pdf.

[63] Sony Global Education team. "Sony Global Education's Educational Blockchain Website Launch."

https://web.archive.org/web/20220130075205/https:/www.sonyged.com/2017/12/14/news/blockchain-site-launch/.

[64] IBM. “Sony and Sony Global Education Develop a New System to Manage Students' Learning Data, Built on IBM Blockchain: New Cloud-Based Platform to Help Track and Manage Student Data to Improve Efficiencies in Education System.” News release. 2017. https://www.prnewswire.com/news-releases/sony-and-sony-global-education-develop-a-new-system-to-manage-students-learning-data-built-on-ibm-blockchain-300501707.html.

[65] American Council on Education. “The Education Blockchain Initiative: Final Report.” 2021. https://www.acenet.edu/Documents/Education-Blockchain-Initiative-Final-Report.pdf.

[66] U.S. Department of Education. “Blockchain in Education - Office of Educational Technology.” Accessed October 11, 2022. https://tech.ed.gov/blockchain/.

[67] Veris Foundation. “Veris Foundation.” Accessed April 25, 2022. verisfoundation.com.

[68] U.S. Energy Information Administration. “Electric Power Monthly - U.S. Energy Information Administration (EIA).” Accessed October 11, 2022. https://www.eia.gov/electricity/monthly/.

[69] Emergen Research. “Blockchain in Energy Market Top Players | Blockchain in Energy Industry Revenue by 2028.” https://www.emergenresearch.com/blog/top-7-companies-offering-blockchain-technology-in-energy-sector.

[70] Kimani, Alex. “5 Blockchain Startups Disrupting the Energy Sector.” March 4, 2021. https://oilprice.com/Energy/Energy-General/5-Blockchain-Startups-Disrupting-The-Energy-Sector.html.

[71] Ellsmoor, James. “Meet 5 Companies Spearheading Blockchain for Renewable Energy.” *Forbes*, April 27, 2019. https://www.forbes.com/sites/jamesellsmoor/2019/04/27/meet-5-companies-spearheading-blockchain-for-renewable-energy/?sh=25c8746ff2ae.

[72] Brooklyn Microgrid. “Brooklyn Microgrid | Community Powered Energy.” Accessed October 11, 2022. https://www.brooklyn.energy/.

[73] EnergyStartups. “Top 10 Blockchain Energy Startups.” Accessed October 11, 2022. https://www.energystartups.org/top/blockchain-energy/.

[74] COI Energy. “Home - COI Energy.” Accessed October 11, 2022. https://www.coienergy.com/.

[75] Wilkinson, Mark D., Michel Dumontier, IJsbrand Jan Aalbersberg, Gabrielle Appleton, Myles Axton, Arie Baak, and Niklas Blomberg et al. “The FAIR Guiding Principles for Scientific Data Management and Stewardship.” *Scientific Data* 3, no. 1 (2016): 1–9. https://doi.org/10.1038/sdata.2016.18. https://www.nature.com/articles/sdata201618.

[76] Zakari, Nazik, Muna Al-Razgan, Amani Alsaadi, Haya Alshareef, Heba Al saigh, Lamia Alashaikh, Mala Alharbi, Rana Alomar, and and Seham Alotaibi. “Blockchain Technology in the Pharmaceutical Industry: A Systematic Review.” *PeerJ Comput Sci* 8, e840 (2022). Accessed April, 2023. https://doi.org/10.7717/peerj-cs.840.

[77] Kamenivskyy, Yuriy, Abhinav Palisetti, Layal Hamze, and and Sara Saberi. “A Blockchain-Based Solution for COVID-19 Vaccine Distribution.” *IEEE Engineering Management Review* 50, no. 1 (2022): 43–53. Accessed February, 2023. https://doi.org/10.1109/EMR.2022.3145656.

[78] Schofield, Hannah, and Lavan Thasarathakumar. "Blockchain, COVID-19 and the Pharmaceutical Supply Chain." https://www.pharmexec.com/view/blockchain-covid-19-and-the-pharmaceutical-supply-chain.

[79] Jafri, Rabab, and Shikha Singh. *Blockchain Applications for Healthcare Informatics: Blockchain Applications for the Healthcare Sector: Uses Beyond Bitcoin*., 2022. Accessed March, 2023. https://doi.org/10.1016/B978-0-323-90615-9.00022-0.

[80] e-Estonia. "KSI Blockchain - E-Estonia." Accessed October 11, 2022. https://e-estonia.com/solutions/cyber-security/ksi-blockchain/.

[81] Guardtime. "Estonian EHealth | Health Care Blockchain." Accessed October 11, 2022. https://guardtime.com/blog/estonian-ehealth-partners-guardtime-blockchain-based-transparency.

[82] Hyperledger Foundation. "Case Study: Change Healthcare Using Hyperledger Fabric to Improve Claims Lifecycle Throughput and Transparency." 2019. https://www.hyperledger.org/wp-content/uploads/2019/06/Hyperledger_CaseStudy_ChangeHealthcare_Printable_6.19.pdf.

[83] Southey, Stewart. "Guardtime HSX - the Global Foundation for Health Data Integrity?." Accessed April, 2023. https://www.forbes.com/sites/stewartsouthey/2020/04/28/guardtime-hsxthe-global-foundation-for-health-data-integrity/?sh=68c5ded33929.

[84] CrunchBase.com. "Hashed Health." Accessed April, 2023. https://www.crunchbase.com/organization/hashed-health.

[85] Hashed Health. "Home - Hashed Health." Accessed October 11, 2022. https://hashedhealth.com/.

[86] CBSG Consortium. "CSBG Consortium - CBSG Consortium." Accessed October 11, 2022. https://cbsg.tbcasoft.com/.

[87] CBSG Consortium. "Historical Timeline - CBSG Consortium." Accessed October 11, 2022. https://cbsg.tbcasoft.com/historical-timeline/.

[88] Pe, Daniele, and Nicola Purrello. "Industry Voices—Blockchain Has Massive Potential for the Telecom Industry." https://www.fiercetelecom.com/telecom/industry-voices-blockchain-has-massive-potential-for-telecom-industry.

[89] Adib, Dalia. "Why Aren't Telecoms Blockchain Use Cases Moving Beyond the Lab? ITU Webinar - DLT Meet-Ups Episode #3: Telecoms Use Cases." October 14, 2020. https://www.itu.int/en/ITU-T/webinars/20201014/Documents/Dalia%20Adib_2020-10-14%20ITU%20DLT%20Why%20aren%27t%20telecoms%20use%20cases%20moving%20beyond%20the%20lab.pdf?csf=1&e=niYI7g.

[90] Deloitte. "Blockchain in Health and Life Insurance." Accessed April, 2023. https://www2.deloitte.com/us/en/pages/life-sciences-and-health-care/articles/blockchain-in-insurance.html.

[91] EY. "World's First Blockchain Platform for Marine Insurance Now in Commercial Use." Accessed April, 2023. https://www.ey.com/en_gl/news/2018/05/world-s-first-blockchain-platform-for-marine-insurance-now-in-co.

[92] Insurwave. "Client Success Stories." Accessed March, 2023. https://insurwave.com/client-success-stories/.

[93] Daley, Sam. "10 Blockchain Insurance Examples to Know." https://builtin.com/blockchain/blockchain-insurance-companies.

[94] McKinsey. “Blockchain in Insurance--Opportunity or Threat?,” 2016. https://www.mckinsey.com/~/media/mckinsey/industries/financial%20services/our%20insights/blockchain%20in%20insurance%20opportunity%20or%20threat/blockchain-in-insurance-opportunity-or-threat.ashx.

[95] Sapien Nation. “Homepage.” Accessed October 11, 2022. https://www.sapien.network/.

[96] Vevue. “Vevue: Next-Gen Social Media.” Accessed October 11, 2022. https://www.vevue.com/.

[97] Cloudflare. “What Is Ad Fraud? | Ad Click Fraud | Cloudflare.” Accessed October 11, 2022. https://www.cloudflare.com/learning/bots/what-is-ad-fraud/.

[98] Google Developers. “Search Engine Optimization (SEO) Starter Guide: The Basics | Google Search Central.” Accessed February 2, 2023. https://developers.google.com/search/docs/fundamentals/seo-starter-guide.

[99] Daley, Sam. “9 Ways Blockchain in Marketing and Advertising Is Getting Our Attention.” https://builtin.com/blockchain/blockchain-marketing-advertising-examples.

[100] Kubient. “Kubient – Kubient Home.” Accessed October 11, 2022. https://kubient.com/.

[101] Logiq Inc. “Logiq Acquires Rebel AI to Bring E-Commerce Growth to Brands and Agencies.” *Globe Newswire*, 2021. https://www.globenewswire.com/news-release/2021/03/30/2201539/0/en/Logiq-Acquires-Rebel-AI-to-Bring-E-commerce-Growth-to-Brands-and-Agencies.html.

[102] Ismail, Kaya. “How Blockchain Is Changing Advertising.” *CMSWire.com*, September 7, 2021. https://www.cmswire.com/digital-marketing/how-blockchain-is-changing-advertising/.

[103] RCS Global. “Blockchain for Traceability in Minerals and Metals Supply Chains: Opportunities and Challenges.” 2017. https://www.rcsglobal.com/wp-content/uploads/2018/09/ICMM-Blockchain-for-Traceability-in-Minerals-and-Metal-Supply-Chains.pdf.

[104] Thomasson, Emma. “Carrefour Says Blockchain Tracking Boosting Sales of Some Products.” *Reuters Media*, 2019. https://www.reuters.com/article/us-carrefour-blockchain/carrefour-says-blockchain-tracking-boosting-sales-of-some-products-idUSKCN1T42A5.

[105] Nestlé. “Nestlé Expands Blockchain to Zoégas Coffee Brand.” News release. 2020. https://www.nestle.com/media/news/nestle-blockchain-zoegas-coffee-brand.

[106] De Beers Group. “Tracr.” Accessed October 11, 2022. https://www.debeersgroup.com/sustainability-and-ethics/leading-ethical-practices-across-the-industry/tracr.

[107] Ikea. “Digital Experiments Explores How Technology Can Connect and Protect Us.” https://about.ikea.com/en/newsroom/2021/05/26/digital-experiments-explores-how-technology-can-connect-and-protect-us.

[108] Grey, Eva. “Cargo Theft: A Billion-Dollar Problem.” *Ship Technology*, July 30, 2017. https://www.ship-technology.com/analysis/featurecargo-theft-a-billion-dollar-problem-5882653/.

[109] DHL. “Blockchain in Logistics.” 2018. https://www.dhl.com/content/dam/dhl/global/core/documents/pdf/glo-core-blockchain-trend-report.pdf.

[110] DHL. "DHL and Accenture Unlock the Power of Blockchain in Logistics." https://www.dhl.com/global-en/home/press/press-archive/2018/dhl-and-accenture-unlock-the-power-of-blockchain-in-logistics.html.

[111] Musienko, Yuri. "Top Logistic Companies That Use Blockchain." *Merehead*, November 16, 2021. https://merehead.com/blog/top-logistic-companies-that-use-blockchain/.

[112] Maersk. "The TradeLens Platform." Accessed October 11, 2022. https://www.maersk.com/apa-tradelens.

[113] Known Traveller Digital Identity. "KTDI." Accessed October 11, 2022. https://ktdi.org/.

[114] World Economic Forum. *The Known Traveller: Unlocking the Potential of Digital Identity for Secure and Seamless Travel*. World Economic Forum: World Economic Forum, 2018. https://www3.weforum.org/docs/WEF_The_Known_Traveller_Digital_Identity_Concept.pdf.

[115] Artificial Lawyer. "AXA Scraps Fizzy Insurance Smart Contract…But Still Interested in the Tech." Accessed February 22, 2023. https://www.artificiallawyer.com/2020/10/08/axa-scraps-fizzy-insurance-smart-contract-but-still-interested-in-the-tech/.

[116] Rijmenam, Van. "5 Ways How Blockchain Will Change the Travel Industry." https://www.thedigitalspeaker.com/how-blockchain-changes-travel-industry/.

[117] Lesavre, Loïc, Priam Varin, and Dylan Yaga. "NISTIR 8301-Blockchain Networks: Token Design and Management Overview." *National Institute of Standards and Technology*, 2021. https://doi.org/10.6028/NIST.IR.8301. https://csrc.nist.gov/publications/detail/nistir/8301/final.

[118] National Energy Technology Laboratory. "Blockchain for Optimized Security and Energy Management (BLOSEM)." Accessed October 12, 2022. https://netl.doe.gov/BLOSEM.

[119] Maughan, Douglas. "Testimony of Douglas Maughan Before the Committee on Science, Space, and Technology Subcommittee on Oversight Subcommittee on Research and Technology." May 08, 2018. Accessed May 17, 2023. https://www.dhs.gov/news/2018/05/08/written-testimony-st-house-science-space-technology-subcommittee-oversight-and.

[120] European Blockchain Partnership. "What Is EBSI." Accessed October 11, 2022. https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/What+is+ebsi.

[121] König, Lukas, Yuliia Korobeinikova, Simon Tjoa, and Peter Kieseberg. "Comparing Blockchain Standards and Recommendations." *Future Internet* 12, no. 12 (2020): 222. https://doi.org/10.3390/fi12120222. https://www.mdpi.com/1999-5903/12/12/222.

[122] International Standards Organization. "ISO - ISO/TC 307 - Blockchain and Distributed Ledger Technologies." Accessed October 11, 2022. https://www.iso.org/committee/6266604/x/catalogue/p/1/u/0/w/0/d/0.

[123] International Standards Organization. "ISO - Deliverables." Accessed October 11, 2022. https://www.iso.org/deliverables-all.html.

[124] Institute of Electrical and Electronics Engineers. "Standards - IEEE Blockchain Initiative." Accessed October 11, 2022. https://blockchain.ieee.org/standards.

[125] Accredited Standards Committee, Inc. - Financial Industry Standards. “ASC X9 TR 54-2021 - Blockchain Risk Assessment Framework.” https://webstore.ansi.org/Standards/ASCX9/ASCX9TR542021?source=blog.

[126] Permissioned Distributed Ledger ETSI Industry Specification Group. “Permissioned Distributed Ledgers (PDL) Smart Contracts System Architecture and Functional Specification.” ETSI GR PDL 004 v1.1.1, 2021. https://www.etsi.org/deliver/etsi_gr/PDL/001_099/004/01.01.01_60/gr_PDL004v010101p.pdf.

[127] CEN-CENELEC. “CEN Technical Bodies - CEN/CLC/JTC 19.” Accessed October 11, 2022. https://standards.cencenelec.eu/dyn/www/f?p=205:7:0::::FSP_ORG_ID:2702172&cs=148F2B917E4B67BCFD6FE36CE0EA923AC.

[128] Enterprise Ethereum Alliance. “About - Enterprise Ethereum Alliance.” Accessed October 11, 2022. https://entethalliance.org/about/.

[129] Enterprise Ethereum Alliance. “Membership FAQs - Enterprise Ethereum Alliance.” Accessed October 11, 2022. https://entethalliance.org/faqs/.

[130] The Linux Foundation. “Linux Foundation Unites Industry Leaders to Advance Blockchain Technology.” https://web.archive.org/web/20170717193806/https:/www.linuxfoundation.org/news-media/announcements/2015/12/linux-foundation-unites-industry-leaders-advance-blockchain.

[131] Hyperledger Foundation. “Blockchain Technology Projects – Hyperledger Foundation.” Accessed October 11, 2022. https://www.hyperledger.org/use.

[132] Global Blockchain Business Council. “Global Blockchain Business Council: Advocating for Blockchain Technology.” Accessed October 11, 2022. https://gbbcouncil.org/.

[133] Information Services Group. “Blockchain Collaborative Consortium.” Accessed October 11, 2022. https://bccc.global/.

[134] Energy Blockchain Consortium. “About – Energy Blockchain Consortium.” Accessed October 11, 2022. https://energy-blockchain.org/about/.

[135] R3. “R3 | Enterprise Technology & Services Leader.” Accessed October 11, 2022. www.r3.com.

[136] Bonifii. “Home - Bonifii.” Accessed October 11, 2022. https://bonifii.com/.

[137] The Wall Street Blockchain Alliance. “WSBA.” Accessed October 11, 2022. https://www.wsba.co/.

[138] International Telecommunication Union. “ITU-T Work Programme: [2022-2024] [SG20] [Q2/20].” Accessed July 7, 2022. https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=17949.

[139] Grassi, Paul A, Michael E Garcia, and James L Fenton. “NIST Special Publication 800-63-3: Digital Identiry Guidelines.” Gaithersburg, MD, 2017. https://www.nist.gov/special-publication-800-63#:~:text=NIST%20has%20co%2Ddeveloped%20SP,for%20innovations%20on%20the%20horizon.

[140] The Better Identity Coalition. “Better Identity in America: A Blueprint for Policymakers.” July 2018.

https://static1.squarespace.com/static/5a7b7a8490bade8a77c07789/t/5b4fe83b1ae6cfa99e58a05d/1531963453495/Better_Identity_Coalition+Blueprint+-+July+2018.pdf.

[141] U.S. Congress. “H.R.4258 - 117th Congress (2021-2022): Improving Digital Identity Act of 2021.” https://www.congress.gov/bill/117th-congress/house-bill/4258.

[142] E-Government Act of 2002’. Public Law 107-347. U.S. Congress. December 17, 2002. Accessed October 11, 2022. https://www.govinfo.gov/content/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf.

[143] Xu, Li Da, Wu He, and Shancang Li. “Internet of Things in Industries: A Survey.” *IEEE Transactions on Industrial Informatics* 10, no. 4 (2014): 2233–43. https://doi.org/10.1109/tii.2014.2300753.

[144] Department of Commerce Internet Policy Task Force & Digital Economy Leadership Team. “Fostering the Advancement of the Internet of Things.” 2017. https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf.

[145] Prewett, Kyleen W, Gregory L Prescott, and Kirk Phillips. “Blockchain Adoption Is Inevitable—Barriers and Risks Remain.” *Journal of Corporate Accounting & Finance* 31, no. 2 (2020): 21–28. https://doi.org/10.1002/jcaf.22415.

[146] Microsoft. “Decentralized Identity.” 2018. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2DjfY.

[147] Finck, Michèle. *Blockchains and Data Protection in the European Union*. Max Planck Institute for Innovation & Competition Research Paper No. 18-01: European Data Protection Law Review, 2017. https://doi.org/10.2139/ssrn.3080322.

[148] Khan, Shafaq Naheed, Faiza Loukil, Chirine Ghedira-Guegan, Elhadj Benkhelifa, and Anoud Bani-Hani. “Blockchain Smart Contracts: Applications, Challenges, and Future Trends.” *Peer-to-Peer Networking and Applications* 14, no. 5 (2021): 2901–25. https://doi.org/10.1007/s12083-021-01127-0. https://link.springer.com/article/10.1007/s12083-021-01127-0.

[149] U.S. Department of the Treasury. “Illicit Finance Risk Assessment of Decentralized Finance.” https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf.

[150] Giancaspro, Mark. “Is a ‘Smart Contract’ Really a Smart Idea? Insights from a Legal Perspective.” *Computer Law & Security Review* 33, no. 6 (2017): 825–35. https://doi.org/10.1016/j.clsr.2017.05.007. https://www.sciencedirect.com/science/article/pii/S026736491730167X.

[151] Schatsky, David, Amanpreet Arora, and Aniket Dongre. “Blockchain, COVID-19 and the Pharmaceutical Supply Chain.” Deloitte, 2018. https://www2.deloitte.com/content/dam/insights/us/articles/4600_Blockchain-five-vectors/DI_Blockchain-five-vectors.pdf.

[152] Braucher, Robert. “Security Transfers by Fiduciaries.” *Minnesota Law Review*, 1958. https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=3205&context=mlr.

[153] National Conference of State Legislatures. “Blockchain 2021 Legislation.” Accessed October 11, 2022. https://www.ncsl.org/research/financial-services-and-commerce/blockchain-2021-legislation.aspx.

[154] Cybersecurity and Infrastructure Security Agency. “2021-2025 Strategic Technology Roadmap Overview.” February 2021. https://www.cisa.gov/sites/default/files/publications/040521_STRv3-FINAL_508.pdf.

[155] Securities and Exchange Commission. “Report of Investigation Pursuant to Section 21(A) Of the Securities Exchange Act of 1934: The DAO.” News release. July 25,

2017. Accessed October 11, 2022. https://www.sec.gov/litigation/investreport/34-81207.pdf.

[156] blockspot.io. “List of Cryptocurrency Exchanges.” Accessed October 11, 2022. https://blockspot.io/exchange/.

[157] Miller, Hannah. “Terra $45 Billion Face Plant Creates Crowd of Crypto Losers.” *Bloomberg*, May 13, 2022. Accessed February 22, 2023. https://www.bloomberg.com/news/articles/2022-05-14/terra-s-45-billion-face-plant-creates-a-crowd-of-crypto-losers?leadSource=uverify%20wall.

[158] President's Working Group on Financial Markets, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency. “Report on Stablecoins.” November 2021. https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf.

[159] “Justice Department Announces Report on Digital Assets and Launches Nationwide Network.” Accessed February 22, 2023. https://www.justice.gov/opa/pr/justice-department-announces-report-digital-assets-and-launches-nationwide-network.

[160] Board of Governors of the Federal Reserve System. “Money and Payments: The U.S. Dollar in the Age of Digital Transformation.” January 2022. https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf.

[161] Ethereum. “Intro to Ethereum.” https://ethereum.org/en/developers/docs/intro-to-ethereum/.

[162] Gürkaynak, Gönenç, İlay Yılmaz, Burak Yeşilaltay, and Berk Bengi. “Intellectual Property Law and Practice in the Blockchain Realm.” *Computer Law & Security Review* 34, no. 4 (2018): 847–62. https://doi.org/10.1016/j.clsr.2018.05.027. https://www.sciencedirect.com/science/article/pii/S0267364918302218.

[163] Dutta, Pankaj, Tsan-Ming Choi, Surabhi Somani, and Richa Butala. “Blockchain Technology in Supply Chain Operations: Applications, Challenges and Research Opportunities.” *Transportation research. Part E, Logistics and transportation review* 142 (2020): 102067. https://doi.org/10.1016/j.tre.2020.102067.

[164] Liu, Ye, Xiaoyuan Ma, Lei Shu, Gerhard Petrus Hancke, and Adnan M Abu-Mahfouz. “From Industry 4.0 to Agriculture 4.0: Current Status, Enabling Technologies, and Research Challenges.” *IEEE Transactions on Industrial Informatics* 17, no. 6 (2020): 4322–34. https://doi.org/10.1109/TII.2020.3003910.

[165] Pal, Amitangshu, and Krishna Kant. “Using Blockchain for Provenance and Traceability in Internet of Things-Integrated Food Logistics.” *Computer* 52, no. 12 (2019): 94–98. https://doi.org/10.1109/mc.2019.2942111.

[166] Institute of Electrical and Electronics Engineers. “Four Ways Blockchain Can Enhance Global Food Supply Chains.” *IEEE*, July 8, 2021. Accessed October 12, 2022. https://innovationatwork.ieee.org/four-ways-blockchain-can-enhance-global-food-supply-chains/.

[167] Croft, Genevieve K. “Blockchain Technology and Agriculture.” June 12, 2021. https://crsreports.congress.gov/product/pdf/IF/IF11829.

[168] National Oceanic and Atmospheric Administration. “Tackling Challenges of Global Seafood Traceability Programs.” Accessed October 12, 2022. https://www.fisheries.noaa.gov/feature-story/tackling-challenges-global-seafood-traceability-programs.

[169] Securities and Exchange Commission. “Framework for “Investment Contract” Analysis of Digital Assets.” April 3, 2019. https://www.sec.gov/files/dlt-framework.pdf.

[170] Gensler, Gary. “Prepared Remarks of Gary Gensler on Crypto Markets Penn Law Capital Markets Association Annual Conference.” Penn Law Capital Markets Association Annual Conference, Washington, DC, April 04, 2022. Accessed October 12, 2022. https://www.sec.gov/news/speech/gensler-remarks-crypto-markets-040422.

[171] DeLesDernier, J Matthew. “Self-Regulatory Organizations; BOX Exchange LLC; Notice of Filing of Amendment Nos. 2 and 3 and Order Granting Accelerated Approval of a Proposed Rule Change, as Modified by Amendment Nos. 2 and 3, to Adopt Rules Governing the Trading of Equity Securities on the Exchange Through a Facility of the Exchange Known as BSTX LLC: Release No. 34-94092; File No. SR-BOX-2021-06.” News release. January 27, 2022. Accessed October 12, 2022. https://www.sec.gov/rules/sro/box/2022/34-94092.pdf.

[172] 42 USC Ch. 163: Research and Development, Competition, and Innovation. U.S. Congress. February 22, 2023. Accessed February 22, 2023. https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title42-chapter163&saved=%7CNDI%3D%7CdHJlZXNvcnQ%3D%7CdHJ1ZQ%3D%3D%7C14821%7Ctrue%7Cprelim&edition=prelim.

[173] Scarfone, Karen, Murugiah Souppaya, Amanda Cody, and Angela Orebaugh. *Technical Guide to Information Security Testing and Assessment*. Gaithersburg, MD: National Institute of Standards and Technology, 2008. https://doi.org/10.6028/nist.sp.800-115. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf.

[174] Office of Management and Budget. “Circular No. A-130 to the Heads of Executive Departments and Agencies: Managing Information as a Strategic Resource.” n.d. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.

[175] Dang, Quynh H. “Secure Hash Standard.” Federal Information Processing Standards Publication Series FIPS PUB 180-4, NIST, August 2015.

[176] Barker, Elaine B, and John M Kelsey. “Recommendation for Random Number Generation Using Deterministic Random Bit Generators.” 2015. https://www.nist.gov/publications/recommendation-random-number-generation-using-deterministic-random-bit-generators-2.

[177] Howard, James P, and Maria E Vachino. “Blockchain Compliance with Federal Cryptographic Information-Processing Standards.” *IEEE Security & Privacy* 18, no. 1 (2020): 65–70. https://doi.org/10.1109/MSEC.2019.2944290.

[178] U.S. Department of the Treasury. “U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats.” https://home.treasury.gov/news/press-releases/jy0768.

[179] Funk, Jeffrey L, and David T Methe. “Market- and Committee-Based Mechanisms in the Creation and Diffusion of Global Industry Standards: The Case of Mobile Communication.” *Research Policy* 30, no. 4 (2001): 589–610. https://doi.org/10.1016/S0048-7333(00)00095-0. https://www.sciencedirect.com/science/article/pii/S0048733300000950.

[180] International Organization for Standardization. “ISO/TC 307 - Blockchain and Distributed Ledger Technologies.” https://www.iso.org/committee/6266604.html.

[181] International Organization for Standardization. “ISO 22739:2020 Blockchain and Distributed Ledger Technologies — Vocabulary.” https://www.iso.org/standard/73771.html.

[182] International Organization for Standardization. “Standards by ISO/TC 307 Blockchain and Distributed Ledger Technologies.” https://www.iso.org/committee/6266604/x/catalogue/p/0/u/1/w/0/d/0.

[183] Vogelsteller, Fabian, and Vitalik Buterin. “Ethereum Improvement Proposals: EIP-20: Token Standard.” https://eips.ethereum.org/EIPS/eip-20.

[184] Buterin, Vitalik. “Standardized Contract APIs.” https://github.com/ethereum/wiki/wiki/Standardized_Contract_APIs/499c882f3ec123537fc2fccd57eaa29e6032fe4a.

[185] Baylina, Jordi, Jacques Dafflon, and Thomas Shababi. “EIP-777: Token Standard.” https://eips.ethereum.org/EIPS/eip-777.

[186] Deshmukh, Sumedha, Oceane Boulais, and Tommy Koens. “Global Standards Mapping Initiative: An Overview of Blockchain Technical Standards.” World Economic Forum, October 2020. https://www3.weforum.org/docs/WEF_GSMI_Technical_Standards_2020.pdf.

[187] Myers, Louis. “United States Blockchain and Cryptocurrency Resources.” https://blogs.loc.gov/law/2020/10/united-states-blockchain-and-cryptocurrency-resources/.

[188] Small Business Innovation Research. “SBIR-STTR: America's Seed Fund.” Accessed October 12, 2022. https://www.sbir.gov/.

[189] Small Business Innovation Research. “NSF SBIR Phase I (2020).” Accessed October 12, 2022. https://www.sbir.gov/node/1654791.

[190] Columbia University. “How to Learn Blockchain (2022’s Guide to the Skills You Need) | Columbia Engineering Boot Camps.” Accessed October 12, 2022. https://bootcamp.cvn.columbia.edu/blog/blockchain-guide-to-skills/.

[191] Hiremotely. “6 Must-Have Blockchain Developer Skills (2022).” https://www.hiremotely.com/blog/blockchain-developer-skills.

[192] Sahu, Mayank. “Skills Needed to Become a Blockchain Developer.” *UpGrad*, September 29, 2022. Accessed October 12, 2022. https://www.upgrad.com/blog/skills-needed-to-become-blockchain-developer/.

[193] Sheldon, Robert. “6 Must-Have Blockchain Developer Skills.” *TechTarget*, October 20, 2021. Accessed October 12, 2022. https://www.techtarget.com/whatis/feature/6-must-have-blockchain-developer-skills.

[194] CC2020 Task Force. *Computing Curricula 2020*. New York, NY, USA: ACM, 2020. Accessed July 24, 2022. https://doi.org/10.1145/3467967. https://www.acm.org/binaries/content/assets/education/curricula-recommendations/cc2020.pdf.

[195] Sunday, Eze. “Top 5 Smart Contract Programming Languages for Blockchain.” https://blog.logrocket.com/smart-contract-programming-languages/.

[196] Schwirtz, Michael, and Nicole Perlroth. “DarkSide, Blamed for Gas Pipeline Attack, Says It Is Shutting down: The Hacking Group, Which the F.B.I. Has Said Was Responsible for the Ransomware Attack, Said It Had Received “Pressure” from the U.S.” *The New York Times*, 2021. https://www.nytimes.com/2021/05/14/business/darkside-pipeline-hack.html.

[197] Hinsdale, Jeremy. “Cryptocurrency’s Dirty Secret: Energy Consumption.” *Columbia Climate School*, May 4, 2022. https://news.climate.columbia.edu/2022/05/04/cryptocurrency-energy/#:~:text=But%20crypto%20has%20a%20dirty,of%20Argentina%2C%20population%2045%20million.

[198] Lianxinfa. “Guiding Opinions of the Office of the Central Network Security and Information Committee of the Ministry of Industry and Information Technology on Accelerating the Promotion of Blockchain Technology Application and Industrial Development.” https://www.miit.gov.cn/zwgk/zcwj/wjfb/rjy/art/2021/art_851f2059f13d41a8bba59c8dce9401a8.html.

Appendix L. Abbreviations

AAIS	American Association of Insurance Services
ACM	Association for Computing Machinery
AML	Anti-Money Laundering
ANS	American National Standards
ANSI	American National Standards Institute
API	Application programming Interface
ASIC	Application-Specific Integrated Circuit
BaaS	Blockchain-as-a-Service
BLOSEM	Blockchain for Optimized Security and Energy Management
CAFTA	Central American Free Trade Agreement
CBDC	Central Bank Digital Currency
CBP	U.S. Customs and Border Protection
CEN	European Committee for Standardization
CFT	Combating the Financing of Terrorism
CFTC	Commodity Futures Trading Commission
CISA	Cybersecurity and Infrastructure Security Agency
DAG	Directed Acyclic Graph
DeFi	Decentralized Finance
DHS	Department of Homeland Security
DLT	Distributed Ledger Technology
DOE	Department of Energy
DOJ	Department of Justice
EAR	Export Administration Regulations
EBP	European Blockchain Partnership
ECB	European Central Bank
EEA	Enterprise Ethereum Alliance
EIP	Ethereum Improvement Proposals
ESBI	European Blockchain Services Infrastructure
ETSI	European Telecommunications Standards Institute
FBI	Federal Bureau of Investigation
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Management Act
FITARA	Federal Information Technology Acquisition Reform Act
GBBC	Global Blockchain Business Council
GDPR	General Data Protection Regulation
ICO	Initial Coin Offering
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IP	Intellectual Property
ISO	International Organization for Standardization
IT	Information Technology
ITAR	International Traffic in Arms Regulations
ITU-T	ITU Telecommunication Standardization Sector
KYC	Know-Your-Customer
NAFTA	North American Free Trade Agreement

NFT	Non-Fungible Token
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration
NSF	National Science Foundation
OMB	Office of Management and Budget
OSTP	Office of Science and Technology Policy
PII	Personally Identifiable Information
SBIR	Small Business Innovation Research
SEC	Securities and Exchange Commission
STTR	Small Business Technology Transfer
UCC	Uniform Commercial Code

New and Advanced Materials

Chapter Contents

List of Tables

5. New and Advanced Materials

Summary

In the Consolidated Appropriations Act of 2021 (Public Law 116-260), Congress tasked the National Institute of Standards and Technology (NIST) to prepare a series of studies on critical and emerging technologies, including new and advanced materials (NAMs), and their impact on the U.S. economy. NIST is the lead author of this chapter. The Federal Trade Commission has reviewed this chapter in full to identify interactions with consumer protection and competition concerns. In accordance with the language of the Act, this chapter addresses:

- industry sectors that implement and promote the use of NAMs,
- public-private partnerships (PPPs) focused on promoting adoption of NAMs,
- industry-based bodies developing and issuing standards for NAMs,
- the status of mandatory and voluntary standards, both Federal and industry-based,
- Federal agencies with expertise and jurisdiction in industry sectors implementing NAMs,
- interagency activities relevant to NAMs, Federal regulations, guidelines, mandatory standards, voluntary standards, and other policies concerning NAMs implemented by Federal agencies and industry-based bodies,
- Federal resources that exist for consumers and small businesses to evaluate the use of NAMs,
- risks to NAMs supply chains and marketplace,
- NAMs-based risks to the national security, including economic security,[116] of the United States, and
- long-term trends in NAMs.

NAMs include a wide range of materials categories and applications and are relevant to most U.S. industries. They support critical technologies such as renewable energy and semiconductors and microelectronics. For the purposes of this chapter, NAMs are defined based on previously developed definitions as, "*materials that exhibit novel or enhanced properties and/or superior performance relative to other materials such that they are of interest for integration into one or more commercial products*." Advanced materials can include materials that exhibit lower cost or a wider range of part fabrication possibilities due to improved processing, synthesis, fabrication and manufacturing methods.

[116] The Consolidated Appropriations Act of 2021 refers to "economic and national security," and economic security is understood to be part of national security for the purposes of authorities such as the Consolidated Appropriations Act of 2021 and Section 232 of the Trade Expansion Act of 1962 (Public Law 87-794).

Industry Sectors and Public-Private Partnerships

The materials industry is very broad and is considered, for the purposes of this chapter, to include suppliers and manufacturers of NAMs as well as companies that produce computational tools for NAMs. In general, the industry sectors relevant to NAMs include mining, utilities, construction, manufacturing, retail trade, transportation and warehousing, information, professional and technical services, and healthcare. PPPs on NAMs include, among others, many of the Manufacturing USA institutes, the Medical Device Innovation Consortium (MDIC), the Nanotechnology Characterization Laboratory (NCL) of Frederick National Laboratory for Cancer Research, and the Commonwealth Center for Advanced Manufacturing (CCAM). Other consortia and partnerships that are not necessarily established as PPPs are also important to promoting the adoption and use of NAMs.

Industry-Based Standards

Materials standards can cover raw materials, materials being developed for a particular application, and materials in a final product. Standards organizations are generally interested in standardizing materials when they approach commercialization, though there is a growing trend toward developing standards earlier in the technology development process. Several industry-based organizations are involved in the development of standards and specifications for NAMs: the International Organization for Standardization (ISO), ASTM International, the Versailles Project on Advanced Materials and Standards (VAMAS), IEEE, and SAE International. In addition, the American National Standards Institute (ANSI) promotes and facilitates standards development. This process is ongoing at these organizations and others across NAMs categories.

Federal Standards and Regulations

The Department of Defense (DoD), Department of Energy (DOE), National Science Foundation (NSF), and NIST are key drivers of the NAMs ecosystem, supporting research and providing funding for the development and application of NAMs, including standards development. The Federal Aviation Administration (FAA), the Food and Drug Administration (FDA), and the Environmental Protection Agency (EPA) have the authority to regulate some applications of NAMs in their respective agency mission areas. The Bureau of Industry and Security (BIS) and Department of State (DOS) have authority to control the export of information and use of NAMs in accordance with U.S. laws and regulations. Agencies may develop their own NAMs standards for specialized applications, e.g., the National Aeronautics and Space Administration (NASA) has developed standards for its mission operations. Federal agency staff commonly participate in standards development processes for NAMs.

Interagency Interactions

The four main Federal initiatives focusing on interagency activities for NAMs are the Materials Genome Initiative (MGI), the National Nanotechnology Initiative (NNI), the

Manufacturing USA network, and the National Quantum Initiative (NQI). The MGI is focused on accelerating new materials development using computational tools along with experimentation. Among the goals of the NNI are to support research and development (R&D) of nanotechnology including nanomaterials, to promote commercialization of this research, to support the physical and cyber infrastructure required for nanotechnology R&D, to support education, workforce development, and lifelong learning, and to ensure that nanotechnology is developed responsibly. The Manufacturing USA network consists of 16 institutes, many of which are working with industries relevant to particular categories of NAMs, that receive funding from Federal, State, non-profit, and private sector sources. The NQI seeks to ensure continued U.S. leadership in quantum information science (QIS) and its technology applications using a whole-of-government approach. Other interagency collaborations include the Federal Interagency Materials Representatives (FIMaR) meetings, the Federal Consortium for Advanced Batteries (FCAB), the Critical Minerals Subcommittee (CMS) of the National Science and Technology Council (NSTC), and the Multi-Agency Tissue Engineering Sciences (MATES) group. Federal agencies also establish bilateral partnerships on NAMs or may partner with other Federal agencies plus industry or academia.

Federal Government Resources to Evaluate the Use of NAMs

In addition to direct funding that Federal agencies may provide to small businesses in the form of grants via the Small Business Innovation Research (SBIR) or Small Business Technology Transfer (STTR) programs, which may be used for NAMs development or for development or integration into products, the Federal Government also supports a variety of other resources that are specific to the NAMs industry. These resources include experimental user facilities, computational user facilities, centers, and online resources. NIST supports the Materials Resource Registry, which provides information on both government-hosted and non-government hosted resources. DOE owns or leases the National Laboratories, operated under contract for DOE, which include user facilities that provide advanced research tools to conduct simulation, fabrication, and characterization of materials. The NSF supports Materials Research Science and Engineering Centers (MRSECs) and the National Nanotechnology Coordinated Infrastructure (NNCI) user facilities at universities across the United States. The National Institutes of Health (NIH) has numerous grant mechanisms to support the use of nano- and biomaterials in new diagnostic and therapeutic interventions for multiple diseases.

Supply Chain Risks

Supply chain risks for NAMs lie at the intersection of the economic and technical aspects of the market. NAMs are often produced and used in small quantities, meaning that there is a small market and low business incentive for creating a supply or a stable supply chain. NAMs that are difficult to manufacture or that must be produced at high purities may have limited supply chains. The establishment and ongoing expansion of the Manufacturing USA network reflects Federal efforts to address these risks. Further, critical minerals are a key point of risk in many NAMs supply chains. Critical minerals are defined in the Energy Act of 2020[117] as any mineral, element, substance, or material designated as critical by the Secretary of Energy under section 7002(c) of that Act that is essential to the economic or national security of the United States whose supply chain is vulnerable to disruption, and which serves an essential function in the manufacturing of a product without which there would be significant consequences for the economic, or national security of the United States. The 2022 list of critical minerals published by the U.S. Geological Survey (USGS) includes 50 minerals, many of which are used in NAMs. NAMs supply chains are also complex, which can create a lack of understanding about the impacts of potential disruptions and are subject to potential holdups. Both these factors can lead to market risks.

National Security, Including Economic Security

As NAMs are developed and integrated into technologies across a wide spectrum of applications, ensuring a reliable supply chain of minerals used in NAMs is a key cybersecurity and national security concern. The extraction and processing of many critical minerals is geographically concentrated in U.S. competitor nations such as the People's Republic of China, which constitutes an acute national security risk. Reliance on critical minerals for high-demand and emerging technologies, such as renewable energy technologies needed to address global climate change, motivates R&D of NAMs that do not use critical minerals and can substitute the function of critical minerals in these technologies. The United States is not alone in its reliance on critical minerals. Ally and competitor nations are prioritizing and investing in NAMs development, which could pose a longer-term risk to the United States if materials resources become globally limited.

Long-Term Trends for the NAMs Ecosystem

Three areas where there is long-term potential for positive developments in the NAMs ecosystem are supply chain analysis, sustainability, and workforce development. The diversity of NAMs types and applications and their reliance on critical minerals often results in complex supply chains that are not fully understood by those participating in them. Greater understanding of supply chain complexity will benefit all members of the NAMs ecosystem. Similarly, incorporating sustainability principles and approaches into NAMs development will help to mitigate the impact of supply chain disruptions and provide greater market certainty. Finally, a skilled technical workforce with access to appropriately designed training courses and educational pathways is essential to NAMs development.

Recommendations

Challenge 1: The funding and support needs of the NAMs community vary widely.

[117] Public Law No. 116-260, Division Z–Energy Act of 2020. U.S. House of Representatives Committee on Science, Space, & Technology. 12/2020. https://www.congress.gov/bill/116th-congress/house-bill/133/text.

Recommendation 1: The U.S. Government should assess current funding and support mechanisms for NAMs development at relevant Federal agencies, including identification of existing mechanisms and evaluation of their effectiveness where possible. Consider the different scales at which NAMs development is occurring and identify where barriers exist. Consider whether fundamental research is being effectively translated into NAMs applications.

Challenge 2: Increased global investments in NAMs.

Recommendation 2: The U.S. Government should assess global investments and strategies related to NAMs and, where appropriate, disseminate the results to provide opportunities for increased international collaboration and U.S. leadership. Engage with international partners on standards development to bolster U.S. interests and work towards globally harmonized standards. Assess the effects of existing export control regulations on NAMs development and advancement.

Challenge 3: Many NAMs are based on critical minerals, raising supply chain and sustainability concerns.

Recommendation 3: The U.S. Government should continue to support research that identifies substitute materials, including substitutes for critical minerals, develops methods for the recovery of existing supplies of NAMs containing critical minerals, and develops approaches to enhance critical mineral supplies via improvements in production and processing. Incorporate life cycle approaches that include assessments of feedstocks, energy efficiency, and recyclability into NAMs development to proactively mitigate sustainability issues.

Challenge 4: The diversity of NAMs properties and applications means that their supply chains are complex and global, which creates barriers to their advancement and adoption.

Recommendation 4: The U.S. Government should continue Federal roadmapping efforts that provide the materials community with the information and tools needed to understand and make decisions about NAMs supply chains, including supply chain disruptions. Leverage the extensive expertise in the NAMs community in these efforts.

Challenge 5: The diversity of NAMs applications and the fundamental enabling nature of NAMs for a wide variety of technological advancements requires that the United States maintains leading-edge research infrastructure and a skilled Federal workforce to enable and enhance coordination among Federal agencies and sectors.

Recommendation 5: The U.S. Government should maintain core competencies at Federal agencies, including those directly supporting NAMs research and applications and those playing a more indirect role, to ensure that the U.S. Government maintains its critical role in NAMs development.

> ***Recommendation 5a:*** Ensure that the Federal Government continues to host leading-edge research infrastructure and instrumentation for NAMs characterization and synthesis, such as user facility instrumentation.
>
> ***Recommendation 5b:*** Ensure that Federal agencies maintain a skilled workforce by expanding efforts to train existing personnel and hire new personnel in relevant NAMs fields.

> ***Recommendation 5c:*** Use existing interagency mechanisms to ensure that agencies are coordinating their efforts effectively, including with the larger NAMs community. Continue to coordinate and provide infrastructure for pre-competitive engagement among industry, government, and academia on NAMs manufacturing. Delineate agency roles to provide clear pathways for NAMs community engagement with the Federal Government.

Challenge 6: The NAMs community needs best practices, standards, and guidance around NAMs, including for safe use, data, and cybersecurity.

Recommendation 6: The U.S. Government should provide leadership to the NAMs community by empowering the MGI and other high-level Federal initiatives to develop and disseminate NAMs best practices, standards, risk management, and guidance, including data and cybersecurity standards and protection of intellectual property rights to promote capital investment and further development.

5.1. Overview

5.1.1. Definition of "New and Advanced Materials"

"New and advanced materials" (NAMs) is a term with a very broad scope. In general, NAMs are highly diverse in terms of their properties and applications and are characterized by long development times—on the order of years to decades—between initial research and commercial use. The development of NAMs for any application includes qualification and certification of both the materials and the material manufacturing processes to meet commercial performance and regulatory requirements. The establishment of the qualification and certification pathways for NAMs will likely require modification of existing, or the development of new, standards and guidelines. For the purposes of this chapter, the term "new and advanced materials" is defined as:

> *materials that exhibit novel or enhanced properties and/or superior performance relative to other materials such that they are of interest for integration into one or more commercial products.*

This definition was developed with consideration of existing characterizations of NAMs. Featherstone and O'Sullivan [1] cite a NIST definition published in 2011 of "materials advances"—namely, "materials that have been developed to the point that unique functionalities have been identified and these materials now need to be made available in quantities large enough for innovators and manufacturers to test and validate in order to develop new products." In addition, Kennedy et al. [2] defined an "advanced material" as a "material that exhibits novel or enhanced properties *and* superior performance relative to other materials." Finally, the Technology Strategy Board describes NAMs as "materials designed for targeted properties" that "show novel or improved structural (strength, hardness, flexibility) and/or functional properties (electronic, magnetic, optical)" [1].

Among the many benefits and opportunities that they provide, NAMs can offer new capabilities or improve existing performance of products, enable advanced manufacturing,[118] and provide opportunities for more sustainable production and products. Given the broad scope of this chapter, the definition of NAMs includes materials that have either not previously been integrated into commercially available products or that are at a stage during which applications and full-scale manufacturing methods are areas of active R&D. Further, the definition includes completely novel materials, innovations on established materials, innovative composites that combine conventional materials, and biomaterials.[119] Liquids and molecules used in pharmaceuticals are not included in this review of the NAMs landscape.

NAMs are relevant to practically every industry that produces or relies on physical parts. They are essential to several technology areas of importance to U.S. national security as outlined by the Fast Track Action Subcommittee on Critical and Emerging Technologies of the National Science and Technology Council (NSTC). A recent update to its list of critical

[118] Advanced manufacturing is "[the] use of innovative technologies to create existing products and the creation of new products [that] can include production activities that depend on information, automation, computation, software, sensing, and networking." Advanced Manufacturing National Program Office.

[119] For the purposes of this chapter, "biomaterials" includes bio-derived and bio-inspired materials.

and emerging technologies included advanced engineering materials, as well as advanced manufacturing, including additive and sustainable manufacturing, biotechnology, quantum information technologies, renewable energy generation and storage, and semiconductors and microelectronics [4]. NAMs are a key factor supporting innovation in all these technology areas.

There are several approaches to classifying materials including classification based on selected properties such as physical, chemical, structural, etc. or classification based on use of the material. The categories presented in **Table 1** are intended to give the reader some appreciation for the scope covered by advanced materials through the inclusion of examples and are adapted from the groupings used by Scott et al. [5] with some modifications and additions.

Table 1. New and Advanced Materials Categories and Examples.

New and Advanced Material Category	Examples
Lightweight and Structural Materials	Aluminum alloys, magnesium alloys, ceramic matrix composites (CMCs), carbon-carbon composites (CCCs), metal matrix composites (MMCs), polymer composites, nanocomposites, syntactic foams
Electronic and Photonic Materials	Silicon, germanium, gallium arsenide, cadmium telluride, aluminum nitride, 2D semiconductors, graphene, wide bandgap semiconductors (gallium nitride, silicon carbide), optical fibers (e.g., ZBLAN), organic electronic materials (e.g., organic LEDs, organic photovoltaics), transparent conducting oxides, magnetic materials
Energy Storage and Conversion Materials	Perovskites, solid lithium-ion electrolytes, layered transition metal oxides, advanced cathode and anode materials, advanced permanent magnet materials
Polymers	Block copolymer, bottlebrush, vitrimer, biodegradable polymers
Catalysts	Metal-organic frameworks (MOFs), zeolites, various nanoparticles, 2D materials
Quantum Materials	High-temperature superconductors, high performance rare-earth-free magnets, topological insulators
Biomimetic Materials	Artificial nacre, engineered tissue replacements, bio-inspired adhesives,

	nanolattices, artificial silk, bioresorbable magnesium-based alloys
Soft Materials	Hydrogels, organogels, colloids
Sustainable Building Materials	Bamboo-derived wood products, low-carbon dioxide concrete
Reactive and Responsive Materials	Shape memory alloys, phase change materials, liquid crystals
Materials for Extreme Environments	Tantalum alloys, tungsten alloys, complex concentrated alloys, high-entropy alloys, high-entropy ceramics, diborides, carbides, nitrides, advanced brazing alloys, corrosion resistant coatings, thermal barrier layers
Other	Quantum-grade diamond, additive manufacturing feedstocks, advanced fibers and fabrics, metallic glasses, carbon nanotubes

5.1.2. Federal Prioritization of New and Advanced Materials

Over the last two decades, U.S. prioritization of NAMs to spur innovation and increase U.S. competitiveness in a global economy led to the establishment of four key Federal initiatives: (1) the NNI, which first received funding in fiscal year 2001, (2) the MGI, which was launched in 2011, (3) the Manufacturing USA network of PPPs, which was established in 2012, and (4) the NQI, which was established in 2018. Together, these investments have supported R&D, manufacturing, infrastructure, safety, and workforce development for NAMs industries and created extensive networks of research universities, National Laboratories, Federal agencies, non-profits, and businesses of all sizes. The NQI released a strategic overview in 2018 [6] and subsequently published seven additional strategic documents [7]. Both the NNI and MGI released updated strategic plans in 2021 [8; 9], and new Manufacturing USA institutes continue to be proposed, signaling the ongoing importance of NAMs industries at the Federal level [10]. In addition, the Federal programs and resources outlined in Section 5.3.7, including NSF MRSECs, demonstrate prioritization of NAMs.

Nanotechnology, the focus of the NNI, is closely connected to numerous industries that rely on nanomaterials for innovation and progress, such as the microelectronics industry, biomedical industry, and renewable energy industry. Most nanomaterials can be classified as NAMs, including graphene and other two-dimensional materials, carbon nanotubes, and numerous nanoparticles and nanocomposites made of both organic and inorganic materials.[120] The NNI seeks to support R&D of nanotechnology including nanomaterials; to promote commercialization of this research; to provide infrastructure that can support

[120] Not all nanomaterials meet the definition of "NAMs" as presented in this chapter: some types of glass that incorporate nanoparticles have been produced for hundreds of years, and some novel nanomaterials are not yet of interest for integration into commercial products.

nanotechnology research, development, and deployment; to engage the public and expand the nanotechnology workforce; and to ensure that nanotechnology is developed responsibly [9]. The NNI submits a supplement to the President's budget annually that summarizes programmatic activities and plans for the next fiscal year [11].

The MGI, in contrast, is not directed towards a specific class of NAMs, but instead aims "to accelerate the discovery, design, and deployment of new materials, at a fraction of the cost, by harnessing the power of data and computational tools in concert with experiment" [8]. This initiative involves investments in an interconnected materials innovation infrastructure (MII), which includes computational tools, experimental tools, digital data, and workforce development. The MGI is the culmination of thinking and efforts to accelerate materials discovery and insertion that began in the 1980s with advances in the use of computational tools and a "materials by design" concept that led to several efforts and initiatives including integrated computational materials engineering (ICME) [12]. High-performance computing, high-throughput experimentation, and materials data infrastructure are driving a transformation in how NAMs and processing methods for producing them are discovered and optimized. A 2018 publication estimated that the potential economic impact of an improved MII was between $123 billion and $270 billion per year [5].

The Manufacturing USA network of PPPs comprises 16 institutes spread around the country, many of which are focused on industries strongly connected to particular categories of NAMs [13]. These manufacturing institutes are supported by mixed investment from the Federal Government, State governments, non-governmental organizations, and private industry. They have a mission of "connecting people, ideas, and technology to solve advanced manufacturing challenges, enhance industrial competitiveness and economic growth, [and] strengthen our national security" [14]. Manufacturing technology, and particularly technology that enables scalable, cost-effective, reliable methods for materials processing and integration, is critical in determining the ultimate commercial success of individual NAMs. These manufacturing institutes will be discussed further in Section 5.3.1.

The NQI was established by the National Quantum Initiative Act of 2018 (NQIA; Public Law No: 115-368) and strives to enable transformational scientific, technological and industrial advancements in quantum information science (QIS) R&D [6]. The NQIA directed NSF and DOE to establish QIS R&D centers, and the 2022 NDAA directed DoD to establish additional centers; as a result, there are now 13 active QIS Centers [15]. In addition to these Centers, NSF and DOE are carrying out additional center-scale and programmatic work on QIS, including at the DOE National Laboratories [16].

5.2. Background

The Consolidated Appropriations Act of 2021 (Public Law 116-260) required that NIST prepare a series of studies on critical and emerging technologies, including NAMs, and their impact on the U.S. economy [17]. In accordance with the language of the Act, NIST asked the Science and Technology Policy Institute (STPI) to prepare a chapter addressing:

- Industry sectors that implement and promote the use of NAMs,
- PPPs focused on promoting adoption of NAMs,

- Industry-based bodies developing and issuing standards for NAMs,
- The status of mandatory and voluntary standards, both Federal and industry-based,
- Federal agencies with expertise and jurisdiction in industry sectors implementing NAMs,
- Interagency activities relevant to NAMs,
- Federal regulations, guidelines, mandatory standards, voluntary standards, and other policies concerning NAMs implemented by Federal agencies and industry-based bodies,
- Federal resources that exist for consumers and small businesses to evaluate the use of NAMs,
- Risks to NAMs supply chains and marketplace,
- NAMs-based risks to the national security, including economic security, of the United States, and
- Long-term trends in NAMs.

A definition of NAMs was developed for the purposes of this work. Broad materials categories were incorporated within this definition. Recent reports and scientific publications related to NAMs were reviewed along with responses to the public request for information (RFI) and conducted interviews with Federal employees and representatives of manufacturing institutes and standards development organizations. Given the breadth of types and uses for NAMs, this chapter provides a snapshot of the NAMs landscape in an effort to capture the salient issues around NAMs rather than an exhaustive summary of every NAM in development or use. It should also be that the Act refers to “economic and national security”. However, economic security is understood to be part of national security under authorities such as Section 232 of the Trade Expansion Act of 1962 (Public Law 87-794) [18].

5.3. Observations

This section presents information on how industry, Federal agencies, PPPs, standards development organizations, and other groups contribute to the development and application of NAMs. Regulations, standards, and Federal resources related to NAMs are also discussed. It should be noted that NAMs are relevant to several of the other chapter topics; Appendix N contains more information on how NAMs play a role in each of these technology areas.

5.3.1. Industry

5.3.1.1. NAMs in Industry[121]

Materials companies are motivated to discover and develop NAMs to meet current manufacturer needs and to stimulate innovation and markets for these materials.

[121] Economists classify industries as primary, secondary, tertiary, and quaternary: primary industry produces raw materials; secondary industry, also called the manufacturing industry, makes consumer goods or components of consumer goods and includes energy-producing companies; tertiary industry is the services industry; and quaternary industry provides information or knowledge services. Typically, the development and use of NAMs involves more than one of these classifications.

Computational software and tools development companies look to advance computational capabilities to realize the materials informatics and simulation infrastructure that is part of the MGI and other efforts. Manufacturers are open to using a NAM if it addresses known issues with current materials, improves performance in existing systems or desired performance in future systems, provides the possibility of the realization of new capabilities, allows efficient and effective integration into existing manufacturing and supply chain infrastructure, has the potential to improve supply chain reliability, and/or has a lower overall cost. For the purposes of this chapter, the NAMs industry is considered to include suppliers and manufacturers of NAMs; companies that produce modeling software for NAMs, including material and process modeling software and materials informatics software; and companies that produce manufacturing equipment.

5.3.1.2. Industry Sectors that Develop, Implement, and Promote the Use of NAMs

A wide range of industry sectors are involved in developing, implementing, and promoting the use of NAMs. **Table 2** indicates the industry sectors most highly relevant to NAMs and briefly describes their relevance. The descriptions provided do not comprehensively explain the relevance of the industry to NAMs but aim to illustrate how each sector contributes to the development, implementation, or promotion of NAMs.

Table 2. Industry Sectors Relevant to NAMs.

NAICS Code [19]	Sector	Description of relevance to NAMs
11	Agriculture, Forestry, Fishing, and Hunting	Inclusive of forestry, this sector provides the supply of wood products that serve as an input to sustainable building materials.
21	Mining	Provides the supply of raw materials on which the production of NAMs relies. NAMs also can be used to improve the equipment used in mining processes.
22	Utilities	Many power generation and distribution technologies rely on NAMs. Batteries and other energy storage technologies also involve NAMs.
23	Construction	Sustainable construction materials are NAMs.
31–33	Manufacturing	The production of NAMs relies on the manufacturing industry. NAMs are also an important component of advanced manufacturing processes (including additive manufacturing).
44–45	Retail Trade	Products of many types incorporate NAMs, including cars, electronics, and appliances.

NAICS Code [19]	Sector	Description of relevance to NAMs
48–49	Transportation and Warehousing	Transportation and warehousing are important in the NAMs supply chain. This sector also benefits from the implementation of NAMs into the infrastructure that supports it (e.g., advanced materials improve airplanes that are used to transport goods).
51	Information	Inclusive of communications companies and data processing services, this sector relies on NAMs as inputs to information technologies including computer chips.
54	Professional, Scientific, and Technical Services	Engineering and architecture firms may use NAMs, technical consultants may analyze and promote use of NAMs, and scientific researchers research NAMs.
56	Administrative Support and Waste Management and Remediation Services	Inclusive of hazardous waste collection and materials recovery facilities that may manage collection and disposal of NAMs.
61	Educational Services	Universities are key proponents of R&D and workforce development that is critical to the NAMs ecosystem.
62	Health Care and Social Assistance	Includes medical devices that are used in providing health care that may rely on NAMs, such as nano-devices, as well as nanoparticle- and biomaterial-based diagnostics and therapeutics.
81	Other Services (except Public Administration)	Inclusive of repair and maintenance industries, which may use NAMs.

American companies that have interests in or are involved with the production of NAMs are represented by various professional societies. The companies may be NAMs producers, utilities, and financial institutions, among others. Examples include NAATBatt International, which advocates for advancements in battery technologies in North America [20]; the U.S. Advanced Ceramics Association, which represents companies working on ceramics [21]; the Refractory Metals Association, which represents companies that produce refractory metals or alloys that are at least 50% refractory metals [22];[122] and the Semiconductor Industry Association [23].

In addition to companies focused on the design, development, and manufacturing of materials, companies providing computational software and tools are also important in the context of the NAMs industry. Materials informatics companies provide machine learning (ML) and data management and integration technologies to support product developers to accelerate development of chemicals and materials.

NAMs have been and are important to achieve needed performance in defense systems to provide essential capabilities. The defense industrial base involves several industry sectors. A non-exhaustive list of NAMs applications includes their use in the development of enhanced coatings, improved battery materials, components with advanced composites for aerospace, high temperature components for hypersonics, and joining techniques that can withstand extreme environments [24]. R&D efforts for defense systems aim to produce materials that can exceed the performance of existing materials and applications of materials in a variety of environments.

5.3.1.3. Public-Private Partnerships Focused on Promoting the Adoption and Use of NAMs

Collaboration across industry, academia, and government is essential to the development and adoption of NAMs. This section lists several collaborations including PPPs, other consortia and partnerships, and other organizations that involve industry, academia, and government participation to advance NAMs.[123]

PPPs

Several PPPs are focused on promoting the adoption and use of NAMs. Many of the Manufacturing USA institutes interface with materials in some capacity, as materials are deeply intertwined with and are a key component of manufacturing processes. The network of Manufacturing USA institutes is introduced and briefly discussed in Section 5.1.2. The institutes also interact with Federal agencies on NAMs issues of mutual interest, some examples of which are noted below. The institutes with strong interests in NAMs are listed here.

- Advanced Functional Fabrics of America (AFFOA) focuses on the textile industry, developing advanced fibers and smart fabrics that incorporate NAMs as well as sensing materials that can be considered NAMs [26].
- AIM Photonics works with other institutes, companies, and Federal agencies and entities to advance photonics manufacturing, involving advanced material processing techniques and incorporating existing materials into products in new ways [27].

[122] Refractory metals are tungsten, molybdenum, tantalum, columbium, chromium, rhenium, vanadium, boron, hafnium, cobalt, and rare earth metals (cerium, lanthanum, and yttrium).

[123] For the purposes of this chapter, collaborations that self-described as PPPs were identified as such. Broadly, a PPP is a collaboration between Federal and non-Federal partners to achieve specific goals in which the roles and responsibilities of each partner in the collaboration are mutually agreed upon Administrative Conference of the United States.

- America Makes focuses on additive manufacturing (AM), to which NAMs are highly relevant [28].
- The Advanced Robotics for Manufacturing (ARM) Institute works to advance robotics technologies, which involve NAMs; materials science companies are members of the institute [29].
- BioFabUSA advances tissue engineering and related medical products. The institute works to understand materials that will integrate in a tissue or an organ as well as materials amenable to interaction with cells [30].
- Bioindustrial Manufacturing and Design Ecosystem (BioMADE) aims to establish a sustainable, domestic bioindustrial manufacturing ecosystem, focusing on workforce and infrastructure but related in that materials development and integration are critical to that ecosystem [31].
- The Institute for Advanced Composites Manufacturing Innovation (IACMI) develops composite materials for implementation in applications including lightweight vehicles, renewable energy generation (e.g., wind blades for offshore turbines), and alternative fuel sources.[124] IACMI largely focuses on establishing low-cost, high-volume manufacturing of advanced composites including carbon fiber, other advanced reinforcements, and polymers [32].
- Lightweight Innovations for Tomorrow (LIFT) focuses on developing novel and innovative lightweight materials [33].
- NextFlex develops flexible electronics, which incorporate NAMs and advanced material processing techniques [34].
- PowerAmerica researches advanced semiconductor components involving NAMs [35].
- Reducing Embodied-energy and Decreasing Emissions (REMADE) focuses on reducing emissions in the manufacture of materials, and conducts work with metals, fibers, polymers, and e-waste. Partners across all industry sectors have interests in high-quality and high-purity materials. The design and development of NAMs is critical to enabling sustainable manufacturing and the circular economy [36].

The National Center for Defense Manufacturing and Machining maintains a team of nearly 200 partners across government, academia, and industry to ensure the U.S. remains globally competitive by advancing manufacturing technologies [37]. It manages five entities: America Makes, a Manufacturing USA institute described above; the Advanced Manufacturing Innovation and Integration Center, which accelerates adoption of manufacturing technologies; the Advanced Manufacturing and Applied Research Innovation Institute, which advances manufacturing technologies; the Advanced Manufacturing Intelligence Platform, a testbed for developing a digital AM supply chain for the U.S. Army and DoD contractors; and the V4 Institute, a product and service accelerator.

[124] Some work conducted by IACMI is relevant to DoD, DOE, NASA, and other agencies. Input from the Joint Defense Manufacturing Technology Panel helps to inform some of this work. See: https://www.dodmantech.mil/JDMTP/

In addition, the MDIC was established in 2011 by the FDA's Center for Devices and Radiological Health (CDRH) and Medical Alley Association, formerly known as LifeScience Alley, Inc. [38]. The organization is focused on regulatory science, promoting improvements to medical care and devices by working across industry and FDA. Regulatory science involves tools, methods, standards, and applied science, to which NAMs and advanced manufacturing are relevant.

The NCL of the Frederick National Laboratory for Cancer Research, which is managed by the National Cancer Institute (one of the NIH), is "a national resource and knowledge base for all cancer researchers to facilitate characterization of nanotechnologies intended for cancer therapies and diagnostics" [39]. The laboratory conducts pre-clinical efficacy and toxicity testing of nanoparticles intended for use in treating or diagnosing cancer. The laboratory is also an informational resource that can help researchers develop methods and optimize or reformulate their nanotechnology.

The Commonwealth Center for Advanced Manufacturing (CCAM) was founded in 2011 under a PPP to serve as an applied research center that convenes universities and companies [40]. A member of America Makes, CCAM enables public-private collaboration to solve advanced manufacturing challenges—including those related to NAMs.

Other consortia and partnerships

Other consortia and partnerships that are not necessarily established as PPPs are also important to promoting the adoption and use of NAMs.

The Materials Project at Lawrence Berkeley National Laboratory (LBNL), supported primarily by programs through the Department of Energy's (DOE) Office of Science, leverages funding from DOE and NSF to support collaboration with other research facilities and with industry [41]. The focus of research is the development of a database of materials properties to improve material design and accelerate innovation in materials research [42].

DOE's Energy Materials Network (EMN) is a network of consortia that aims to address challenges in the design and development of materials that can enable innovative solutions related to energy applications. Each consortium focuses on unique types of materials or applications; overall, the EMN works to accelerate the development and application of high-performance materials, including both functional materials and structural materials [43].

Beginning in 2010, DOE established five Innovation Hubs, of which four are focused on topics involving development of NAMs [44]. These Energy Innovation Hubs include engagement from the private sector as well as academia and aim to facilitate key research that is needed to help innovate in their respective focus areas and transition discoveries into commercial products. The five DOE Innovation Hubs that concern NAMs are:

- Liquid Sunlight Alliance [45] and Center for Hybrid Approaches in Solar Energy to Liquid Fuels [46], both of which study methods of generating fuels from sunlight
- Joint Center for Energy Storage Research, which studies future battery technologies [47]
- Critical Materials Institute, which seeks to accelerate innovative science and technological solutions to develop resilient and secure supply chains for rare earth

metal elements and other critical materials that are essential for clean energy technologies [48]

- National Alliance for Water Innovation, which studies desalination and water treatment technologies [49]

These centers interact with small and large businesses through affiliation and partnership programs that allow commercial entities to engage directly with researchers and in some cases participate in research.

The Quantum Economic Development Consortium (QED-C) was established with support from NIST in response to the 2018 NQI strategic overview and includes partners from industry, academia, the non-profit sector, and government [50]. The goals of the QED-C include identifying high impact use cases and applications for quantum-based technologies; identifying gaps in enabling technologies, standards and performance metrics, and workforce that need to be addressed advance QIS applications; and working with stakeholders to fill these gaps [51].

The Hypersonics Advanced Manufacturing Technology Center (HAMTC) at Purdue University is another example of an effort that convenes large companies, small businesses, and academic researchers to advance materials and manufacturing, providing opportunities for collaboration and resources such as testing capabilities at the facility [52].

Facilities focused on materials science such as those at Oak Ridge National Laboratory (ORNL) also illustrate the potential for consortia and partnerships to advance NAMs R&D that may lead to application. For example, ORNL's Manufacturing Demonstration Facility (MDF), National Transportation Research Center (NTRC), and Carbon Fiber Technology Facility (CFTF) provide resources that enable materials and manufacturing analysis and simulation, among other R&D [53]. Additional information about these user facilities and related resources is provided in Section 5.3.7.

Consortia focused on NAMs-related data are also making important contributions to NAMs adoption and use. The Open Databases Integration for Materials Design (OPTIMADE) consortium created an "application programming interface (API) to make materials databases accessible and interoperable" [54]. The consortium is open to all contributions and is working to develop a specification that enables more efficient and effective material design processes by making materials databases interoperable[125] [55]. The Metallic Materials Properties Development and Standardization (MMPDS) Handbook, developed through coordination between industry and government steering groups, also serves as an important reference for the commercial and military aerospace industries, providing design-pedigree data (material allowables) for metallic materials and joints [56]. Volume 2 of the MMPDS, focused on process-intensive material technologies, is under development [57; 58]. The Composite Materials Handbook-17 (CMH-17), administered by the CMH-17 Organization, reflects the efforts of Coordination Groups that focus on polymer matrix composites, CMCs, and MMCs. CMH-17 coordinates with other relevant bodies such as SAE International's polymer matrix composites committee (committee P-17) and the National Center for Advanced Materials Performance (NCAMP) at Wichita State University [59]. NCAMP

[125] OPTIMADE is not a general materials database, but is working to broaden the accessibility and interoperability of materials databases.

collaborates with its industry partners and FAA to qualify material systems and maintain a publicly-available materials database [60].

Other organizations that have industry, academia, and government participation to advance NAMs

In addition to the previously described PPPs, consortia, and partnerships, other organizations also have a role in coordinating or enabling collaboration across industry, academia, and government. For example, professional materials societies such as the Minerals, Metals & Materials Society (TMS) [61]; the American Institute of Chemical Engineers (AIChE) [62]; the American Chemical Society (ACS) [63]; the American Ceramics Society (ACerS) [64]; the American Physical Society (APS) [65]; and the Materials Research Society (MRS) [66] bring together materials researchers, scientists, and engineers to support collaboration and professional development in each respective field. ASM International (formerly the American Society for Metals) [67] has a similar role to these organizations, in addition to its work to develop products that enable the use of NAMs, such as ASM Handbooks and the ASM Data Ecosystem that was launched in 2022 [68]. The National Academies of Sciences, Engineering, and Medicine's (NASEM's) National Materials and Manufacturing Board provides technical and policy analyses on materials and manufacturing [69]. While not an exhaustive list of organizations, it exemplifies a limited number of the more than 100 U.S. or global associations that are directly related to materials and manufacturing or have elements that are strongly focused on materials or manufacturing.

Industry associations such as the United States Council for Automotive Research, American Institute of Architects, and National Defense Industrial Association, though not specific to NAMs, also serve as resources to professionals in each respective field that involves NAMs in some capacity. The U.S. Chamber of Commerce Technology Engagement Center (C_TEC) also plays a role in promoting the importance of technology in general to the economy [70].

Standards, which are essential for the quality of NAMs, may take months to years to develop, and therefore ensuring that the standards development process is complementary to NAMs development timelines is important. Standards development organizations coordinate industry and government entities in support of the advancement and implementation of NAMs by bringing together members from industry and academia with Federal agencies on committees. Information about the leading industry-based bodies that contribute to standards development is provided in the following section.

5.3.1.4. Industry-Based Bodies that Develop Mandatory or Voluntary Standards for NAMs

Materials standards can cover raw materials, feedstock materials, materials that are "in-process," meaning that the material will undergo further processing for use in the final product, and the materials in the final product. As such, several private sector organizations are involved in the development of standards and specifications for NAMs. These standards will evolve as the materials and material forms (e.g., plate, sheet, bar) are developed for and used in applications. Federal agency staff can participate in the development of these voluntary standards, as described in OMB Circular A-119 [71]. Private sector-developed voluntary standards can be incorporated into regulation, making them mandatory. The following list describes noteworthy organizations involved in standards development or the coordination of standards development related to NAMs in the United States:

- The ISO is an independent international organization with a membership of 165 national standards bodies that develops voluntary consensus standards for global markets. Standards can be searched online [72].
- The American National Standards Institute (ANSI) is a non-profit organization that administers and coordinates U.S. voluntary standards and conformity assessment, serving as representative to the ISO for the United States. ANSI oversees standards activities in the United States and coordinates U.S. participation in ISO's international activities through ANSI-accredited U.S. Technical Advisory Groups (TAGs).
    - ANSI does not develop standards itself but provides a framework for standards development and ensures integrity in standards development.
    - The organization coordinates member companies' positions regarding standards and publishes documents publicly on standards activities [73].
- ASTM International (formerly the American Society for Testing and Materials) develops voluntary consensus standards for a broad range of industries for global markets. Standards and a brief scope are available online [74].
- The American Society of Mechanical Engineers (ASME) is a professional association that engages in standards development, including those related to materials. In many cases, ASTM standards are the foundation for ASME standards. Titles and brief descriptions of standards are available online [75].
- The Versailles Project on Advanced Materials and Standards (VAMAS) was founded in 1982 by the G7 nations and the European Commission.[126] The purpose of VAMAS is to "promote world trade by innovation and adoption of advanced materials through international collaborations that provide the technical basis for harmonization of measurement methods, leading to best practices and standards" [77].
- The American Welding Society (AWS) develops standards related to joining of materials and inspection of joined materials at joint. Information about standards is available online [78].
- The American Institute of Aeronautics and Astronautics (AIAA) is accredited by ANSI and publishes national aerospace standards, recommended practices, and guides. AIAA also administers two space-related ISO subcommittees. Information on AIAA standards is available online [79].
- IEEE (formerly the Institute of Electrical and Electronics Engineers) is a professional association for engineers that engages in standards development for a variety of

[126] The VAMAS steering committee is currently composed of representatives from Australia, Brazil, Canada, the People's Republic of China, Chinese Taipei, France, Germany, India, Italy, Japan, Republic of Korea, Mexico, South Africa, the United Kingdom, and the United States Versailles Project on Advanced Materials and Standards Versailles Project on Advanced Materials and Standards (VAMAS).

industries, including those to which NAMs are relevant. Titles and brief descriptions of standards are available online [80].

- SAE International (formerly the Society of Automotive Engineers and now concerned with mobility in general) is a professional association for engineers that engages in standards development, contributing to the development of standards for the automotive, aerospace, and commercial vehicle industries. Lists of recently published standards and standards under development are available online [81].
- SEMI is an industry association of companies involved in electronics manufacturing and design supply chain [65]. Their Electronic Materials Group focuses on the design and manufacturing of electronic materials, including semiconductors, and is involved in industry advocacy and providing voluntary technical standards for these materials [82].
- Several organizations have a focus on advancing the field of soft matter, such as the American Physical Society's (APS) Division on Soft Matter [83].

5.3.1.5. Status of Industry-Based Mandatory or Voluntary Standards

Standards development work is constantly ongoing, and each standards organization may have many TAGs or committees, each of which may be tasked with handling multiple standards at a given time. Given the breadth of ongoing standards development relevant to NAMs, this section provides an overview of current efforts at ISO as a snapshot of current efforts. Most standards development organizations also have a schedule for updating their standards. As the U.S. representative to ISO, ANSI TAGs contribute to the efforts of ISO's Technical Committees (TCs), which develop standards relevant to a wide range of NAMs. Table 3 provides an overview of ongoing standards development work by the ISO TCs on NAMs and NAM-related areas. The table is not exhaustive but is intended to provide a snapshot of current areas at ISO where NAMs standard development is active. The remainder of this section describes processes by which standards organizations develop mandatory and voluntary standards and presents a landscape view of current standards work on NAMs. Additional information on standards and guidelines can be found in Sections 5.3.5 and 5.3.6.

Table 3. ISO Technical Committees (TCs) with NAMs-Relevant Standards in Progress.[127]

ISO Technical Committee	Example Areas with Standards under Development
TC 2 Fasteners	Reference standards; Fasteners with metric external thread; Surface coatings
TC 6 Paper, board and pulps	Cellulose nanomaterial optical properties
TC 20 Aircraft and space vehicles	Surface treatment of hardenable stainless steel parts
TC 22 Road vehicles	Brake lining friction materials; Electrically-propelled vehicles

[127] A searchable list of TCs is available at https://www.iso.org/standards-catalogue/browse-by-tc.html.

ISO Technical Committee	Example Areas with Standards under Development
TC 24 Particle characterization including sieving	Reference materials for particle size measurement; Methods for zeta potential determination – Streaming potential and streaming current methods for porous materials
TC 33 Refractories	Chemical analysis of refractory material glass and glazes; Testing of ceramic raw and basic materials
TC 35 Paints and varnishes	Evaluation of degradation of coatings
TC 37 Textiles	Manmade fiber – Determination of burning behavior
TC 44 Welding and allied processes	Soldering materials
TC 61 Plastics	Thermoplastic materials; Biodegradability
TC 71 Concrete, reinforced concrete and pre-stressed concrete	Fiber-reinforced polymer (FRP) reinforcement for concrete structures
TC 79 Light metals and their alloys	Magnesium and alloys of cast or wrought magnesium; Titanium and titanium alloys
TC 85 Nuclear energy, nuclear technologies, and radiological protection	Neutron radiation protection shielding
TC 106 Dentistry	Filling, restorative materials, prosthodontic materials, implants, CAD/CAM systems
TC 119 Powder metallurgy	Hot isostatic pressing
TC 150 Implants for surgery	Metallic minerals
TC 164 Mechanical testing of metals	Ductility testing; Hardness testing
TC 171 Optics and photonics	Optical materials and components
TC 201 Surface chemical analysis	Surface chemical analysis of nanoscale heavy metal oxide thin films
TC 209 Cleanrooms and associated controlled environments	Classification of air cleanliness; Cleanroom performance
TC 229 Nanotechnologies	Performance evaluation of nanosuspensions; Silica nanomaterials; Chemical characterization of graphene; Physicochemical characterization of liposomes
TC 261 Additive manufacturing	Feedstock materials; Use of metallic materials

ISO Technical Committee	Example Areas with Standards under Development
TC 298 Rare earth	Rare earth sustainability; Recycling of rare earth elements; Determination of rare earth content
TC 333 Lithium	Lithium sustainability across the value chain; Lithium carbonate
TC 334 Reference materials	Good practice in using reference materials; Guidance for the production of reference materials

The standards bodies and development organizations described previously have processes in place to review, revise, and develop new standards to meet members' needs. Several organizations are accredited by the ANSI. Standards developers are accredited by ANSI if they meet ANSI's requirements "… for openness, balance, consensus, and due process and adhere to ANSI's neutral oversight, assuring that all interested parties have an opportunity to participate in a standard's development" [73].

Standards organizations are generally interested in standardizing materials when they approach commercialization, though there is a growing trend toward developing standards earlier in the technology development process (i.e., at pre-competitive or pre-commercial stages). Through coordinating with subject matter experts and companies, standards development organizations work to draft, develop, and reach consensus around issues and to determine which standards are required or would be beneficial. Standards may include specifications, practices, test methods, or other guidelines; materials-related standards are relevant to all these categories. Most standards organizations have three tiers of documents—standards/specifications, best practices, and technical/information reports—and this tiered system is helpful in addressing new and evolving technologies. Standards development by these organizations is conducted in a manner consistent with best antitrust practices to avoid abuses of the process which, for example, could lead one or more industry participants to gain an unfair competitive advantage over other participants.

5.3.1.6. Description of the Ways Entities Develop, Implement, and Promote the Use of NAMs

Government managers and researchers, university researchers, and personnel from industry sector entities participate in PPPs and other collaborations, industry associations and professional societies, standards development organizations, and government-sponsored workshops—each of which play a role in developing, implementing, and promoting the use of NAMs.

Minimal or determined acceptable risk and access to funding are foundational to the broader use and commercialization of NAMs. Industry uses these technologies when it can realize profit or improve competitiveness; the government can decrease barriers to entry and risk through establishing effective policy and regulation, and supporting research and standardization, thereby increasing economic benefit. While companies across many industrial sectors are involved with the use of materials, Manufacturing USA institutes are particularly important in promoting the adoption of NAMs, as several are focused specifically on advancing a particular subset of relevant materials. Section 5.3.1. briefly describes the work of these Manufacturing USA institutes. The following list provides additional context and information about the activities of select institutes:

- IACMI is working with Dassault Systems to advance and implement digital manufacturing capabilities for materials production; the institute opened the Dassault 3DEXPERIENCE Center of Excellence in Advanced Composites at Purdue University, creating a physical space with large-scale equipment essential for the automotive industry that is a digital manufacturing capability test bed and education and training facility [84].
- AIM Photonics is working to improve photonics manufacturing, requiring research into materials and materials processing. AM has been identified as a promising area, with the potential to greatly simplify optical interconnect fabrication.
- In addition to R&D related to textiles and other NAMs, AFFOA actively works to build a network and ecosystem that includes materials suppliers, other manufacturing institutes, and other stakeholders. The institute brings together organizations that have a problem with other organizations that have developed a new material that could provide a solution.
- REMADE, through its focus on sustainable manufacturing, is actively considering how new materials at the start of the manufacturing process can improve the potential for reuse and recycling at the end of life of products. Accordingly, REMADE has a design node and conducts work related to materials selection. While the institute does not fund research for development of new materials directly, it produces knowledge and information that can inform specification for new materials that can be more effectively reused and recycled.

5.3.2. Federal Agencies with Jurisdiction

Several agencies support and oversee the development and application of NAMs; however, few agencies have the direct authority to regulate NAMs. The Department of Defense, DOE, NASA, and NSF are key drivers of the NAMs ecosystem, supporting research and providing funding for the development and application of NAMs. DoD, EPA, FAA, FDA, the Nuclear Regulatory Commission (NRC), and USDA have the authority to regulate materials and the sector-specific application of materials, and these regulations can be applied to NAMs. Within the Federal mineral estate, DOI administers the Mining Law on public domain lands and mineral leasing statues on acquired lands, in conjunction with any other Federal agency administering the surface estate. The Bureau of Industry and Security (BIS) and the Department of State both provide regulatory oversight in the form of export controls that may include NAMs. BIS controls the export of dual-use technologies,[128] while DOS controls defense goods, services and technologies, including technical data or information. Other agencies have less direct and clear jurisdiction over NAMs but are involved with the development or regulation of NAMs or NAMs marketplaces in various capacities. Further, the major contributors to the MGI are involved in supporting NAMs research, but not all

[128] Dual-use technologies have both military and commercial applications.

necessarily have jurisdiction over NAMs; the relevant activities of these agencies are described in other sections of this chapter. Table 4 lists agencies that have jurisdiction over NAMs in terms of regulation or funding, indicating the nature of oversight or involvement with NAMs.

Table 4. Agencies with Jurisdiction.

Agency	Type of jurisdiction	Description of jurisdiction
BIS [85]	Regulatory	Provides regulatory oversight of export controls on military and dual-use technologies which may include NAMs.
CPSC [86]	Regulatory	Establishes regulations and standards (mandatory and voluntary) for consumer products, including those related to materials.
DoD [87]	Funding, research	Funds NAMs research related to national security, including through Manufacturing USA institutes; engaged in the MGI.
DOE [88; 89]	Funding, research	Supports R&D of materials related to energy generation, storage, and transmission through multiple programs and offices; regulates activities and research on its own sites, including its National Laboratories; supports user facilities of critical importance to broad NAMs development; funds Manufacturing USA institutes; engaged in the MGI.
DOI [90]	Regulatory	Issues leases and permits for critical minerals in acquired lands and permits on public domain lands, including lands reserved for the National Forest System.
DOS [91]	Regulatory	Provides regulatory oversight of commercial exports of defense articles and services which may include NAMs.
EPA [92]	Regulatory, research	Develops and enforces regulations related to environmental topics, including regulations affecting materials, recycling, and the handling and disposal of hazardous materials; engages in research on nanomaterials.
FAA [93]	Regulatory, research	Regulates aviation; establishes partnerships with universities to create Centers of Excellence (COE) for aviation research, including on materials.
FDA [94]	Regulatory, coordination	Regulates products that involve nanomaterials with the goal of safeguarding public health; governs application of medical devices that

Agency	Type of jurisdiction	Description of jurisdiction
		use advanced materials; works to build knowledge and facilitate collaborations and partnerships to support the advancement of NAMs; engaged in the MGI.
FHWA [95; 96]	Research, coordination	Conducts research on/supports R&D on materials for surface transportation use; manages the Exploratory Advanced Research program and coordinates with the National Academies/Transportation Research Board's National Cooperative Highway Research Program (NCHRP), which research materials and materials applications.
NASA [97]	Research, guidance	Conducts materials research and develops materials to enable and support NASA missions and for technology transfer; engaged in the MGI.
NHTSA [98]	Regulatory	Establishes Federal Motor Vehicle Safety Standards (FMVSS), including those related to materials, requiring adherence to standards (e.g., ANSI).
NIH [99; 100]	Funding, research	Funds and manages research related to medical applications of advanced materials; has an NCL for pre-clinical efficacy and toxicity testing of nanoparticles; supports research into nanomaterials to understand their potential biocompatibility or toxicity to human health.
NIOSH [101]	Guidance	Protects health and safety of workers by promoting responsible development and use of advanced manufacturing technologies, including those involving research on advanced materials, such as nanomaterials and materials for and produced by additive manufacturing.
NIST [102]	Coordination, guidance, research	Develops testbeds, defines benchmarks, and develops formability measurements and models for materials; works to develop computational tools, databases, and experimental techniques to enable the design of materials; engaged in the MGI.

Agency	Type of jurisdiction	Description of jurisdiction
NRC [103]	Regulatory	Regulates commercial nuclear power plants and other uses of nuclear materials, such as in nuclear medicine, through licensing, inspection and enforcement of its requirements
NSF [104]	Coordination, funding, research	Supports fundamental research on novel materials, including through the Materials Innovation Platforms program; engaged in the MGI.
OSHA [105; 106]	Regulatory, guidance	Establishes guidelines for the handling and storage of hazardous materials; regulates occupational exposure to hazardous chemicals in laboratories.
PHMSA [107]	Regulatory	Oversees the transport of hazardous materials in all modes of transportation, except maritime [USCG], including NAMs (e.g., energetics).
USDA [108; 109]	Regulatory, funding, research	Supports research on biomaterials and bioproducts derived from agricultural and forestry products via the Agricultural Research Service, National Institute of Food and Agriculture, and Forest Service.
USDOT [110; 111]	Funding, research	Funds university consortia to create University Transportation Centers for surface transportation research and technology transfer, including on materials. Authorized to implement the Advanced Research Projects Agency-Infrastructure (ARPA-I), including developing and deploying advanced transportation infrastructure and materials (49 USC 119).
USGS [112]	Funding, research	Provides science and data on mineral potential, production, consumption, recycling, disposal, and interaction with the environment; engaged in the MGI.

In addition to the agencies listed in **Table 4**, the Department of Justice’s Antitrust Division and the Federal Trade Commission enforce laws that prevent firms from creating or exploiting market power that would distort allocation of resources or reduce innovation and, thereby, harm consumers. This mandate applies broadly across industries including those associated with NAMs.

5.3.3. Interaction of Federal Agencies with Industry Sectors

Federal agencies interact with industry sectors in several ways, including collaborating with manufacturers through PPPs, holding and participating in public meetings and workshops where one or more NAMs topics are being discussed, participating in industry working groups and consortia, providing regulatory oversight and guidance, and supporting basic and applied R&D. Representative examples of individual agency interactions are summarized in this section.

5.3.3.1.Bureau of Industry and Security (BIS)

BIS develops, implements, and interprets Federal export control policy for dual-use commodities, software, and technologies, some of which may be NAMs or may contain NAMs. As part of this mission, BIS provides policy guidance for exporters, including information on parties of concern, country guidance, and product guidance [113], along with online training [114], and hosts Technical Advisory Committees composed of Federal and industry representatives that advise the Department of Commerce on export controls on dual-use commodities and technology [115]. BIS also provides guidance on deemed exports—the release or transfer of technology to a foreign national in the United States—which may be relevant to domestic NAMs R&D [116].

5.3.3.2. Department of Defense (DoD)

DoD undertakes a variety of activities in support of developing and applying NAMs technology in the defense sector through the Basic Research Office, Service-based research offices such as the Air Force of Scientific Research, Army Research Office, and Office of Naval Research, and through the Defense Advanced Research Projects Agency (DARPA). In addition, DoD supports the development of the defense industrial base for advanced materials, coordinating investment in advanced materials and manufacturing through the activities of the Materials & Manufacturing Processes (M&MP) Community of Interest (CoI) [24]. DoD also sponsors 9 of the 16 Manufacturing USA institutes. These manufacturing institutes contribute to the adoption of NAMs by manufacturing products that incorporate NAMs. One example is LIFT, which supports the material and manufacturing process development of a lightweight steel alloy developed for use in ground vehicle armor [14]. A brief overview of relevant manufacturing institutes is provided in Section 5.3.1. DoD also supports joint research centers such as the MIT Institute for Soldier Nanotechnologies [117], the Center for Materials in Extreme Dynamic Environments (CMEDE) [118], and the Center for Research in Extreme Batteries (CREB) [119]. In addition to supporting NAMs R&D, DoD has air worthiness authority for military aircraft [120]; air worthiness certification criteria are contained in DoD Handbook 516C [121].

In addition to the various material societies and industry associations meetings, the Defense Manufacturing Conference (DMC) is one of the events where DoD, Service and industrial materials and manufacturing scientists, engineers, military leaders, program managers, and policy makers interact on materials and manufacturing innovations [122]. The DoD's Joint Defense Manufacturing Technology Panel (JDMTP) has four subpanels focused on electronics, composites, metals, and the advanced manufacturing enterprise, and includes representatives from industry as members [123].

5.3.3.3. Department of Energy (DOE)

DOE has several means of interacting with industry, primarily through its research and user facilities and via grant programs. The agency regulates the operations at its own, facilities, including the National Laboratories. In its role as regulator of these facilities, it sets its own standards and adopts external standards for the safe operations of its facilities. It also often participates in standard-setting organizations and conducts research to support safe operation of its facilities.

Industry and academia work to address materials challenges through the DOE's EMN, consisting of consortia focused on different energy materials challenges. Members can access National Laboratory facilities and personnel through Cooperative Research and Development Agreements (CRADAs) [43]. DOE funds academia and industry through grant programs, facilitating collaboration among academia, industry, and National Laboratory researchers through its Energy Frontier Research Centers (EFRCs) and other efforts to establish and support priority areas for fundamental research [124]. DOE funded 41 centers through 2021, 20 of which have the word "materials" or mention a class of material in the center title [125], and is funding 51 EFRCs in 2022.

DOE's Office of Energy Efficiency & Renewable Energy (EERE) focuses on applied R&D and experimental integration. R&D supported by EERE emphasizes next generation materials that can improve manufacturing processes and works to bring together industry partners and expertise in different areas needed to advance materials effectively. Further, DOE's EMN of consortia aims to accelerate the development and application of high-performance materials, including both functional materials and structural materials [43]. In response to national investments in advanced manufacturing and decarbonization, EERE split its Advanced Manufacturing Office in October 2022 into the Advanced Manufacturing and Materials Technologies Office (AMMTO) and the Industrial Efficiency and Decarbonization Office [126]. AMMTO focuses on accelerating innovation in the manufacturing sector and building a domestic clean energy technology manufacturing economy [127].

The Advanced Research Projects Agency-Energy (ARPA-E) is funding work on "exploratory topics" including recovery of critical minerals from waste streams and more efficient mining methods [128]. DOE's Vehicle Technologies Office (VTO) is funding ReCell, an advanced battery recycling research center [129]. DOE also collaborates with industry through voluntary partnerships such as the U.S. Driving Research and Innovation for Vehicle efficiency and Energy sustainability (U.S. DRIVE) partnership [130].

DOE's National Laboratories also have programs focused on small business users. For example, the Small Business Vouchers program provides opportunities for small businesses working on clean energy technology to use National Lab facilities to do prototyping, materials characterization, high-performance computation, modeling and simulation, product scaling, and technology performance validation [131].

5.3.3.4. Department of State (DOS)

DOS oversees the implementation of the Arms Export Control Act (AECA) and administers the International Traffic in Arms Regulations (ITAR) (22 CFR Parts 120-130), which include the United States Munitions List (USML; 22 CFR Part 121). The AECA and ITAR require that manufacturers, exporters, temporary importers, and brokers of defense articles and technology on the USML be registered with the DOS Directorate of Defense Trade Controls, that they maintain records of their export activities, and that they obtain licenses for all export activities. DOS provides guidance and support for exporters to comply with these requirements [132]. DOS also leads the Defense Trade Advisory Group, a formal body that regularly consults and coordinates with U.S. private sector defense exporters and defense trade specialists on topics pertaining to U.S. laws, policies, and regulations for exports of defense articles, services, and related technical data [133].

5.3.3.5. Food and Drug Administration (FDA)

An important part of FDA’s mission is to ensure the safety, efficacy, and security of drugs, biological products, and medical devices. FDA’s oversight includes requesting materials information from manufacturers on materials used in devices and products to produce toxicological reports to ensure product safety. In addition, FDA participates in meetings with industry associations including the Medical Device Manufacturers Association (MDMA) and in consortia such as the MDIC. The CDRH at FDA participates in 12 collaborative communities [134]. These communities are forums where public and private sector members address medical device challenges. These communities are established and managed by external organizations, [135] not by the FDA [136]. None of these collaboratives are NAMs-specific, but FDA participation allows the FDA to maintain awareness of advancements in the device and product technologies, and of emerging materials use and challenges.

5.3.3.6. Federal Aviation Administration (FAA)

FAA’s primary focus on materials and manufacturing technologies is in the context of products certification to ensure the safety of aviation in the United States. It works closely with industry both directly and through standards development organizations, working groups and consortia—including the Aerospace Industries Association, ASTM, the CMH-17 Coordination Group, MMPDS Emerging Technology Working Group, and SAE—to develop industry-based standards for the advanced materials and processes used to make aircraft parts. In addition, FAA collaborates with other Federal agencies and industry partners through the MMPDS, and CMH-17. FAA also supports materials R&D conducted by university partners through its Centers of Excellence [93], and has a process of early engagement with industry on new technologies including NAMs.

5.3.3.7. National Aeronautics and Space Administration (NASA)

As the U.S. civilian space agency, NASA has a variety of interests concerning the use of NAMs and manufacturing processes for aeronautics and space systems. NASA develops and issues standards for the design and building certification qualifications of hardware for spaceflight as needed. In addition to defining its own standards, NASA interacts with industry through its membership in Manufacturing USA institutes—including America Makes, AIM Photonics, and NextFlex—and through its participation in ASTM and SAE standards committees and working groups. NASA also works with the ASTM Additive Manufacturing Center of Excellence and the National Center for Additive Manufacturing Excellence (NCAME) at Auburn University [137; 138]. NASA conducts R&D in advanced materials for use in aircraft and other aerospace applications in coordination with the FAA and standards development organizations. For example, NASA's Hi-Rate Composite Aircraft Manufacturing (HiCAM) project aims to significantly reduce the time required to manufacture lightweight composite materials used in transport aircraft, in coordination with the FAA and industry partners [139].

5.3.3.8. National Institutes of Health (NIH)

The mission of the NIH "…is to seek fundamental knowledge about the nature and behavior of living systems and the application of that knowledge to enhance health, lengthen life, and reduce illness and disability" [140]. Materials advancements that have a specific function or medical utility—focused on materials in contact with human biology—are of interest to NIH. NIH interacts with industry and non-profit organizations through a variety of mechanisms, including grants and contracts, to address medical questions, not materials per se. NIH does interact with industry via standards development organizations when it is determined to be important as part of activities and goals for a specific NIH program or effort.

5.3.3.9. National Institute of Standards and Technology (NIST)

NIST's core mission focuses on advancing measurements, standards and technology to enhance national economic security by promoting innovation and industrial competitiveness. Currently, NIST NAMs activities are intended to advance the MGI paradigm and MII in areas of NIST's mission and technical expertise. NIST is establishing protocols and means to advance data and model accessibility, utility, and quality for all stakeholders interested in accelerated materials development. In addition to internal projects, NIST is working towards these goals in conjunction with industry, academia, and government stakeholders. NIST internal, cross-laboratory efforts include projects to develop advanced superalloys and composites for the transportation and mobility industries [141]. NIST also interacts with industry in other ways, including holding workshops, industry meetings, and outreach events attended by industry representatives, researchers, and standards development organizations. NIST personnel are active in professional society TCs and serve on standards TCs.

Understanding the NAMs ecosystem is another area in which NIST is providing support, funding multiple projects to carry out industry-driven roadmapping for microelectronics, semiconductors, and digital thread as part of the manufacturing supply chain [142].

5.3.3.10. National Science Foundation (NSF)

Similar to other agencies, NSF has no regulatory authority, but it does interact with industry through its participation in Manufacturing USA institutes—America Makes and NextFlex. NSF supports advanced materials R&D aligned with the MGI goals and strategy through the Designing Materials to Revolutionize and Engineer our Future (DMREF) and the Materials Innovation Platforms (MIPs) programs. DMREF is the principal NSF program responsive to MGI, and supports teams within and across disciplines that synergistically work to significantly accelerate the materials discovery-to-use timeline by building the fundamental knowledge base needed to advance the design, development, or manufacturability (i.e., properties relevant to manufacturing, process-property relationships, property performance metrics, scalable synthesis routes, economic feasibility, supply chain considerations, or life cycle issues) of materials with desirable properties or functionality. MIPs support collaboration of teams to develop cutting edge tools and establish a user facility allowing access to advanced materials and manufacturing stakeholders, including academic and industrial researchers [143]. In addition, NSF has the Grant Opportunities for Academic Liaison with Industry (GOALI) program that encourages interaction among academia and industry as supplemental funding for an existing NSF-funded award [144]; NSF also funds institutes of higher education.

5.3.3.11. Nuclear Regulatory Commission (NRC)

NRC is responsible for licensing and regulating the Nation's civilian use of radioactive materials. The agency's focus on NAMs is currently on assessing gaps from a technical and regulatory perspective, although the agency's role in standards development also covers additional activities. As with other regulatory agencies, NRC is primarily concerned with the safety and quality of components and their constituent materials.

NRC actively participates in SDO activities with ASTM as well as other SDOs, to identify potential safety concerns so that they can be addressed during standards development. The agency engages with ASTM on NAMs standards and is a participant in the NNI.

NRC's participation facilitates more efficient regulatory process and potential approval of the use of NAMs in nuclear applications. In addition, NRC provides effective oversight of the nuclear supply chain by performing inspections to assure the quality and specifications of safety-related systems, structures and components, including those produced using NAMs, meet applicable regulatory, technical, and quality requirements. The NRC participates in public forums to address technical and regulatory issues and solicit feedback.

5.3.3.12. U.S. Geological Survey (USGS)

USGS Mineral Resources Program studies the location, availability, and quality of mineral resources. Activities also include research into and assessment of the effects—environmental and economic—of resource extraction and use [145]. USGS provides information on mineral criticality that can be used by the materials community to inform development of new materials for new products and innovative substitution approaches for scarce critical minerals used in existing products. This criticality information may be particularly relevant to the development of clean energy technologies. The USGS compiles industry information on domestic and global production of minerals, and conducts geologic research to inform resource assessments, including field work, geologic mapping, geochemical analysis, and remote sensing of topographic, geophysical, and hyperspectral data.

5.3.4. U.S. Federal Government Interagency Activities

The MGI, NNI, and NQI are the three most noteworthy Federal interagency efforts supporting the advancement of NAMs. Other cross-agency collaborations are also important in supporting and advancing the NAMs ecosystem. This section provides an overview of the MGI, NNI, NQI, and other interagency efforts relevant to NAMs.

5.3.4.1. The Materials Genome Initiative (MGI)

The MGI aims to accelerate materials discovery, manufacturing, and deployment by creating policy and providing resources to support materials R&D. Materials R&D that is consistent with the MGI strategy and with the ICME approach and initiatives, will reduce the time needed for materials and process development and qualification. ICME is " the integration of materials information, captured in computational tools, with engineering product performance analysis and manufacturing-process simulation," [146] and entails the integration of personnel (e.g., engineers, designers, scientists), models, and computational development programs. [147] Participating agency partners in the MGI include DOE, DoD (including the U.S. Army, U.S. Air Force, U.S. Navy, and DARPA), FDA, NASA, NIH, NIST, NNI, NSF, OSTP, and USGS, among others [148]. These agencies support the goals of the MGI through efforts aligned with the goals of the initiative, detailed in the 2021 MGI Strategic Plan. The three goals defined in the strategic plan are included and briefly described below [8]:

- "Unify the Materials Innovation Infrastructure," which provides a framework for knowledge sharing among stakeholders to support materials R&D, manufacturing, and deployment.
- "Harness the Power of Materials Data," which can use the MMI as a foundation to enable data analysis and the application of artificial intelligence (AI) to rapidly accelerate materials R&D.
- "Educate, Train, and Connect the Materials R&D Workforce," which includes efforts to strengthen the workforce across the materials development continuum.

5.3.4.2. The National Nanotechnology Initiative (NNI)

The NNI is a R&D initiative focused on advancing and improving understanding of nanotechnology and associated applications to benefit industry and society [149]. Over 30 participating agencies contribute to work toward the goals of the initiative outlined in the 2021 NNI Strategic Plan. The five goals of the plan are included below [9]:

- "Ensure that the United States remains a world leader in nanotechnology research and development;
- Promote commercialization of nanotechnology R&D;

- Provide the infrastructure to sustainably support nanotechnology research, development, and deployment;
- Engage the public and expand the nanotechnology workforce; and
- Ensure the responsible development of nanotechnology.

As indicated in other sections of this chapter, several agencies also operate research facilities available for use by researchers. DOE, the National Cancer Institute (part of NIH), NIST, and NSF each specifically operate nanotechnology research facilities and are affiliated with the NNI [100].

5.3.4.3. The National Quantum Initiative (NQI)

The NQI features broad participation from Federal agencies, including: DHS, DoD (including the U.S. Army, U.S. Air Force, U.S. Navy, DARPA, and NSA), DOE, DOI, DOJ, DOS, DOT, NASA, NIH, NIST, NOAA, NSF, ODNI (including IARPA), OMB, USDA, and USPTO [150]. Interagency coordination occurs via the NSTC Subcommittee on QIS and Subcommittee on Economic and Security Implications of Quantum Science [151].

The 2020 report *Quantum Frontiers: Report on Community Input to the Nation's Strategy for Quantum Information Science* describes eight areas or frontiers that are priorities for R&D investment through the NQI [152]:

Expanding opportunities for quantum technologies to benefit society;

Building the discipline of quantum engineering;

Targeting materials science for quantum technologies;

Exploring quantum mechanics through quantum simulations;

Harnessing quantum information technology for precision measurements;

Generating and distributing quantum entanglement for new applications;

Characterizing and mitigating quantum errors; and

Understanding the universe through quantum information.

The NQI seeks to identify research opportunities at the intersection of materials science and quantum technologies to "advance the theories, tools, and techniques that will enable researchers to explore the fundamental quantum nature of materials, predict material properties, devise new synthesis and integration processes, and target new kinds of materials" [152]. Key areas include, but are not limited to, advances in atomic-scale imaging, advances in materials characterization for quantum materials, advances in quantum computing accelerating AI-driven materials discovery. As with any emerging technology area, developing a deeper understanding of processing, structure, properties, and performance of quantum materials and devices presents both opportunities and challenges [152].

5.3.4.4. Other Federal Interagency Efforts

In addition to the MGI and the NNI, several other interagency collaborations support NAMs. FIMaR Meetings were held annually in recent years, focusing on a different topic each year related to materials. The meetings are open to Federal employees, and have been organized by NIST, DOE, and other agencies to bring together program managers from across disciplines to discuss materials research and cross-agency coordination and collaboration [153].

Another example of cross-agency efforts are strategic partnerships established by NSF—rather than limiting collaborations with other agencies to co-funding, NSF aims to develop solutions alongside other agencies. The Air Force Research Lab (AFRL) has a strong relationship with NSF, for example, that involves funding as well as joint academic research and workforce initiatives [154]. DOE also collaborates strategically with NSF in areas including workforce development. The Nanotechnology Characterization Laboratory (NCL), supported by the National Cancer Institute, was established under an agreement between NCI, FDA, and NIST [39]. The effort aims to strengthen the medical device development ecosystem and support small businesses by providing toolsets, methodologies, and other resources.

The FCAB, led by DOE, DoD, the Department of Commerce, and DOS, brings together Federal agencies interested in ensuring a robust domestic supply of materials required for the production of lithium batteries; the FCAB encourages coordination of advanced battery efforts across Federal agencies to strengthen the domestic battery ecosystem [155]. The FCAB has released documents in support of this mission, including a pre-application battery test manual and the *National Blueprint for Lithium Batteries 2021-2030* report [156; 157].

The MATES group is focused on regenerative medicine, which involves the development and application of NAMs. NIH, FDA, NSF, VA, NIST, DoD, and NASA are engaged in the effort, established in 2000 and operating as an ad hoc interagency working group since 2007 [158]. The technological needs to advance the fields of tissue science and engineering and regenerative medicine, which drive the working group, rely heavily on NAMs and advanced manufacturing [159].

FAA engages with other agencies on projects related to NAMs, such as NASA and DoD. For example, FAA collaborates with America Makes to fund the National Institute for Aviation Research (NIAR) at Wichita State University [160]. The FAA Center of Excellence for Composites and Advanced Materials (CECAM) and NCAMP, funded jointly by FAA and AFRL, are also located at NIAR. FAA has also jointly sponsored research with DoD on developing a public AM material database [161].

The NSTC Critical Minerals Subcommittee (CMS) is co-chaired by OSTP, DOE, and USGS. The CMS coordinates interagency activities related to critical minerals, which are relevant to NAM activities.

5.3.5. Regulations, Guidelines, Mandatory Standards, Voluntary Standards, and Other Policies Implemented by Federal Agencies

Federal agencies use, develop, and participate in the development and implementation of regulations, mandatory and voluntary standards, and other policies according to their missions and needs. The scope of NAMs and the ways in which Federal agencies may interact with NAMs-related regulations, mandatory and voluntary standards, and other policies is too large to enumerate in this chapter. Instead, the sections below highlight how Federal agencies implement these instruments and include some examples of particular importance to individual agencies' development and/or use of NAMs.

5.3.5.1. BIS

BIS oversees Federal Export Administration Regulations (15 CFR parts 730-774) for dual-use technologies [162], which include the Commerce Control List (CCL) [163]. The CCL consists of 10 categories, which may include NAMs:

- Category 0, Nuclear materials facilities and equipment;
- Category 1, Materials, chemicals, microorganisms, and toxins;
- Category 2, Materials processing;
- Category 3, Electronics design, development, and production;
- Category 4, Computers;
- Category 5, Telecommunications and information security;
- Category 6, Sensors and lasers;
- Category 7, Navigation and avionics;
- Category 8, Marine; and
- Category 9, Aerospace and propulsion.

These categories are further divided into 5 groups: end items, equipment, accessories, attachments, parts, components, and systems; test, inspection, and production equipment; materials; software; and technology. Exporters must determine the category and group for any item (commodity or technology) that will be exported and must also identify an Export Control Classification Number that indicates whether export of that item is controlled because of its characteristics, qualities, or end-use.

5.3.5.2. DoD

DoD engages with standards development at different stages of NAMs research, development, and deployment. The Defense Standardization Program develops standards for DoD use, many of which are for non-commercial products, but DoD also implements public standards to maximize the utility of its products [164]. DoD personnel, including the Office of the Secretary of Defense (OSD) and U.S. military service personnel participate in standards development processes for AM (with ASME) and metals/alloys (with SME, formerly the Society of Mechanical Engineers).

DoD interfaces with NIST to develop standards, such as to measure the effectiveness of environmental cleanup processes. Standards are also relevant at the testing stage to ensure that materials meet performance specification. DoD works with the Department of Transportation indirectly to meet requirements/regulations to get materials from one place to another and may interact directly if new vehicles are being developed to ensure that all materials used are appropriate. The U.S Navy is leading efforts on DoD-wide battery standards, taking into consideration elements such as cold weather or airworthiness requirements. OSD is working to develop shareable data requirements for AM that would be overseen by the Joint Additive Manufacturing Working Group and the Industrial Base Council. New technology areas in which DoD is engaging where there may be a need for regulations and standards include synthetic biology and human augmentation.

Guidelines developed by other Federal agencies and non-governmental organizations may be relevant to DoD's use of materials. For example, DoD uses standards on hexavalent chromium exposure from the American Conference of Governmental Industrial Hygienists that sets out operational limits and drives efforts to eliminate these chemicals from paints and other materials [165]. Similarly, EPA emissions regulations on hazardous solvents drive the removal of these chemicals from paints and other coatings used by DoD [166].

5.3.5.3. DOE

DOE regulates the operations at its own, facilities, including the National Laboratories. In its role as regulator of these facilities, it sets its own standards and adopts external standards for the safe operations of its facilities. It also often participates in standard-setting organizations and conducts research to support safe operation of its facilities. Other parts of DOE focused on demonstration and/or deployment of energy technologies are more engaged with standards, as they make it possible for performance results to be compared to assess progress and to ensure that technologies will function as expected during use. Materials-related standards developed by DOE primarily focus on nuclear materials [167]. DOE interacts with standards development organizations both formally and informally, and DOE industry partners may also participate in these processes.

5.3.5.4. DOS

Under section 38 of the AECA, DOS has the authority to control the commercial export of defense articles and services enumerated on the USML. These authorities are primarily implemented via the ITAR, which apply to the manufacture, export and temporary import of defense articles. Currently, USML categories include:

- Firearms and related articles;
- Guns and armament;
- Ammunition and ordnance;
- Launch vehicles, missiles, rockets, torpedoes, bombs, and mines;
- Explosive and energetic materials, propellants, and incendiary agents;
- Surface vessels of war and special naval equipment;
- Ground vehicles;
- Aircraft;
- Military training equipment and training;
- Personal protective equipment (PPE);
- Military electronics;
- Fire control, laser, imaging, and guidance equipment;
- Materials;
- Toxicological agents;
- Spacecraft;

- Nuclear weapons-related articles; and
- Directed energy weapons;
- Gas turbine engines; and
- Submersible vessels.

NAMs may be relevant to any of these categories, e.g., in coatings, structural components, and electronics. DOS makes frequent updates and revisions to the ITAR and USML to reflect changes in technology and U.S. national security and foreign policy interests. Defense articles not subject to the ITAR or specified by other regulations are controlled by BIS' Export Administration Regulations.

5.3.5.5. EPA

EPA regulates nanomaterials under the Toxic Substances Control Act (TSCA; 15 C.F.R. §2601) (1976) [168] and, if they are used for pesticides, under the Federal Insecticide, Fungicide, and Rodenticide Act (FIFRA) (7 U.S.C. 136) [169]. As part of its TSCA authority, EPA issued a rule in 2017 that requires manufacturers to do one-time reporting and accounting on available exposure and health and safety information on certain nanomaterials in commercial use. TSCA also requires that manufacturers submit premanufacture notification under section 5 of TSCA and provide the required information on any nanomaterials that are considered new chemical substances. EPA is required to review that information, make a determination, and address any unreasonable risks before those nanomaterials are manufactured. EPA may also regulate nanomaterials at specific sites under the Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA), Resource Conservation and Recovery Act (RCRA), Clean Water Act (CWA), or Clean Air Act (CAA) [169]. These regulatory authorities are also relevant to cases where nanomaterials are used in a way that leads to the release of hazardous pollutants.

EPA is contributing to the efforts of ISO technical committee ISO/TC 229, which is working to develop standards for nanomaterial-related terminology, metrology, and instrumentation [170]. These efforts include development of reference materials and test methods, modeling and simulation, and science-based health, safety and environmental practices.

5.3.5.6. FAA

FAA is a regulatory and safety agency. Regulations relevant to FAA's mission are in 14 C.F.R. §21 (general requirements for certifying a product for design, production or airworthiness) and 14 C.F.R. §23-§35 (unique regulations for specific product types, e.g., engines, propellers, rotorcraft). Broadly, these requirements focus on "controlling the material" and "controlling the process," as well as on materials strength and design values, rather than on specific materials.

FAA guidance typically provides methods of compliance or interprets regulations for specific technologies. Industry handbooks such as the CMH-17 are the basis for some of this guidance, and MMPDS and CMH-17 also provide material data [171]. Standards developed by SAE International are relevant to aerospace materials, particularly metals and composites, but companies may also create their own standards and methods of compliance [81]. Industry standards fill many purposes, including material and process specifications and qualification procedures. These standards may be used by applicants as part of their data package for demonstrating compliance with FAA regulations. FAA accepts NCAMP specifications and allowables for composite materials [172].

The FAA participates in industry organizations to document best industry practices and publish standards for applicants to use to support certification. These include CMH-17, MMPDS, America Makes, SAE additive manufacturing committees and P-17 Polymer Matrix Composites Committee, and the ASTM F42 committee on AM. The agency has also participated in the AIA Additive Manufacturing Working Group, the AWS S20 committee, and ASTM committee D30 on composite materials. The FAA also publishes its own guidance in the form of advisory circulars and policy statements or memos [173].

5.3.5.7. FDA

FDA regulates food contact materials, most of which are not NAMs [174]. One exception is nanomaterials, which may be used in food contact materials, as food additives, in drug formulations, and in cosmetics [175]. Based on recommendations made in the agency's 2007 *Nanotechnology Task Force Report* [176], FDA issued a series of industry guidelines focused on the use of nanomaterials and nanotechnology in these product categories [177]. FDA also released the *2013 Nanotechnology Regulatory Research Plan*, which featured four main areas: staff training and professional development, laboratory core facilities, the Collaborative Opportunities for Research in Science program, and internal FDA coordination on nanotechnology research [178].

In addition to nanomaterials, FDA evaluates and regulates medical devices, which may include NAMs, in their final, completed, sterilized form [179]. FDA is therefore interested in all of the NAMs that make up a device, how those devices are manufactured, and their final application. FDA is working to develop clearer and more streamlined processes for materials assessment in devices, such as using statistical and computational modeling methods.

Biocompatibility of device materials is a key property that FDA evaluates based on ISO standard ISO 10993-1, and the agency has issued guidance for FDA staff and others on how to use this standard [180; 181]. The agency is also currently developing a framework for understanding and communicating the potential risks associated with materials used in medical devices that are implanted long-term (e.g., pacemakers, artificial joints) [182]. Elements currently under consideration for the framework include product labeling and materials lists for products. FDA has also partnered with ECRI, a non-profit organization, to carry systematic literature reviews on materials that are commonly used in implanted medical devices [183].

FDA regulates materials intended for dental, oral, and craniofacial applications, including dental amalgams, under 21 C.F.R. part 872, and works with the National Institute of Dental and Craniofacial Research at NIH to support advancement of NAMs in dentistry and address a lack of clinically relevant standards for adequate preclinical evaluations of safety and effectiveness [184]. This is also the only area where FDA regulates a single NAM, yttria-stabilized zirconia (YSZ), which is used in dental crowns. Dental ceramics are also being produced using AM techniques. FDA also works with the National Cancer Institute of NIH on developing characterization assays used by the Nanotechnology Characterization Laboratory (NCL).

Industry groups are an important partner for FDA, and the agency works with these groups to clarify agency processes and requirements around materials. FDA maintains a “regulatory assistance” website that lists databases relevant to materials, including a searchable public database of recognized voluntary consensus standards [185; 186]. The agency has also developed “Safety and Performance-Based Pathway” guidance that applies to well-understood types of devices and sets out performance criteria that can be used to help obtain premarket authorization for devices in this category [187].

FDA participates in international standards development and partially or fully recognizes some international standards. One standard that is particularly important is ISO IEC 60601 on medical electrical equipment and medical electrical systems used in home healthcare [188].

5.3.5.8. NASA

NASA does not develop regulations around its activities, but standards play an important role in its programs. NASA’s Commercial Crew Program includes programmatic standards, which may be existing standards that the program must meet or may be standards developed by private sector companies partnering with NASA on a program. NASA works with these partners to ensure the standards are technically sound and meet the intent of NASA’s programs. NASA may also develop its own standards in cases where standards do not exist and the need for the standard is unique to NASA’s work [189]. NASA research related to NAMs used in civil aviation applications informs development of industry standards used by the FAA and the civil aviation equipment manufacturers.

In terms of specific NAMs, NASA is interested in certification and qualification standards around AM materials, as well as standards for flammability and compatibility of materials [190]. NASA has also developed a materials standard for spaceflight [191]. Standards that help identify flaws, such as fracture control standards, are also very important [192]. NASA staff participate in standards development organization committees on NAMs topics of relevance to the agency.

5.3.5.9. NIH

NIH does not develop or implement regulations. The importance and need for standards varies according to the R&D stage of NAMs in NIH-funded projects. Standards are generally not a major component of early-stage research, but software and data standards may be important. Later-stage research may benefit from standards to ensure that a particular platform or technology can be more broadly applied, and standards development will depend on the needs of the NAMs research community and whether the community indicates it will adopt standards. NIH often relies on NAMs standards developed by IEEE and ASME.

NIH is also working on interoperability of data, and standards are a key component of that effort, as relates to collecting, annotating, and curating data and to developing relevant tools and best practices. NIH developed a new Data Management and Sharing Policy tool that went into effect in January 2023 [193].

5.3.5.10. NSF

NSF does not participate in the development of NAMs regulations or standards, but standards may be a topic of interest to principal investigators on NSF grants depending on their research community. For example, development of NAMs in the biology or electronics community might require standards to allow for comparison of experimental results. However, NSF proposals do not often include standards. Research areas where standards are needed include biofoundries and 2D materials. Standards will also likely be relevant to the new Technology, Innovation and Partnerships Directorate at NSF [194].

Standards for materials data is an area in which NSF participates, including funding a recent workshop to develop a governing group to support data standards development. A key challenge of implementing these data standards is that there is no single NAMs community. Initial efforts have focused on 2D materials data, and the MIPs have also been a way for the community to access relevant datasets.

5.3.6. Guidelines, Mandatory Standards, Voluntary Standards, and Other Policies Implemented by Industry-Based Bodies

Any standards that apply to materials, including specifications for materials performance, may be applicable to NAMs. This section provides an overview of efforts by some industry-based bodies to develop guidelines, standards, and policies on materials.

5.3.6.1. ASTM

Federal agency staff participate in most NAMs standards development processes at ASTM. ASTM standards are also frequently incorporated by reference into Federal regulations. ASTM provides free access to all standards that are referenced in Federal regulations in the “ASTM Reading Room” [195]. Examples of NAMs-relevant ASTM standards committees include:

- Committee E56 on Nanotechnology [196], which has subcommittees focused on informatics and terminology; physical and chemical characterization; environment, health, and safety; nano-enabled consumer products; education and workforce development; and nano-enabled medical products [197].
- Committee C28 on Advanced Ceramics [198], which has subcommittees focused on mechanical properties and performance; physical properties and non-destructive evaluation; applications; and CMCs [199].
- Committee D30 on Composite Materials [200], which has subcommittees focused on lamina and laminate test methods; structural test methods; interlaminar properties; sandwich construction; and composites for civil structures [201].

- Committee B09 on Metal Powders and Metal Powder Products [202], which has subcommittees focused on structural parts and metal powders for use in AM applications [203].
- Committee B08 on Metallic and Inorganic Coatings [204], which has subcommittees focused on soft metals and coatings, including those used in extreme environments [205].
- Committee E44 on Solar, Geothermal and Other Alternative Energy Sources [206], which has subcommittees focused on materials for developing alternative energy sources [207].
- Committee D20 on Plastics [208], which has subcommittees focused on thermoplastic materials; material content origin; natural environment degradation/biodegradation; and man-made environmental degradation/biodegradation [209].
- Committee F42 on Additive Manufacturing, which has subcommittees focused on design, materials and processes, environmental safety and health, and applications [210].

5.3.6.2. IEEE

Nanotechnology is a focus of IEEE via its Nanotechnology Council. IEEE published standard IEEE 1906.1, “Practice for nanoscale and molecular communication framework” in 2015 [211]. IEEE is also interested in three-dimensional body processing using new sensor technologies, with standard IEEE P3141 “Standard for 3D Body Processing” currently under development [212]. IEEE recently released its “International Roadmap for Devices and Systems” focused on commercialization of microelectronics products, including relevant materials, and is working on an effort to roadmap future technologies such as micromechanical universal switches and mixing sensors and relays [213]. Standards development is currently happening in the traditional power sector with the aim of increasing efficiency using NAMs.

5.3.6.3. VAMAS

Standards are developed by VAMAS in Technical Working Areas (TWAs), in which one or more standards may be under development at any given time. The TWAs that are currently active are shown in Table 5 [214].

Table 5. VAMAS Technical Working Areas.

TWA Number	Topic
TWA 2	Surface Chemical Analysis
TWA 5	Polymer Composites
TWA 16	Superconducting Materials

TWA Number	Topic
TWA 24	Performance Related Properties of Electroceramics
TWA 31	Creep, Crack and Fatigue Growth in Weldments
TWA 33	Polymer Nanocomposites
TWA 34	Nanoparticle Populations
TWA 36	Printed, flexible and stretchable electronics
TWA 37	Quantitative Microstructural Analysis
TWA 39	Solid Sorbents
TWA 40	Synthetic Biomaterials
TWA 42	Raman Spectroscopy and Microscopy
TWA 43	Thermal Properties
TWA 44	Self-Healing Ceramics
TWA 45	Micro and Nano Plastics in the Environment

5.3.6.4. Manufacturing USA Institutes

The information presented in this section is based on discussion with individual Manufacturing USA institutes and may not reflect all of the NAMs-related standards work that these institutes are conducting.

AFFOA works with standards development organizations on standards for smart fibers and sensing fibers. This standards work can be challenging because these fibers are not one-component materials and are new technology that requires rules and guidelines for its use and characterization—the standards work is starting from a blank page. AFFOA is also looking to engage its members using standards.

BioFabUSA has a focus on biocompatibility of its biomaterials, with a particular focus on NAMs and their appropriate use for implants that interact with the human body. These NAMs should have the appropriate physical characteristics of an implant and be able to interact chemically with the body to allow a patient's own cells to grow into the implant or to integrate with existing tissues to function. As part of this work, BioFabUSA is part of the Standards Coordinating Body for Regenerative Medicine, a small nonprofit organization headquartered at NIST that aims to coordinate standards development in this area and has published a report of needed standards indicating where there are gaps [215; 216].

IACMI is currently working on NAMs that lack standards—composite materials have physical testing standards and reinforced plastics have standards, but neither set of standards is sufficient for new composites, particularly when they are being used in AM. The need for standards in this area is to translate and provide continuity between process, validation, and qualification.

LIFT established a recent program with the U.S. Army Ground Vehicles Service Center on weld standards where LIFT acted as a neutral third party to facilitate the revision of the standard.

REMADE is currently working with NIST on an ISO standard related to the circular economy, as part of the institute's mission is to bring together people working on materials, re-manufacturing, and design to standardize terminology, advance technology, and address knowledge gaps. REMADE has not yet made a lot of direct investment in standards but is working to standardize language around emissions reduction and circular economy.

5.3.7. Federal Government Resources for Consumers and Small Businesses to Evaluate the Use of NAMs

In addition to direct funding that Federal agencies may provide to small businesses in the form of grants via the Small Business Innovation Research (SBIR) or Small Business Technology Transfer (STTR) programs, which may be used for NAMs development or for development or integration into products, the Federal Government also supports a variety of other resources that are specific to the NAMs industry. This section is divided into several subsections that describe particular categories of government resources that may be used by small businesses, consumers, or others to evaluate the use of NAMs. These include a variety of experimental user facilities, computational user facilities, centers, and other online resources that fit this description [217]. DOE defines a user facility as "a Federally-sponsored research facility available for external use to advance scientific or technical knowledge" under conditions related to access and use.[129]

5.3.7.1. Documents, Data, and Informational Resources

The Federal Government makes available a variety of documents, data sets, and informational resources that may be used by small businesses or consumers to evaluate or assess NAMs. This section describes several examples of these.

The National Institute for Occupational Safety and Health (NIOSH) has published a variety of documents covering the occupational risks and hazards associated with nanomaterials, many of which are developed by its Nanotechnology Research Center [219; 220].[130] Guidance documents available from NIOSH cover workplace safety, health effects of occupational exposure, guidance on building a safety program for the nanotechnology workforce tailored to small- and medium-sized enterprises, and information about occupational exposure to a few particular materials (titanium dioxide, carbon nanotubes and nanofibers, and silver nanomaterials). Other nanotechnology-related publications from NIOSH include strategic plans for the agency and progress reports. NIOSH has also developed resources for AM, including safe working with metal powders and thermoplastics [221].

[129] The DOE definition of "user facilities" indicates that facilities are available for use under the following conditions: they are open to all interested potential users; resources are allocated based on merit review of the proposed work; user fees are not charged for non-proprietary work; facilities provide resources sufficient for users to conduct work safely and efficiently; facilities support information-sharing and collaboration; and facility capabilities do not compete with available private sector capabilities DOE Office of Science.

[130] A full list of guidance and publications concerning nanotechnology is available on the NIOSH website National Institute for Occupational Safety and Health.

NIOSH also provides documentation on other workplace and safety topics related to chemical hazards, which may be relevant for the processing or disposal of NAMs. A good resource on this topic is the *NIOSH Pocket Guide to Chemical Hazards*, which is offered in print, online, in PDF form, and via a mobile web application [222].

The FDA also has produced a number of documents related to safety of metals and materials used in medical devices. These resources include information about FDA's evaluation methods, reviews of scientific literature, as well as material-specific summaries of safety information [183].[131] These documents are available to the public and may be of interest to both consumers and small businesses in evaluating material selection related to medical devices. Links to many relevant resources are available on the FDA website [179].

NIST supports the "Materials Resource Registry" (MRR), which is a central service that helps with discoverability of materials resources [223]. The MRR is a comprehensive resource that can be used to find materials data infrastructure and information including both government-hosted and non-government hosted resources. There are nearly 300 entries included in the MRR, covering organizations, data collections, data sets, services, informational websites, software, and semantic assets. This registry is open to the public and is an efficient way for small businesses to locate useful data, tools, information, or organizations. This resource can also help curious consumers find information of interest for understanding NAMs and their use. Numerous materials data repositories, including government-hosted repositories, may be accessed through the MRR [224].[132]

NIST also makes available standard reference materials (SRMs), which can be used for calibrating instruments. Instrument calibration is needed for quality assurance of materials produced by researchers as well as commercial entities large and small. NIST SRMs may be ordered from NIST, and NIST has produced extensive documentation in connection with their SRMs [225].

The FAA shares results of their funded research in the area of NAMs through its William J. Hughes Technical Center reports and other publications, as well as other information dissemination mechanisms. For example, the FAA has been organizing annual workshops on qualification and certification of composites and AM, and proceedings of such workshops are made available to the public [226].

The NNI produces an *Annual Supplement to the President's Budget* that describes past budgetary allocations related to nanotechnology, plans for future investment in nanotechnology, and progress towards the goals of the NNI. This annual document includes numerous descriptions of ongoing work supported by the agencies that participate in the NNI and has sometimes been accompanied by supplements that give even more detail [11].

The United States Patent and Trademark Office (USPTO) maintains a searchable, public database of patents and published patent applications [227], a portion of which provides disclosure of patented or patent-pending advanced materials, which may include NAMs. The database may serve as a resource for NAMs researchers or companies interested in licensing NAMs for use in their products.

[131] As of 03/09/2022, the following materials safety summaries were available from the FDA: magnesium, polypropylene, polyurethanes, siloxanes, polyethylene terephthalate (PET), polyethylene glycol (PEG), silver, acrylic acid derivatives, and polyhydroxy acids and other blends and copolymers.

[132] A list of materials data resources specifically hosted by NIST in connection to the MGI is available at the cited source.

5.3.7.2. Department of Energy National Laboratory User Facilities

DOE supports a variety of experimental and computational user facilities that are located at DOE National Laboratories around the country and open to researchers through peer reviewed user programs [228]. DOE's Office of Science stewards 28 of these user facilities with several additional facilities stewarded by DOE's applied energy offices. These user facilities provide advanced research tools that may be used by scientists to conduct simulation, fabrication, and characterization of materials. Users include government, academic, and commercial scientists from the United States and internationally. Determination of access is typically based on a competitive proposal review process, and the work conducted at these facilities includes basic research as well as proprietary work performed on a full cost recovery basis. Users intending to publish their work can access the facilities free of charge if their proposals are accepted; users generating proprietary data typically must pay for access. These experimental and computational facilities represent essential infrastructure that supports the discovery and development of every class of NAMs. The DOE user facilities of primary interest for materials science research and characterization are:

- Argonne National Laboratory (ANL)
    - Advanced Photon Source (APS)
    - Center for Nanoscale Materials (CNM)
    - Argonne Leadership Computing Facility (ALCF)
- Lawrence Berkeley National Laboratory (LBNL)
    - Advanced Light Source (ALS)
    - The Molecular Foundry (TMF)
    - National Energy Research Scientific Computing Center (NERSC)
    - Energy Sciences Network (ESnet)
- Brookhaven National Laboratory (BNL)
    - National Synchrotron Light Source II (NSLS-II)
    - Center for Functional Nanomaterials (CFN)
- Los Alamos National Laboratory (LANL) and Sandia National Laboratory (SNL)
    - Center for Integrated Nanotechnologies (CINT)
- Oak Ridge National Laboratory (ORNL)
    - Carbon Fiber Technology Facility (CFTF)
    - Center for Nanophase Materials Sciences (CNMS)
    - High Flux Isotope Reactor (HFIR)

    - Manufacturing Demonstration Facility (MDF)
    - National Transportation Research Center (NTRC)
    - Oak Ridge Leadership Computing Facility (OLCF)
    - Spallation Neutron Source (SNS)
- SLAC National Accelerator Laboratory
    - LINAC Coherent Light Source (LCLS)
    - Stanford Synchrotron Radiation Lightsource (SSRL)

Included in the above are neutron (SNS, HFIR) and X-ray, ultraviolet, infrared (IR) and/or ultrafast electron (APS, ALS, NSLS-II, LCLS, SSRL) sources that allow researchers to probe materials properties at exceptional resolution in space, time, and energy. Materials of every type may be studied, ranging from metals and ceramics to polymers and biological materials. These tools may be used to probe the electronic, magnetic, and physical structures of materials, to observe processes in real time down to the femtosecond scale, to image materials in two and three dimensions, and to measure their properties and processes in extreme environments. Many of the capabilities provided at these facilities are only available at a few locations in the world.

Also included in the above list are computing facilities (ALCF, OLCF, NERSC), which enable researchers to conduct simulations of materials. Simulations are key in discovery of NAMs, including for screening out huge numbers of potential candidate materials to identify the most promising ones to fabricate and study experimentally. Computational modeling of materials is also key to guiding optimization of materials for a given purpose by helping researchers understand materials properties and processes. Researchers can access the DOE's computing centers and experimental data sets thanks to the ESnet, which is a high-speed network stewarded at LBNL that connects the National Laboratories' data infrastructure and enables large datasets generated at the National Laboratories to be transferred to users globally.

A third category of user facilities in the above list are the Nanoscale Science Research Centers (NSRCs) (CNM, TMF, CFN, CINT, CNMS) that are part of DOE's contribution to the NNI [229]. These centers were created by DOE specifically for the study of materials and phenomena at the nanoscale and contain specialized equipment for the fabrication and characterization of nanoscale materials, such as clean rooms, microscopes, and a variety of other instruments and equipment. NSRC user facilities enable high-impact nanoscience research via a peer-reviewed user program that is open to the scientific community. Four of the NSRCs are co-located at DOE National Labs with major user facilities such as neutron or synchrotron light sources.

5.3.7.3. National Science Foundation Materials Research Science and Engineering Centers (MRSECs)

The NSF MRSECs support sustained materials research and education by establishing and supporting campus-based research centers [194]. These research centers support one or more interdisciplinary research groups that focus on a topic that requires sustained, interactive research among researchers with diverse but complementary technical specialties. MRSECs are funded on a 6-year basis, with a new round of awards granted every 3 years and remain operational after the conclusion of NSF funding through new research grants and other sources. MRSECs may compete for new awards periodically, and many MRSECs have been funded through the MRSEC program more than once. Many MRSECs also support industry cooperation by providing access to their facilities and enabling interactions with their researchers. These centers enable small businesses to access advanced scientific tools that would be far too expensive to purchase directly, while also enabling key collaborations that can help commercial entities solve challenges limiting the development and commercialization of NAMs. MRSECs typically contain a mixture of fabrication and characterization tools. Below is a list of MRSECs that are operating on a current MRSEC award. Note that only awards in the last 6 years are still supported through the NSF MRSEC program—numerous MRSECs awarded prior to 2016 are still operational, but no longer directly supported through the MRSEC program:

- Awarded in 2017:
    - Center for Dynamics and Control of Materials, University of Texas at Austin
    - Illinois Materials Research Center, University of Illinois Urbana-Champaign
    - UW Molecular Engineering Materials Center, University of Washington
    - MRSEC, UC Santa Barbara
    - Cornell Center for Materials Research, Cornell University
    - Center for Multifunctional Materials, Northwestern University
    - MRSEC, University of Pennsylvania
    - Wisconsin MRSEC, University of Wisconsin - Madison
- Awarded in 2020:
    - University of Delaware Center for Hybrid, Active, and Responsive Materials
    - UC Irvine Center for Materials Discovery
    - UC San Diego Materials Research Center
    - Brandeis University Center for Bioinspired Soft Materials
    - Columbia University Center for Precision-Assembled Quantum Materials
    - Harvard University Materials Research Center
    - Ohio State University Center for Emergent Materials
    - Penn State University Center for Nanoscale Science
    - Princeton University Center for Complex Materials
    - University of Chicago Materials Research Center
    - University of Minnesota Materials Research Center

As is apparent from the titles listed, some MRSECs are quite general to a variety of categories of NAMs, and others specialize in particular categories of NAMs or applications for NAMs.

5.3.7.4. NSF National Nanotechnology Coordinated Infrastructure

Similar to the MRSECs, the National Nanotechnology Coordinated Infrastructure (NNCI) centers are user facilities located at universities that allow academic researchers, small companies, large companies, and government access to fabrication and characterization tools and instrumentation, as well as opportunities to collaborate and interact with researchers [230]. The NNCI sites and their coordination office receive about $16M annually, and the program was most recently renewed in 2020 for another 5 years. In all, there are 16 user facilities, as listed in **Table 6**[133]

[133] More information about individual NNCI sites can be found at: https://nnci.net/sites/view-all.

Table 6. National Nanotechnology Coordinated Infrastructure (NNCI) Centers.

NNCI Center	Host University
Center for Nanoscale Systems	Harvard University
Cornell Nanoscale Science and Technology Facility	Cornell University
Kentucky Multi-scale Manufacturing and Nano Integration Node	University of Louisville and University of Kentucky
Mid-Atlantic Nanotechnology Hub for Research, Education and Innovation	University of Pennsylvania and Community College of Philadelphia
Midwest Nanotechnology Infrastructure Corridor	University of Minnesota Twin Cities and North Dakota State University
Montana Nanotechnology Facility	Montana State University and Carlton College
nano@stanford	Stanford University
Nanotechnology Collaborative Infrastructure Southwest	Arizona State University, Maricopa County Community College District, and Science Foundation Arizona
Nebraska Nanoscale Facility	University of Nebraska-Lincoln
Northwest Nanotechnology Infrastructure	University of Washington and Oregon State University
Research Triangle Nanotechnology Network	North Carolina State University, Duke University, and University of North Carolina-Chapel Hill
San Diego Nanotechnology Infrastructure	University of California, San Diego
Soft and Hybrid Nanotechnology Experimental Resource	Northwestern University and University of Chicago
Southeastern Nanotechnology Infrastructure Corridor	Georgia Institute of Technology, North Carolina A&T State University, and University of North Carolina-Greensboro
Texas Nanofabrication Facility	UT Austin

The NNCI sites are available to students and professionals from throughout the United States and the world. They are equipped to support R&D as well as product and process development, which can assist start-ups and more established companies with commercialization of nanotechnology innovations.

5.3.7.5. NSF Science and Technology Centers (STCs)

The NSF STC: Integrative Partnerships program funds multi-institute centers that focus on complex research and education topics requiring long-term grant awards [231]. The centers are initially funded for 5 years with the possibility of additional years of funding. STCs partner with industry, National Labs, and other entities and focus their work on a broad range of subject areas, including NAMs. For example, the 2013 cohort of STCs included the Center for Integrated Quantum Materials [232] and the 2021 cohort included the Center for Integration of Modern Optoelectronic Materials on Demand [233].

5.3.7.6. NIST and NSF Center for High Resolution Neutron Scattering (CHRNS)

The CHRNS is a neutron scattering user facility that can be used to study the structure and dynamics of materials at a variety of length and energy scales [234]. Of all the neutron facilities in North America, the CHRNS has the widest range of accessible length and energy scales (1 nm to ~10 µm, ~30 neV to ~100 meV), which makes this facility of broad applicability to researchers studying all types of NAMs. Like the DOE user facilities, the CHRNS can be accessed by university, government, and industrial researchers through a competitive proposal review process.

5.3.7.7. NIST Center for Nanoscale Science and Technology (CNST)

The CNST is a user facility that makes nanomaterials fabrication and characterization equipment available to researchers from industry, academia, and government on a pay-for-time basis [235]. Like the DOE's Nanoscale Science Research Centers, the CNST is a place where researchers from academia and industry can prepare samples, test fabrication processes, and characterize materials. The CNST has a relatively simple application process that eases access to the facility.

5.3.7.8. Department of Defense-Supported Facilities

DoD supports several facilities that may be accessed by industry; those facilities include characterization and fabrication tools for NAMs R&D, such as the Cornell CHESS MSN-C Beamline [236]. Like the DOE, NIST, and NSF facilities listed above, industry players including small businesses may access the facilities or collaborate with researchers at these facilities based on the particular project, which may include evaluation of NAMs.

5.3.7.9. Computational Materials Science Centers (CMSCs) and the Network for Computational Nanotechnology

DOE, NSF, and NIST each support one or more CMSCs (Table 7). DOE CMSCs produce validated community codes and databases that may be used for designing materials and predicting their properties [237]. Validated codes can be used by small and large businesses for accelerating development and deployment of NAMs. Many of these centers also supply other educational resources that may be of interest for understanding NAMs or NAMs simulation methods. The websites corresponding to these centers are typically hosted by a National Laboratory, although contributors may be distributed around the country.

Table 7. Computational Materials Science Centers (CMSCs).

CMSC	Funding Agency
Center for Computational Study of Excited-State Phenomena in Energy Materials [238]	DOE
Center for Predictive Simulation of Functional Materials [239]	DOE
Midwest Integrated Center for Computational Materials [240]	DOE
Comscope Center for Computational Materials Spectroscopy and Design at Brookhaven National Laboratory[a] [241]	DOE
Non-Perturbative Studies of Functional Materials under Non-Equilibrium Conditions (NPNEQ) [242]	DOE
Center for Hierarchical Materials Design (CHiMaD) at Northwestern University [243]	NIST
Molecular Sciences Software Institute (MolSSI)[b] [244]	NSF[c] [245]
Science Gateways Community Institute [246]	NSF

[a]Comscope was funded as the "Center for Computational Design of Functional Strongly Correlated Materials and Theoretical Spectroscopy"; [b]MolSSI is also the host of the Quantum Chemistry Archive, which is a source for compiling, aggregating, querying, and sharing quantum chemistry data; [c]MolSSI is supported by a 5-year $15M award from NSF.

NSF also funds the Network for Computational Nanotechnology to advance nanoscience and nanotechnology [247], which includes two nodes associated with research and education efforts that focus on different areas of nanoscience: nanoMFG and Engineered nanoBio [248; 249].

5.4. Marketplace and Supply Chain

The NAMs marketplace and supply chain faces risks stemming from both economic and technical challenges. Currently, risks involve limited supply chains for material categories that are difficult to manufacture or for which there is a small market and low business incentive for creating a supply; the establishment and ongoing expansion of the Manufacturing USA network reflects Federal efforts to address these risks. Long-term risks involve instability of critical materials supply chains, including critical minerals. Another challenge is developing the NAMs workforce by increasing the accessibility of education and information related to practical NAMs manufacturing and development.

5.4.1. Risks to the NAMs Supply Chain and Marketplace

5.4.1.1. Critical Minerals

Critical minerals are defined in the Energy Act of 2020 as any mineral that is essential to the economic or national security of the United States, whose supply chain is vulnerable to disruption, and which serves an essential function in the manufacturing of a product without which there would be significant consequences for the economic or national security of the United States [250]. The Energy Act requires that the list of critical minerals be updated every 3 years.

The 2022 USGS list of critical minerals includes the following 50 minerals [251]: aluminum, antimony, arsenic, barite, beryllium, bismuth, cerium, cesium, chromium, cobalt, dysprosium, erbium, europium, fluorspar, gadolinium, gallium, germanium, graphite, hafnium, holmium, indium, iridium, lanthanum, lithium, lutetium, magnesium, manganese, neodymium, nickel, niobium, palladium, platinum, praseodymium, rhodium, rubidium, ruthenium, samarium, scandium, tantalum, tellurium, terbium, thulium, tin, titanium, tungsten, vanadium, ytterbium, yttrium, zinc, and zirconium.

Many categories of NAMs require the use of critical minerals (see the examples above and in Figure 1 in the 2022 report by the U.S. Government Accountability Office (GAO) on critical minerals [252]), and therefore supply chain and market concerns around critical minerals are also relevant to NAMs.

Three examples of recent legislation that address the critical minerals supply chain are Infrastructure Investment and Jobs Act (2021)[134], the CHIPS and Science Act (2022)[135], and the Inflation Reduction Act (2022)[136]. The Infrastructure Investment and Jobs Act addresses critical minerals as a component of supply chains for clean energy technologies, calling for an improvement to the Federal permitting process for critical mineral production on Federal land; development of critical mineral mining and recycling research; establishment of a grant program for processing, recycling, or development of critical minerals; and coordination of Federal science and technology efforts to ensure secure and reliable supplies of critical minerals by the NSTC CMS. The CHIPS and Science Act authorizes NSF to advance R&D related to mapping, mining, extraction, and processing of critical minerals and calls for establishing a CMS under the NSTC to support interagency coordination of critical minerals R&D. Language in the Inflation Reduction Act amends the Federal clean vehicle tax credit program to address critical mineral requirements in vehicle batteries, extends the Federal advanced energy project tax credit, and designates facilities for processing, refining, or recycling critical materials as “advanced energy properties” that serve to reduce greenhouse gas emissions.

5.4.2. Risks by Materials Category

The following list includes selected supply chain and marketplace risks for various categories of NAMs as defined in **Table 1**:

- **Biomimetic:** Biomimetic materials are difficult to manufacture at scale.
- **Catalysts:** Platinum-group metals are a concern, as they are major catalysts for many reaction chemistries.

[134] The text of the Infrastructure Investment and Jobs Act of 2021 (H.R. 3684) can be found at: https://www.congress.gov/bill/117th-congress/house-bill/3684/text

[135] The text of the CHIPS and Science Act of 2022 (H.R. 4346) can be found at: https://www.congress.gov/bill/117th-congress/house-bill/4346/text.

[136]The text of the Inflation Reduction Act of 2022 (H.R. 5376) can be found at: https://www.congress.gov/bill/117th-congress/house-bill/5376/text.

- **Correlated materials:** Rare earth elements (particularly dysprosium, neodymium, and other permanent-magnet rare earth elements) present key concerns and motivate identification and development of NAMs that do not use such critical minerals.
- **Electronic and photonic materials:** While silicon is the dominant material in this category, many other materials are also of interest and present supply chain concerns. Silicon is not a critical mineral, though there are concerns related to scalability to widespread adoption of silicon-based solar. Many new and advanced semiconductor materials use elements derived from critical minerals, such as gallium, arsenic, and tellurium.[137] The most widely used transparent conductive oxides (indium tin oxide, zinc oxide) use indium and tin or zinc, all of which are on the Critical Minerals list. Another integral challenge is the importance of purity in determining if a material is useful for various applications—materials for electronics and photonics require a very high level of purity, which can create supply chain problems even if the elements involved are not critical minerals.
- **Energy storage and conversion materials:** Reliance of lithium-ion battery electrodes on lithium, cobalt, nickel, manganese, copper and graphite presents a key concern. The role of platinum-group metals as catalysts for proton exchange membrane fuel cells presents another concern and relates to the issue of scaling-up solar power [253].
- **Lightweight and structural materials:** Aluminum, magnesium, titanium, and lithium are on the 2022 USGS list of critical minerals. Further, manufacturing of CCCs is very challenging, and suppliers are limited. Composite reinforcements in general could have supply chain vulnerabilities if not produced domestically.
- **Materials for extreme environments:** Tungsten, tantalum, and a variety of other transition metal elements (e.g., cerium, yttrium, and zirconium) may be of interest for high temperature or oxidation-resistant environments, as may aluminum oxide.
- **Polymers and polymer composites:** Polymers use petrochemicals as feedstock, presenting a risk through dependence on the petrochemical supply chain.
- **Reactive and responsive materials:** Shape memory alloys require aluminum, nickel, titanium and zinc, all of which are on the USGS critical minerals list [254].
- **Soft materials:** Any materials using rare earth elements or platinum group metals may present a supply chain risk, as many are on the USGS critical minerals list.
- **Other:** Quantum-grade diamond has a very limited set of suppliers, and carbon nanotubes are difficult to manufacture.

5.4.2.1. Supply Chain Risks

NAMs supply chain risks lie at the intersection of the economic and technical aspects of the market. Multiple manufacturing institutes and standards organizations indicated that a lack of business incentives contributes to unstable supply chains for certain materials. Specifically,

[137] For example, lithium niobate faces supply chain issues not only based on the shortage of lithium supply, but also because of the manufacturing expense. There are very few suppliers for this material.

small-market users for a particular NAM do not promise widespread enough use to justify the production of that material, meaning that manufacturers must choose to invest for potentially low return. Many advanced technologies also require the use of high-purity materials, which usually require additional processing, and therefore cost, to produce at the desired purity. There are also quality concerns around high-purity materials, as batch-to-batch variation can reduce the reliability of these materials. Some companies are circumventing this challenge by manufacturing their materials in-house to ensure a stable supply chain, but this not always a feasible solution. The complexity of NAMs supply chains can also pose a risk, particularly for manufacturers of finished products. Identifying the "manufacturers" and "suppliers" in the chain can be difficult, which can complicate efforts to address supply chain issues.

As these markets mature, another source of supply chain risk could stem from possible anticompetitive conduct of NAMs suppliers. Suppliers with market power could pursue their private interest by raising price or restricting access, thereby potentially reducing use of NAMs, overall incentives to invest in related R&D, and overall resilience of NAMs markets. Market power could result from: control of critical intellectual property; markets whose size can only support a small number of suppliers; or industry consolidation.

Supply chain risks also exist for products that include NAMs but have a smaller market, such as medical devices. For example, only 2–3 companies globally produce the ultra-high molecular-weight polyethylene needed to produce artificial joints. Because these devices are ordered in small quantities and to precise specifications, manufacturers are unwilling to invest in their production. This is a supply chain issue, but also a barrier to innovation. Point-of-care AM may be one solution to improving the supply chain for devices, and this is an area that FDA is exploring [255].

Even common materials such as nitrile and polypropylene, both widely used in healthcare, can experience supply chain shocks that raise concerns about quality and U.S. access to products. The U.S. supply of personal protective equipment (PPE) was severely disrupted by the COVID-19 pandemic, which also raised concerns around the quality of PPE that the United States was able to obtain [256]. There is interest in the materials community in ensuring that high-quality products are available in the U.S. supply chain, part of which may include developing substitute materials such as biomaterials that can provide the same level of quality and performance and be produced domestically.

Critical minerals are a significant motivating factor in the NAMs supply chain, and there is a similar trend toward identifying NAMs that are potential substitutes for existing materials that rely on critical minerals. Motivation to diversify materials outside of critical mineral reliance is seen in multiple industries using permanent magnets, such as the energy storage industry, and Federal agencies are supporting several research centers targeting this concern, such as DOE's ReCell Center.

Recovery of critical minerals from products is another area of interest. The GAO's 2022 report assessed the implementation of recommendations made in the 2019 report *A Federal Strategy to Ensure Secure and Reliable Supplies of Critical Minerals* [257] and identified five major constraints to advancing critical minerals recovery: "(1) limited data and analytical tools to support decision making, (2) limited research and development, (3) limited domestic infrastructure and capacity, (4) potential adverse effects on the environment and worker safety, and (5) limited economic viability of recovery and substitution methods" [252].

The DOE Office of Science held a roundtable in November 2021 on mitigation of supply chain risk for scientific facilities and tools that included representatives from DOE national laboratories and user facilities, academia, and industry [258]. Although the findings are specific to DOE facilities, the roundtable discussed several topics that are broadly relevant to NAMs, including specialty materials, machining, and manufacturing. The report includes examples of materials and components to illustrate specific supply chain challenges and risks and highlights improvements that could be made to DOE's processes, including collaboration and coordination among the national laboratories to address and mitigate supply chain risks. Other longer-term opportunities for improvement that could be relevant to broader domestic supply chain risks for NAMs include:

- Incorporating resiliency considerations into procurement decisions;
- Conducting competitiveness analyses on specific industries, materials, or supply chains to assess domestic capabilities;
- Carrying out cross-laboratory supply chain forecasting;
- Using consortia and other cooperative mechanisms to foster collaboration with industry;
- Supporting the small business ecosystem to supply critical components and technologies, including through technology transfer;
- Initiating career development programs to support technical expertise; and
- Establishing PPPs to develop emerging markets to build the domestic supply chain.

The resiliency of the supply chain is one consideration during standards development for NAMs. Flexible processes for standard development can ensure that standards can be revised or updated as needed in response to minor or major supply chain disruptions so that material and/or product quality and performance are maintained.

5.4.2.2. Marketplace Risks

Development and innovation of NAMs is sensitive to shifts in energy prices and markets. As the DOE *2015 Quadrennial Technology Review* summarized, increases in energy prices motivate greater efficiency and demands for new energy-efficient materials. Conversely, decreases in energy prices can shift demand away from new and improved energy-efficient materials. The Quadrennial Review also emphasized the value of computational and experimental R&D of NAMs in the context of pressing national economic, environmental, and security challenges, highlighting the need for mechanisms to address the energy-dependent sensitivities and risks of the materials market. Specifically, NAMs advancements in high-strength lightweight materials for vehicles, clean energy, increased energy efficiency, and waste reduction—all of which may contribute to mitigating global climate change—face sensitivities and risks based on shifts in energy prices [259, Chapter 6].

The White House's Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth: 100-Day Reviews under Executive Order 14017 report (hereafter "the Building Resilient Supply Chains report") highlights several risk factors for the strategic and critical materials sector, including: concentration of supply; byproduct and coproduction dependency; and market/economic shocks [253]. The report states, “A significant portion of global production for strategic and critical materials is concentrated in only one or a few countries. This lack of supplier diversity creates not only market challenges for nascent producers, it also means a large portion of global supply is subject to single-point disruption risk (e.g., natural disasters, shifting industrial or trade policies).” The report identifies 37 “shortfall strategic and critical materials” for which one country has a share of global production that exceeds half of the total global production of these materials. Byproduct and coproduction dependency is a risk for strategic and critical materials that are generated exclusively from byproduct production, meaning that comparatively small materials markets must rely on the conditions of larger commodity markets. Market/economic shocks may occur due to the small markets for many strategic and critical materials and the financial complexity of increasing their production, which results in short-term inelasticity in supply.

5.4.3. Risks to the National Security, Including Economic Security, of the United States

As NAMs are developed and integrated into technologies across a wide spectrum of applications, ensuring a reliable supply chain of minerals used in NAMs is a key national security concern. Specifically, the issue of critical minerals drives much of NAMs development and security.

5.4.3.1. Critical Minerals

The transition of U.S. energy consumption away from fossil fuels and toward electrification is a broader trend key to the relationship between critical minerals and NAMs development. The *Building Resilient Supply Chains* report forecasts demand for critical minerals to intensify alongside the demand for more “green” technologies such as electric vehicles, wind turbines, and advanced batteries and energy storage capabilities [253]. The report cites estimates that electric cars require six times the mineral inputs of conventional cars, and onshore wind plants require nine times more mineral resources than a gas-fired plant.

Critical minerals such as lithium are key for battery and energy storage technologies. Permanent-magnet rare earth elements, such as dysprosium and neodymium, are integral to insulators and electronic materials. The geographic concentration of certain critical minerals supply chains constitutes a national security risk to the United States. For many critical minerals, production at multiple value chain steps, especially refining and processing, is concentrated in other nations. For example, 89 percent of rare earths separation and 90 percent of rare earths metal refining occurred in the People’s Republic of China (PRC) in 2020 [220].[138]

In September 2022, the White House concurred with the Secretary of Commerce’s finding that neodymium-iron-boron (NdFeB) magnet imports threaten national security under section

[138] The PRC also has made significant investments in mining in other countries. For example, China owns or has a stake in 15 of the 19 cobalt-producing mines in the Democratic Republic of the Congo The Economist, “How Chinese Firms Have Changed Africa,” https://www.economist.com/special-report/2022/05/20/how-chinese-firms-have-changed-africa.

232 of the Trade Expansion Act of 1962, as amended [261]. This finding was based in part on the fact that the United States and its allies and partners are heavily dependent on imports of NdFeB magnets from the PRC, which also dominates the value chain of rare earths used in NdFeB magnets. Reliance on critical minerals for these high-demand and emerging technologies provides a key motivator for the R&D of NAMs that do not use critical minerals and can substitute the function of critical minerals in such technologies.

Critical minerals are of sufficient concern that the White House issued a memorandum in March 2022 that states: “The United States depends on unreliable foreign sources for many of the strategic and critical materials necessary for the clean energy transition…To promote the national defense, the United States must secure a reliable and sustainable supply of such strategic and critical materials” [262]. The memorandum invokes the President’s authority under section 303 of the Defense Production Act (50 U.S.C. 4533) and directs the Secretary of Defense to “create, maintain, protect, expand, or restore sustainable and responsible domestic production capabilities of such strategic and critical materials by supporting feasibility studies for mature mining, beneficiation, and value-added processing projects; by-product and co-product production at existing mining, mine waste reclamation, and other industrial facilities; mining, beneficiation, and value-added processing modernization to increase productivity, environmental sustainability, and workforce safety; and any other such activities authorized under section 303(a)(1) of the Act.”

In June 2022, DOS established the Minerals Security Partnership (MSP), whose goal is “to ensure that critical minerals are produced, processed, and recycled in a manner that supports the ability of countries to realize the full economic development benefit of their geological endowments.” [263] MSP members are Australia, Canada, Finland, France, Germany, Japan, the Republic of Korea, Sweden, the United Kingdom, the United States, and the European Commission. The first convening of the MSP in September 2022 included member nations as well as other mineral-rich countries: Argentina, Brazil, the Democratic Republic of the Congo, Mongolia, Mozambique, Namibia, Tanzania, and Zambia. [264]

5.4.3.2. International Efforts

The United States is not alone in its investments in materials innovation. For example, the European Union has also prioritized the NAMs industry, investing €465 million in technology-focused infrastructure [265].[139] The PRC launched the Materials Genome Engineering project in 2016, with similar goals to the MGI [267]. The United Kingdom recently requested public comment on advanced materials as part of its national Innovation Strategy [268]. These efforts indicate that NAMs are a technological priority globally.

5.4.4. Emerging Risks and Long-Term Trends in the Marketplace and Supply Chain

Given the complexities of NAMs development and associated risks, a comprehensive analysis outlining and visualizing the NAMs supply chain, including an assessment of future

[139] A group of European researchers and industry leaders released the “Materials 2030 Manifesto” in February of 2022, which describes how “a strong European materials ecosystem drives the green and digital transition as well as a sustainable inclusive European society” The European Commission.

risks and of potential bottlenecks, would benefit NAMs developers and regulators. For example, blockchain is emerging as a tool for organizing supply chain logistics of materials [269].

5.4.4.1. Supply Chain Evolution and Sustainability

Critical minerals are integral to many materials with applications outside of energy technologies, applications such as medical imaging, medical and industrial lasers, ceramics and building materials, and electrical contacts and chip resistors in computers [251]. Thus, a comprehensive analysis outlining and visualizing the NAMs supply chain would directly address critical minerals. For example, understanding the evolution of the rare earth elements market may inform an understanding of the future energy-dependent marketplace and supply chain. Understanding shifts in the battery and permanent magnet markets from the 1900s-2000s—including the PRC's role in mining and processing markets, which industries followed the market shift, and other cascading events—may inform the outlook on long-term trends as the demand for energy-efficient technologies increases in response to global climate change.

Sustainability across the life cycle of materials is a concern of many Federal agencies. Sustainable mining and processing, alongside sustainability of the supply chain, are strategic goals and principles in the *Strategy to Support Domestic Critical Mineral and Material Supply Chains* [270]. The *Building Resilient Supply Chains* report emphasizes a renewed focus on sustainability to rebuild for resilience at a national level.

Chapter 6 of DOE's 2015 *Quadrennial Technology Review* also discusses topics related to sustainability, focusing on "Innovating Clean Energy Technologies in Advanced Manufacturing" [259]. The chapter includes details of the importance of new types of materials to achieving reduced energy use and impacts in this context. Among other topics, the chapter and its appendices discuss the circular economy, energy and material efficiency, and critical materials to enable clean energy technologies.

The GAO's 2022 *Trends Affecting Government and Society* report identifies U.S. access to critical materials as a key driver of uncertainty in the "Science, Technology, and the Innovation Economy" category, particularly in relation to future domestic manufacturing of advanced technologies [271]. The report cites "a global shift toward localizing supply chains, along with continued geopolitical conflicts" as critical factors.

5.4.4.2. NAMs Workforce Development

Across manufacturing sectors, there is a critical need to make practical, workforce-targeted education accessible. Key manufacturing jobs do not require advanced academic education, such as a doctorate degree; rather, they require highly skilled technical education [272]. This issue of access to skill-based education affects the NAMs workforce and market. In addition to education accessibility, a critical element of NAMs workforce development is making analysis tools and systems practical for use by members of the workforce performing on-the-ground testing. Ensuring that high-quality career and technical education and science, technology, engineering, and mathematics education is available to K-12 students will also help to create a pipeline for a robust future workforce for NAMs technologies.

To address workforce development and training, all Manufacturing USA Institutes are required to include a workforce component. These workforce initiatives vary across the institutes to target an array of education levels and training modes. Institutes develop educational materials and trainings for manufacturing professionals and students through workshops, registered apprenticeships, virtual and augmented reality simulations, and creation of standards for manufacturing curricula and credentials. In this connection, the utilization of proven workforce training techniques, such as registered apprenticeships and pre-apprenticeships, as well as the effective promotion of labor-management partnerships, could help to accelerate the expansion and development of a skilled NAM workforce within the manufacturing sector. Such expansion should also be carefully designed to ensure the inclusion of underserved communities and populations who have faced barriers to labor market entry in this key industry.

Workforce development is an integral aspect of the MGI, responding to the concern surrounding a U.S.-accessible workforce. Further, multiple Federal agencies call for more internships giving students the ability to connect across components of materials development. The education and training of a next-generation materials R&D workforce is an integral part of the DMREF program. Aligning with Goal 3 of the 2021 MGI Strategic Plan, DMREF promotes diverse and inclusive education, training, and workforce development that can crosslink across all components of the materials development continuum. The four MIP programs, based around the MGI philosophy of building community, provide facilities for synthesis, characterization, computation, and data analysis all available in one program and built around solving a problem. For example, BioPacific, a MIP collaboration between University of California-Santa Barbara and University of California-Los Angeles, is training students to use synthetic biology to make sustainable polymers of the future. Challenges in coordinating interagency funding present barriers to development of such workforce opportunities.

The NQI released the *Quantum Information Science and Technology Workforce Development Strategic Plan* in 2022, which focuses on four major areas: developing and maintaining an understanding of the workforce needs in the quantum information science and technology (QIST) ecosystem; introducing broader audiences to QIST through public outreach and educational materials; addressing QIST-specific gaps in professional education and training opportunities; and making careers in QIST and related fields more accessible and equitable [273].

ASTM E56 on Nanotechnology has a Subcommittee E56.07 on Education and Workforce Development. This subcommittee has developed six standards related to educational curricula in nanotechnology. Certification by examination programs have been developed for several of these standards. Students who successfully complete certificate programs are recognized by the NSF-funded Nanotechnology Applications and Career Knowledge Network and ASTM's Credentialing Program Registry.

5.5. Recommendations

The following recommendations are based on challenges identified in interviews with Federal employees, representatives of manufacturing institutes, and standards development organizations; recent NAMs reports and publications; and responses to the public RFI. The recommendations address:

- Growing the U.S. economy through the safe and secure advancement of NAMs;
- Strengthen U.S. global competitiveness through faster and broader adoption of NAMs;
- Mitigate current and emerging risks to the NAMs marketplace, supply chain, and workforce; and
- Advance the adoption of NAMs where there are advantages and opportunities to be gained.

Challenge 1: The funding and support needs of the NAMs community vary widely.

Recommendation 1: The U.S. Government should assess current funding and support mechanisms for NAMs development at relevant Federal agencies, including identification of existing mechanisms and evaluation of their effectiveness where possible. Consider the different scales at which NAMs development is occurring and identify where barriers exist. Consider whether fundamental research is being effectively translated into NAMs applications.

Challenge 2**:** Increased global investments in NAMs.

Recommendation 2: The U.S. Government should assess global investments and strategies related to NAMs and, where appropriate, disseminate the results to provide opportunities for increased international collaboration and U.S. leadership. Engage with international partners on standards development to bolster U.S. interests and work towards globally harmonized standards. Assess the effects of existing export control regulations on NAMs development and advancement.

Challenge 3: Many NAMs are based on critical minerals, raising supply chain and sustainability concerns.

Recommendation 3: The U.S. Government should continue to support research that identifies substitute materials, including substitutes for critical minerals, develops methods for the recovery of existing supplies of NAMs containing critical minerals, and develops approaches to enhance critical mineral supplies via improvements in production and processing. Incorporate life cycle approaches that include assessments of feedstocks, energy efficiency, and recyclability into NAMs development to proactively mitigate sustainability issues.

Challenge 4: The diversity of NAMs properties and applications means that their supply chains are complex and global, which creates barriers to their advancement and adoption.

Recommendation 4: The U.S. Government should continue Federal roadmapping efforts that provide the materials community with the information and tools needed to understand and make decisions about NAMs supply chains, including supply chain disruptions. Leverage the extensive expertise in the NAMs community in these efforts.

Challenge 5: The diversity of NAMs applications and the fundamental enabling nature of NAMs for a wide variety of technological advancements requires that the United States maintains leading-edge research infrastructure and a skilled Federal workforce to enable and enhance coordination among Federal agencies and sectors.

Recommendation 5: The U.S. Government should maintain core competencies at Federal agencies, including those directly supporting NAMs research and applications and those playing a more indirect role, to ensure that the U.S. Government maintains its critical role in NAMs development.

> ***Recommendation 5a:*** Ensure that the Federal Government continues to host leading-edge research infrastructure and instrumentation for NAMs characterization and synthesis, such as user facility instrumentation.
>
> ***Recommendation 5b:*** Ensure that Federal agencies maintain a skilled workforce by expanding efforts to train existing personnel and hire new personnel in relevant NAMs fields.
>
> ***Recommendation 5c:*** Use existing interagency mechanisms to ensure that agencies are coordinating their efforts effectively, including with the larger NAMs community. Continue to coordinate and provide infrastructure for pre-competitive engagement among industry, government, and academia on NAMs manufacturing. Delineate agency roles to provide clear pathways for NAMs community engagement with the Federal Government.

Challenge 6: The NAMs community needs best practices, standards, and guidance around NAMs, including for safe use, data, and cybersecurity.

Recommendation 6: The U.S. Government should provide leadership to the NAMs community by empowering the MGI and other high-level Federal initiatives to develop and disseminate NAMs best practices, standards, risk management, and guidance, including data and cybersecurity standards, and protection of intellectual property rights to promote capital investment and further development.

References

[1] Featherston, Charles, and Eoin O'Sullivan. "A Review of International Public Sector Strategies and Roadmaps: A Case Study in Advanced Materials." 2014. https://www.ifm.eng.cam.ac.uk/uploads/Resources/Featherston__OSullivan_2014_-_A_review_of_international_public_sector_roadmaps-_advanced_materials_full_report.pdf.

[2] Kennedy, Alan, Jonathon Brame, Taylor Rycroft, Matthew Wood, Valerie Zemba, Charles Weiss, Matthew Hull, Cary Hill, Charles Geraci, and Igor Linkov. "A Definition and Categorization System for Advanced Materials: The Foundation for Risk-Informed Environmental Health and Safety Testing." *Risk Analysis* 39, no. 8 (2019): 1783–95. https://doi.org/10.1111/risa.13304. https://onlinelibrary.wiley.com/doi/10.1111/risa.13304.

[3] Advanced Manufacturing National Program Office. "Advanced Manufacturing." https://www.manufacturing.gov/glossary/advanced-manufacturing.

[4] National Science and Technology Council (NSTC) Fast Track Action Subcommittee on Critical and Emerging Technologies. "Critical and Emerging Technologies List Update." https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf.

[5] Scott, Troy, Amanda Walsh, Benjamin Anderson, Alan O'Connor, and Gregory Tassey. "High-Tech Infrastructure and Economic Growth: The Materials Genome Initiative." *Science and Public Policy* 48, no. 5 (2021): 649–61. https://doi.org/10.1093/scipol/scab042. https://academic.oup.com/spp/article/48/5/649/6311311.

[6] Subcommittee on Quantum Information Science under the Committee on Science of the National Science & Technology Council. "National Strategic Overview for Quantum Information Science." https://www.quantum.gov/wp-content/uploads/2020/10/2018_NSTC_National_Strategic_Overview_QIS.pdf.

[7] National Quantum Initiative. "National Quantum Strategy." https://www.quantum.gov/strategy/#STRATEGY-DOCUMENTS.

[8] National Science and Technology Council. "Materials Genome Initiative Strategic Plan." National Science and Technology Council (NSTC), Subcommittee on the Materials Genome Initiative, Washington, DC, November 2021. https://www.mgi.gov/sites/default/files/documents/MGI-2021-Strategic-Plan.pdf.

[9] National Science and Technology Council (NSTC), Subcommittee on Nanoscale Science, Engineering, and Technology. "National Nanotechnology Initiative Strategic Plan." National Science and Technology Council (NSTC), Washington, DC, October 2021. https://www.nano.gov/sites/default/files/pub_resource/NNI-2021-Strategic-Plan.pdf.

[10] DOE Office of Energy Efficiency and Renewable Energy. "Department of Energy Seeks Input for a New Clean Energy Manufacturing Institute to Catalyze Industrial Decarbonization." https://www.energy.gov/eere/articles/department-energy-seeks-input-new-clean-energy-manufacturing-institute-catalyze.

[11] National Nanotechnology Initiative. "NNI Budget Supplements and Strategic Plans." https://www.nano.gov/NNIBudgetSupplementsandStrategicPlans.

[12] White, Ashley. “The Materials Genome Initiative: One Year on.” *MRS Bulletin* 37, no. 8 (2012): 715–16. https://doi.org/10.1557/mrs.2012.194. https://link.springer.com/article/10.1557/mrs.2012.194.

[13] Manufacturing USA. “Institutes.” https://www.manufacturingusa.com/institutes.

[14] National Institute of Standards and Technology. “Manufacturing USA Highlights Report.” Washington, DC, 2021. https://nvlpubs.nist.gov/nistpubs/ams/NIST.AMS.600-9.pdf.

[15] National Quantum Initiative. “Getting the Science Right.” https://www.quantum.gov/science/.

[16] National Quantum Initiative. “Large QIS Efforts.” https://www.quantum.gov/action/large-qis-efforts/.

[17] Consolidated Appropriations Act, 2021. H.R.133. U.S. Congress. December 27, 2020. https://www.congress.gov/bill/116th-congress/house-bill/133/text.

[18] Congressional Research Service. “Section 232 of the Trade Expansion Act of 1962.” https://crsreports.congress.gov/product/pdf/IF/IF10667.

[19] U.S. Census Bureau. “North American Industry Classification System (NAICS).” https://www.census.gov/naics/.

[20] NAATBatt International. “Members.” https://naatbatt.org/members/.

[21] U.S. Advanced Ceramics Association. “USACA Members.” https://advancedceramics.org/usaca-members/.

[22] Metal Powder Industries Federation. “Refractory Metals Association.” https://my.mpif.org/MPIF/Associations/RMA.

[23] Semiconductor Industry Association. “SIA Members.” https://www.semiconductors.org/about/members/.

[24] Defense Innovation Marketplace. “Materials & Manufacturing Processes (M&MP).” https://defenseinnovationmarketplace.dtic.mil/communities-of-interest/materials-manufacturing-processes-mmp/.

[25] Administrative Conference of the United States. “Public-Private Partnerships.” https://www.acus.gov/recommendation/public-private-partnerships.

[26] Advanced Functional Fabrics of America. “AFFOA.” https://affoa.org/.

[27] AIM Photonics. “AIM Photonics.” https://www.aimphotonics.com/.

[28] America Makes. “America Makes.” https://www.americamakes.us/.

[29] Advanced Robotics for Manufacturing Institute. “ARM Institute.” https://arminstitute.org/.

[30] Advanced Regenerative Manufacturing Institute. “BioFabUSA.” https://www.armiusa.org/.

[31] Bioindustrial Manufacturing and Design Ecosystem. “BioMADE.” https://www.biomade.org/.

[32] The Institute for Advanced Composites Manufacturing. “IACMI.” https://iacmi.org/.

[33] Lightweight Innovations for Tomorrow. “LIFT.” https://lift.technology/.

[34] NextFlex. “NextFlex.” https://www.nextflex.us/.

[35] PowerAmerica. “PowerAmerica: Accelerating the Next Generation of Power Electronics.” https://poweramericainstitute.org/.

[36] REMADE Institute. “REMADE Institute: Accelerating the Transition to a Circular Economy.” https://remadeinstitute.org/.

[37] National Center for Defense Manufacturing and Machining. “Home.” https://www.ncdmm.org/.

[38] Medical Device Innovation Consortium. “History.” https://mdic.org/about/history/.

[39] National Institutes of Health (NIH), National Cancer Institute. “Nanotechnology Characterization Laboratory.” https://www.cancer.gov/nano/research/ncl.

[40] Commonwealth Center for Advanced Manufacturing. “About Commonwealth Center for Advanced Manufacturing.” https://ccam-va.com/about-ccam/.

[41] The Materials Project. “About the Materials Project.” https://materialsproject.org/about.

[42] Ye, Weike, Chi Chen, Shyam Dwaraknath, Anubhav Jain, Shyue Ping Ong, and Kristin A. Persson. “Harnessing the Materials Project for Machine-Learning and Accelerated Discovery.” *MRS Bulletin* 43, no. 9 (2018): 664–69. https://doi.org/10.1557/mrs.2018.202. https://link.springer.com/article/10.1557/mrs.2018.202.

[43] DOE Office of Energy Efficiency and Renewable Energy. “Energy Materials Network.” https://www.energy.gov/eere/energy-materials-network/energy-materials-network.

[44] Department of Energy. “Hubs.” https://www.energy.gov/science-innovation/innovation/hubs.

[45] Liquid Sunlight Alliance. “Liquid Sunlight Alliance.” https://www.liquidsunlightalliance.org/.

[46] Center for Hybrid Approaches in Solar Energy to Liquid Fuels. “CHASE Mission.” https://solarhub.unc.edu/.

[47] Joint Center for Energy Storage Research. “About JCESR.” https://www.jcesr.org/about/.

[48] Critical Materials Institute. “CMI Partners.” https://www.ameslab.gov/cmi/cmi-partners.

[49] National Alliance for Water Innovation. “National Alliance for Water Innovation.” https://www.nawihub.org/.

[50] The Quantum Economic Development Consortium. “QED-C Members.” https://quantumconsortium.org/members/.

[51] The Quantum Economic Development Consortium. “Home.” https://quantumconsortium.org/.

[52] Purdue University. “Purdue Hypersonics Combines Industry, Academia in New Materials and Manufacturing Center.” https://www.purdue.edu/newsroom/releases/2022/Q1/purdue-hypersonics-combines-industry,-academia-in-new-materials-and-manufacturing-center.html.

[53] Oak Ridge National Laboratory. “User Facilities.” https://www.ornl.gov/content/user-facilities.

[54] Andersen, Casper W., Rickard Armiento, Evgeny Blokhin, Gareth J. Conduit, Shyam Dwaraknath, Matthew L. Evans, and Ádám Fekete et al. “OPTIMADE, an API for Exchanging Materials Data.” *Scientific Data* 8, no. 1 (2021): 217. https://doi.org/10.1038/s41597-021-00974-z. https://www.nature.com/articles/s41597-021-00974-z.

[55] Open Databases Integration for Materials Design. “Open Databases Integration for Materials Design (OPTIMADE).” https://www.optimade.org/.

[56] Rubadue, Jana. “Metallic Materials Properties Development and Standardization (MMPDS).” https://mmpds.org/wp-content/uploads/2015/03/mmpds_2015_overview_presentation.pdf.

[57] CMH-17 Composite Materials Handbook. “About CMH-17.” https://www.cmh17.org/.

[58] CMH-17 Composite Materials Handbook. “Composite Materials Handbook Organization.” https://www.cmh17.org/HOME/Organization.

[59] SAE International. “AMS P17 Polymer Matrix Composites Committee.” https://standardsworks.sae.org/standards-committees/ams-p17-polymer-matrix-composites-committee.

[60] National Institute for Aviation Research. “National Center for Advanced Materials Performance.” https://www.wichita.edu/industry_and_defense/NIAR/Research/ncamp.php.

[61] The Minerals, Metals, and Materials Society. “The Minerals, Metals, and Materials Society.” https://www.tms.org/.

[62] American Institute of Chemical Engineers. “The Global Home of Chemical Engineers.” https://www.aiche.org/.

[63] The American Chemical Society. “The American Chemical Society.” https://www.acs.org/content/acs/en.html.

[64] American Ceramic Society. “American Ceramic Society.” https://ceramics.org/.

[65] American Physical Society. “Division of Materials Physics.” https://engage.aps.org/dmp/home.

[66] Materials Research Society. “Materials Research Society.” https://www.mrs.org/.

[67] ASM International. “ASM International.” https://www.asminternational.org/.

[68] ASM International. “Data Ecosystem: Enhancing Materials Performance.” https://www.asminternational.org/data-ecosystem.

[69] National Academies of Sciences, Engineering, and Medicine. “National Materials and Manufacturing Board.” https://www.nationalacademies.org/nmmb/national-materials-and-manufacturing-board.

[70] U.S. Chamber of Commerce. “Chamber Technology Engagement Center.” https://www.uschamber.com/program/chamber-technology-engagement-center.

[71] Office of Management and Budget. “OMB Circular a-119: Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities.” https://www.whitehouse.gov/wp-content/uploads/2020/07/revised_circular_a-119_as_of_1_22.pdf.

[72] International Standards Organization. “Standards.” https://www.iso.org/standards.html.

[73] American National Standards Institute. “ANSI's Roles.” https://www.ansi.org/about/roles.

[74] ASTM International. “Standards & Publications.” https://www.astm.org/products-services/standards-and-publications.html.

[75] American Society of Mechanical Engineers. “Find a Standard.” https://www.asme.org/codes-standards/find-codes-standards.

[76] Versailles Project on Advanced Materials and Standards. “Steering Committee Representatives.” http://www.vamas.org/contacts/representatives.html.

[77] Versailles Project on Advanced Materials and Standards. “VAMAS Formation and Objectives.” http://www.vamas.org/formation.html.
[78] American Welding Society. “Standards.” https://www.aws.org/standards/page/home.
[79] AIAA Aerospace Research Central. “Browse Standards.” https://arc.aiaa.org/action/showPublications?pubType=standards.
[80] IEEE Standards Association. “Standards.” https://standards.ieee.org/standard/.
[81] SAE International. “SAE Standards Development.” https://www.sae.org/standards/development.
[82] SEMI. “Electronic Materials Group.” https://www.semi.org/en/communities/emg.
[83] American Physical Society. “Division on Soft Matter.” https://engage.aps.org/dsoft/home.
[84] 3DExperience. “3DExperience Edu Centers of Excellence.” https://edu.3ds.com/en/edu-centers.
[85] Bureau of Industry and Security. “Bureau of Industry and Security Website.” https://bis.doc.gov/.
[86] U.S. Consumer Product Safety Commission. “Regulations, Laws & Standards.” https://www.cpsc.gov/Regulations-Laws--Standards.
[87] Materials Genome Initiative. “National Security.” https://www.mgi.gov/national-objectives/national-security.
[88] DOE Office of Energy Efficiency and Renewable Energy. “Advanced Manufacturing: Next Generation Materials.” https://www.energy.gov/eere/amo/next-generation-materials.
[89] DOE Office of Science. “Materials Sciences and Engineering (MSE) Division.” https://science.osti.gov/bes/mse.
[90] Bureau of Land Management. “Mining and Minerals: About Mining and Minerals.” https://www.blm.gov/programs/energy-and-minerals/mining-and-minerals/about.
[91] U.S. Department of State. “Directorate of Defense Trade Controls Public Portal.” https://www.pmddtc.state.gov/ddtc_public.
[92] U.S. Environmental Protection Agency. “Research on Nanomaterials.” https://www.epa.gov/chemical-research/research-nanomaterials.
[93] U.S. Federal Aviation Administration. “FAA Air Transportation Centers of Excellence.” https://www.faa.gov/about/office_org/headquarters_offices/ang/grants/coe.
[94] U.S. Food and Drug Administration. “Nanotechnology Programs at FDA.” https://www.fda.gov/science-research/science-and-research-special-topics/nanotechnology-programs-fda.
[95] Federal Highway Administration. “Exploratory Advanced Research Overview.” https://highways.dot.gov/research/research-programs/exploratory-advanced-research/exploratory-advanced-research-overview.
[96] National Academies of Sciences, Engineering, and Medicine. “National Cooperative Highway Research Program 2022 Annual Report.” https://onlinepubs.trb.org/onlinepubs/nchrp/nchrpannual2022.pdf.
[97] National Aeronautics and Space Administration. “NASA Technology Transfer Program: Eight Disruptive NASA Materials and Coatings Technologies Ready for

Commercialization." https://technology.nasa.gov/page/eight-disruptive-nasa-materials-and.

[98] Federal Motor Vehicle Safety Standards. Title 49 Part 571. U.S. Department of Transportation. 2022. https://www.ecfr.gov/current/title-49/subtitle-B/chapter-V/part-571.

[99] National Institute of Environmental Health Sciences. "Nano Environmental Health and Safety (Nano EHS)." https://www.niehs.nih.gov/research/supported/exposure/nanohealth/index.cfm.

[100] National Nanotechnology Initiative. "NNI R&D User Facilities." https://www.nano.gov/userfacilities.

[101] National Institute for Occupational Safety and Health. "Advanced Manufacturing." https://www.cdc.gov/niosh/topics/advancedmnf/default.html.

[102] National Institute of Standards and Technology. "Materials." https://www.nist.gov/materials.

[103] U.S. Nuclear Regulatory Commission. "How We Regulate." https://www.nrc.gov/about-nrc/regulatory.html.

[104] National Science Foundation. "Division of Materials Research (DMR)." https://www.nsf.gov/div/index.jsp?div=DMR.

[105] Occupational Safety and Health Administration. "Chemical Hazards and Toxic Substances." https://www.osha.gov/chemical-hazards.

[106] Occupational Safety and Health Administration. "Nanotechnology." https://www.osha.gov/nanotechnology.

[107] U.S. Department of Transportation. "Pipeline and Hazardous Materials Safety Administration (PHMSA) Mission." https://www.phmsa.dot.gov/about-phmsa/phmsas-mission.

[108] U.S. Forest Service. "Energy." https://www.fs.usda.gov/science-technology/energy-forest-products/energy.

[109] USDA Agricultural Research Service. "Manuscripts by Strategic Topical Areas." https://www.ars.usda.gov/research/manuscripts-by-strategic-topical-areas/?stpCode=4111.

[110] U.S. Department of Transportation. "University Transportation Centers." https://www.transportation.gov/content/university-transportation-centers.

[111] White House Office of Science and Technology Policy. "The Potential Role of ARPA-I in Accelerating the Net-Zero Game Changers Initiative." *The White House*, December 7, 2022. https://www.whitehouse.gov/ostp/news-updates/2022/12/07/the-potential-role-of-arpa-i-in-accelerating-the-net-zero-game-changers-initiative/.

[112] U.S. Geological Survey. "Energy and Minerals." https://www.usgs.gov/mission-areas/energy-and-minerals.

[113] Bureau of Industry and Security. "Policy Guidance." https://www.bis.doc.gov/index.php/policy-guidance.

[114] Bureau of Industry and Security. "Compliance & Training." https://www.bis.doc.gov/index.php/compliance-a-training.

[115] Bureau of Industry and Security. "Technical Advisory Committees (TAC)." https://tac.bis.doc.gov/.

[116] Bureau of Industry and Security. "Deemed Exports." https://www.bis.doc.gov/index.php/policy-guidance/deemed-exports.

[117] MIT Institute for Soldier Nanotechnologies. “MIT Institute for Soldier Nanotechnologies.” https://isn.mit.edu/.

[118] Center for Materials in Extreme Dynamic Environments. “Center for Materials in Extreme Dynamic Environments.” https://hemi.jhu.edu/cmede/.

[119] Center for Research in Extreme Batteries. “Center for Research on Extreme Batteries.” https://creb.umd.edu/.

[120] Department of Defense. “Directive: DoD Airworthiness Policy.” https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/503061p.pdf.

[121] Department of Defense. “MIL-HDBK-516 Airworthiness Certification Criteria.” https://quicksearch.dla.mil/qsDocDetails.aspx?ident_number=212162.

[122] Department of Defense Manufacturing Technology Program. “DoD ManTech at the 2021 Defense Manufacturing Conference!.” https://www.dodmantech.mil/News/News-Display/Article/2873075/dod-mantech-at-the-2021-defense-manufacturing-conference/.

[123] Department of Defense (DOD) Manufacturing Technology Program. “Joint Defense Manufacturing Technology Panel (JDMTP).” https://www.dodmantech.mil/JDMTP/.

[124] DOE Office of Science. “Energy Frontier Research Centers.” https://science.osti.gov/bes/efrc.

[125] DOE Office of Science. “EFRC Centers.” https://science.osti.gov/bes/efrc/Centers.

[126] DOE Office of Energy Efficiency & Renewable Energy. “About the AMO Restructure.” https://www.energy.gov/eere/amo/about-amo-restructure.

[127] DOE Office of Energy Efficiency & Renewable Energy. “Advanced Materials and Manufacturing Technologies Office (AMMTO).” https://www.energy.gov/eere/amo/advanced-materials-and-manufacturing-technologies-office.

[128] Advanced Research Project Agency - Energy. “Exploratory Topics.” https://arpa-e.energy.gov/technologies/exploratory-topics.

[129] ReCell. “The ReCell Center.” https://recellcenter.org/.

[130] DOE Office of Energy Efficiency and Renewable Energy. “U.S. DRIVE.” https://www.energy.gov/eere/vehicles/us-drive.

[131] Department of Energy. “Small Business Vouchers.” https://www.energy.gov/eere/solar/small-business-voucher-pilot-program.

[132] U.S. Department of State. “Conduct Business - Directorate of Defense Trade Controls Public Portal.” https://www.pmddtc.state.gov/ddtc_public?id=ddtc_public_portal_business_landing.

[133] U.S. Department of State. “The Defense Trade Advisory Groups (DTAG) - Directorate of Defense Trade Controls Public Portal.” https://www.pmddtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=1902fc7bdbb8d300d0a370131f9619eb.

[134] U.S. Food and Drug Administration. “FDA Participates in New ‘Collaborative Communities’ to Address Emerging Challenges in Medical Devices.” https://www.fda.gov/news-events/press-announcements/fda-participates-new-collaborative-communities-address-emerging-challenges-medical-devices.

[135] U.S. Food and Drug Administration. “Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) Action Plan.” January 2021. https://www.fda.gov/media/145022/download.

[136] U.S. Food and Drug Administration. “Collaborative Communities: Addressing Health Care Challenges Together.” https://www.fda.gov/about-fda/cdrh-strategic-priorities-and-updates/collaborative-communities-addressing-health-care-challenges-together.

[137] ASTM International Additive Manufacturing Center of Excellence. “Additive Manufacturing Center of Excellence.” https://amcoe.org/.

[138] Auburn University. “National Center for Additive Manufacturing Excellence.” https://www.eng.auburn.edu/research/centers/additive/index.html.

[139] NASA Aeronautics Research Mission Directorate. “Hi-Rate Composite Aircraft Manufacturing (HiCAM) Project.” https://www.nasa.gov/aeroresearch/programs/aavp/hicam.

[140] National Institutes of Health. “Mission and Goals.” https://www.nih.gov/about-nih/what-we-do/mission-goals.

[141] National Institute of Standards and Technology. “Materials Genome Initiative.” https://www.nist.gov/mgi.

[142] National Institute of Standards and Technology. “NIST Awards Funding to Strengthen Advanced Manufacturing for Microelectronics, Digital and Biomanufacturing.” https://www.nist.gov/news-events/news/2022/04/nist-awards-funding-strengthen-advanced-manufacturing-microelectronics.

[143] National Science Foundation. “Materials Innovation Platforms (MIP).” https://beta.nsf.gov/funding/opportunities/materials-innovation-platforms-mip.

[144] National Science Foundation. “Grant Opportunities for Academic Liaison with Industry (GOALI) Proposal.” https://www.nsf.gov/eng/eec/goali.jsp.

[145] U.S. Geological Survey. “Mission Areas.” https://www.usgs.gov/science/mission-areas.

[146] National Research Council. *Integrated Computational Materials Engineering: A Transformational Discipline for Improved Competitiveness and National Security*. Washington D.C.: National Academies Press, 2008. https://doi.org/10.17226/12199. https://nap.nationalacademies.org/catalog/12199/integrated-computational-materials-engineering-a-transformational-discipline-for-improved-competitiveness.

[147] The Minerals, Metals, and Materials Society. “Integrated Computational Materials Engineering (ICME): Implementing ICME in the Aerospace, Automotive, and Maritime Industries.” https://www.tms.org/portal/Publications/Studies/ICME_Implementation_Study.aspx .

[148] Materials Genome Initiative. “Materials Genome Initiative.” https://www.mgi.gov/.

[149] National Nanotechnology Initiative. “NNI Vision and Goals.” Accessed April 21, 2022. https://www.nano.gov/about-nni/what/vision-goals.

[150] National Quantum Coordination Office. “National Quantum Initiative.” https://www.quantum.gov/wp-content/uploads/2022/04/NQI-Factsheet.pdf.

[151] National Quantum Initiative. “About the National Quantum Initiative.” https://www.quantum.gov/about/.

[152] National Quantum Coordination Office. “Quantum Frontiers: Report on Community Input to the Nation's Strategy for Quantum Information Science.” https://www.quantum.gov/wp-content/uploads/2020/10/QuantumFrontiers.pdf.

[153] Nekuda Malik, Jennifer A. “US Interagency Meeting for Materials Science Enhances Research Coordination.” *MRS Bulletin* 42, no. 05 (2017): 339–40. https://doi.org/10.1557/mrs.2017.100. https://link.springer.com/article/10.1557/mrs.2017.100.

[154] Air Force Research Lab. “AFRL Researchers Partner with National Science Foundation Awardees on Advanced Materials Research.” https://afresearchlab.com/news/afrl-researchers-partner-with-national-science-foundation-awardees-on-advanced-materials-research/.

[155] DOE Office of Energy Efficiency and Renewable Energy. “Federal Consortium for Advanced Batteries (FCAB).” https://www.energy.gov/eere/vehicles/federal-consortium-advanced-batteries-fcab.

[156] DOE Office of Energy Efficiency and Renewable Energy. “National Blueprint for Lithium Batteries.” https://www.energy.gov/eere/vehicles/articles/national-blueprint-lithium-batteries.

[157] Federal Consortium for Advanced Batteries. “Pre-Application Battery Test Manual.” https://cet.inl.gov/ArticleDocuments/FCABManualRev1Final.pdf.

[158] National Institute of Standards and Technology. “MATES.” https://www.nist.gov/mml/bbd/interagency-coordination/mates.

[159] National Science and Technology Council (NSTC), Multi-Agency Tissue Engineering Science. “Advancing Tissue Science and Engineering.” National Science and Technology Council (NSTC), Multi-Agency Tissue Engineering Science (MATES), Washington, DC, June 2007. https://files.givewell.org/files/labs/animal-product-replacements/advancing_tissue_science_and_engineering.pdf.

[160] National Institute for Aviation Research. “About.” https://www.wichita.edu/industry_and_defense/NIAR/about-us.php.

[161] Waggoner, Edgar G. “Explore Flight - FAA REDAC Briefing.” https://www.faa.gov/about/office_org/headquarters_offices/ang/redac/media/full/2021/oct/fullComm-Oct2021-211020REDACDr_Waggoner.pdf.

[162] Bureau of Industry and Security. “Export Administration Regulations (EAR).” https://bis.doc.gov/index.php/regulations/export-administration-regulations-ear.

[163] Bureau of Industry and Security. “Commerce Control List (CCL).” https://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl.

[164] Department of Defense. “Defense Standardization Program Specifications and Standards.” https://www.dsp.dla.mil/Specs-Standards/.

[165] Army Public Health Center. “Hexavalent Chromium.” https://phc.amedd.army.mil/topics/workplacehealth/ih/Pages/Cr6.aspx.

[166] U.S. Environmental Protection Agency. “Clean Air Act Guidelines and Standards for Solvent Use and Surface Coating Industry.” https://www.epa.gov/stationary-sources-air-pollution/clean-air-act-guidelines-and-standards-solvent-use-and-surface.

[167] Department of Energy. “Standards.” https://www.standards.doe.gov/standards-browse.

[168] U.S. Environmental Protection Agency. “Control of Nanoscale Materials Under the Toxic Substances Control Act.” https://www.epa.gov/reviewing-new-chemicals-under-toxic-substances-control-act-tsca/control-nanoscale-materials-under.

[169] U.S. Environmental Protection Agency. “Technical Fact Sheet – Nanomaterials.” https://www.epa.gov/sites/default/files/2014-03/documents/ffrrofactsheet_emergingcontaminant_nanomaterials_jan2014_final.pdf.

[170] International Standards Organization. “ISO/TC 229 - Nanotechnologies.” https://www.iso.org/committee/381983.html.

[171] Composite Materials Handbook-17. “CMH-17 Composite Materials Handbook.” https://www.cmh17.org/.

[172] Federal Aviation Administration. “Memorandum: Acceptance of Composite Specifications and Design Values Developed Using the NCAMP Process.” https://www.wichita.edu/industry_and_defense/NIAR/Documents/FAA-AIR-100-2010-120-003.pdf.

[173] U.S. Federal Aviation Administration. “Dynamic Regulatory System.” https://drs.faa.gov/browse.

[174] U.S. Food and Drug Administration. “Determining the Regulatory Status of Components of a Food Contact Material.” https://www.fda.gov/food/packaging-food-contact-substances-fcs/determining-regulatory-status-components-food-contact-material.

[175] U.S. Food and Drug Administration. “FDA’s Approach to Regulation of Nanotechnology Products.” https://www.fda.gov/science-research/nanotechnology-programs-fda/fdas-approach-regulation-nanotechnology-products.

[176] U.S. Food and Drug Administration. “Nanotechnology Task Force Report 2007.” https://www.fda.gov/science-research/nanotechnology-programs-fda/nanotechnology-task-force-report-2007.

[177] U.S. Food and Drug Administration. “Nanotechnology Guidance Documents.” Accessed June 30, 2022. https://www.fda.gov/science-research/nanotechnology-programs-fda/nanotechnology-guidance-documents.

[178] U.S. Food and Drug Administration. “2013 Nanotechnology Regulatory Science Research Plan.” https://www.fda.gov/science-research/nanotechnology-programs-fda/2013-nanotechnology-regulatory-science-research-plan.

[179] U.S. Food and Drug Administration. “Safety of Metals and Other Materials Used in Medical Devices.” https://www.fda.gov/medical-devices/products-and-medical-procedures/safety-metals-and-other-materials-used-medical-devices.

[180] International Standards Organization. “Biological Evaluation of Medical Devices — Part 1: Evaluation and Testing Within a Risk Management Process (ISO 10993-1:2018).” https://www.iso.org/standard/68936.html.

[181] U.S. Food and Drug Administration. “Use of International Standard ISO 10993-1, "Biological Evaluation of Medical Devices - Part 1: Evaluation and Testing Within a Risk Management Process".” https://www.fda.gov/regulatory-information/search-fda-guidance-documents/use-international-standard-iso-10993-1-biological-evaluation-medical-devices-part-1-evaluation-and.

[182] U.S. Food and Drug Administration. “Conveying Materials Information About Medical Devices to Patients and Healthcare Providers: Considerations for a Framework.” May 20, 2021. https://www.fda.gov/media/148860/download.

[183] U.S. Food and Drug Administration. “Medical Device Material Safety Summaries: ECRI Reports.” https://www.fda.gov/medical-devices/science-and-research-medical-devices/medical-device-material-safety-summaries-ecri-reports.

[184] U.S. Food and Drug Administration. “Code of Federal Regulations Title 21 - Food and Drugs.” https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=872.

[185] U.S. Food and Drug Administration. “Recognized Consensus Standards.” https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfStandards/search.cfm.

[186] U.S. Food and Drug Administration. “Medical Device Databases.” https://www.fda.gov/medical-devices/device-advice-comprehensive-regulatory-assistance/medical-device-databases.

[187] U.S. Food and Drug Administration. “Safety and Performance Based Pathway: Guidance for Industry and Food and Drug Administration.” https://www.fda.gov/media/112691/download.

[188] International Standards Organization. “Medical Electrical Equipment — Part 1-11: General Requirements for Basic Safety and Essential Performance — Collateral Standard: Requirements for Medical Electrical Equipment and Medical Electrical Systems Used in the Home Healthcare Environment (IEC 60601-1-11:2015).” https://www.iso.org/standard/65529.html.

[189] National Aeronautics and Space Administration (NASA), Office of the NASA Chief Engineer. “NASA Technical Standards.” https://standards.nasa.gov/nasa-technical-standards.

[190] National Aeronautics and Space Administration (NASA), Office of the NASA Chief Engineer. “6000 - Materials and Processes, Parts.” https://standards.nasa.gov/materials-and-processes-parts.

[191] National Aeronautics and Space Administration (NASA), Office of the NASA Chief Engineer. “Standard Materials and Processes Requirements for Spacecraft.” https://standards.nasa.gov/standard/NASA/NASA-STD-6016.

[192] National Aeronautics and Space Administration (NASA), Office of the NASA Chief Engineer. “Fracture Control Requirements for Spaceflight Hardware.” https://standards.nasa.gov/standard/nasa/nasa-std-5019.

[193] National Institutes of Health. “NOT-OD-21-013: Final NIH Policy for Data Management and Sharing.” https://grants.nih.gov/grants/guide/notice-files/NOT-OD-21-013.html.

[194] National Science Foundation. “Materials Research Science and Engineering Centers.” https://mrsec.org/.

[195] ASTM International. “Reading Room.” https://www.astm.org/products-services/reading-room.html.

[196] ASTM International. “Committee E56 on Nanotechnology.” https://www.astm.org/get-involved/technical-committees/committee-e56.

[197] ASTM International. “Committee E56 Subcommittees.” https://www.astm.org/get-involved/technical-committees/committee-e56/subcommittee-e56.

[198] ASTM International. “Committee C28 on Advanced Ceramics.” https://www.astm.org/get-involved/technical-committees/committee-c28.

[199] ASTM International. “Committee C28 Subcommittees.” https://www.astm.org/get-involved/technical-committees/committee-c28/subcommittee-c28.

[200] ASTM International. “Committee D30 on Composite Materials.” https://www.astm.org/get-involved/technical-committees/committee-d30.

[201] ASTM International. “Committee D30 Subcommittees.” https://www.astm.org/get-involved/technical-committees/committee-d30/subcommittee-d30.

[202] ASTM International. “Committee B09 on Metal Powders and Metal Powder Products.” https://www.astm.org/get-involved/technical-committees/committee-b09.

[203] ASTM International. “Committee B09 Subcommittees.” https://www.astm.org/get-involved/technical-committees/committee-b09/subcommittee-b09.

[204] ASTM International. “Committee B08 on Metallic and Inorganic Coatings.” https://www.astm.org/get-involved/technical-committees/committee-b08.

[205] ASTM International. “Committee B08 Subcommittees.” https://www.astm.org/get-involved/technical-committees/committee-b08/subcommittee-b08.

[206] ASTM International. “Committee E44 on Solar, Geothermal and Other Alternative Energy Sources.” https://www.astm.org/get-involved/technical-committees/committee-e44.

[207] ASTM International. “Committee E44 Subcommittees.” https://www.astm.org/get-involved/technical-committees/committee-e44/subcommittee-e44.

[208] ASTM International. “Committee D20 on Plastics.” https://www.astm.org/get-involved/technical-committees/committee-d20.

[209] ASTM International. “Committee D20 Subcommittees.” https://www.astm.org/get-involved/technical-committees/committee-d20/subcommittee-d20.

[210] ASTM International. “Committee F42 Subcommittees.” https://www.astm.org/get-involved/technical-committees/committee-f42/subcommittee-f42.

[211] Institute of Electrical and Electronics Engineers. “IEEE 1906.1-2015 - IEEE Recommended Practice for Nanoscale and Molecular Communication Framework.” https://standards.ieee.org/ieee/1906.1/5171/.

[212] Institute of Electrical and Electronics Engineers. “Standard for 3D Body Processing.” https://standards.ieee.org/standard/.

[213] Institute of Electrical and Electronics Engineers. “IEEE International Roadmap for Devices and Systems.” https://irds.ieee.org/.

[214] Versailles Project on Advanced Materials and Standards. “Technical Working Areas.” http://www.vamas.org/twa.html.

[215] The Standards Coordinating Body for Regenerative Medicine. “Community Perspectives: Needed Standards in Regenerative Medicine.” December 2020. https://static1.squarespace.com/static/58a331b0db29d63c7fb64528/t/5fdcd93257b8971cd7ab4ef2/1608309045242/NeededStandardsReportDecember2020.pdf.

[216] The Standards Coordinating Body for Regenerative Medicine. “The Standards Coordinating Body for Regenerative Medicine.” https://www.standardscoordinatingbody.org/.

[217] DOE Office of Science. “Definition.” https://science.osti.gov/User-Facilities/Policies-and-Processes/Definition.

[218] DOE Office of Science. “User Facilities: Definition.” https://science.osti.gov/User-Facilities/Policies-and-Processes/Definition.

[219] National Institute for Occupational Safety and Health. “Nanotechnology: Guidance and Publications.” https://www.cdc.gov/niosh/topics/nanotech/pubs.html.

[220] National Institute for Occupational Safety and Health. “Nanotechnology Research Center.” https://www.cdc.gov/niosh/programs/nano/default.html.

[221] National Institute for Occupational Safety and Health. “Additive Manufacturing/3D Printing.” https://www.cdc.gov/niosh/topics/advancedmnf/additivemnf.html.

[222] National Institute for Occupational Safety and Health. “NIOSH Pocket Guide to Chemical Hazards (2005-149).” https://www.cdc.gov/niosh/docs/2005-149/pdfs/2005-149.pdf.

[223] National Institute of Standards and Technology. “Materials Resource Registry.” https://materials.registry.nist.gov/.

[224] National Institute of Standards and Technology. “Materials Data Resources.” https://www.nist.gov/mgi/materials-data-resources.

[225] National Institute of Standards and Technology. “Standard Reference Materials.” https://www.nist.gov/srm.

[226] Federal Aviation Administration. “William J. Hughes Technical Center |.” https://www.faa.gov/about/office_org/headquarters_offices/ang/offices/tc.

[227] United States Patent and Trademark Office. “Patent Public Search | USPTO.” https://ppubs.uspto.gov/pubwebapp/static/pages/landing.html.

[228] DOE Office of Science. “User Facilities at a Glance.” https://science.osti.gov/User-Facilities/User-Facilities-at-a-Glance.

[229] DOE Office of Science. “Nanoscale Science Research Centers.” https://nsrcportal.sandia.gov/.

[230] National Nanotechnology Coordinated Infrastructure. “NNCI: National Nanotechnology Coordinated Infrastructure.” https://nnci.net/.

[231] National Science Foundation. “Science and Technology Centers (STCs).” https://www.nsf.gov/od/oia/programs/stc/.

[232] National Science Foundation. “Award #1231319 - Center for Integrated Quantum Materials.” https://www.nsf.gov/awardsearch/showAward?AWD_ID=1231319&HistoricalAwards=false.

[233] National Science Foundation. “Award #2019444 - STC: Center for Integration of Modern Optoelectronic Materials on Demand.” https://www.nsf.gov/awardsearch/showAward?AWD_ID=2019444&HistoricalAwards=false.

[234] National Institute of Standards and Technology. “Center for High Resolution Neutron Scattering.” https://www.nist.gov/ncnr/chrns.

[235] National Institute of Standards and Technology. “Center for Nanoscale Science and Technology.” https://www.nist.gov/cnst.

[236] Cornell High Energy Synchrotron Source. “Materials Solutions Network at CHESS (MSN-C).” https://www.chess.cornell.edu/partners/msn-c.

[237] DOE Office of Science. “Computational Materials Science Awards 2016 FOA.” https://science.osti.gov/bes/Funding-Opportunities/Closed-FOAs/Computational-Materials-Sciences-Awards-2016-FOA.

[238] Center for Computational Study of Excited-State Phenomena in Energy Materials. "C2SEPEM: Center for Computational Study of Excited-State Phenomena in Energy Materials." https://c2sepem.lbl.gov/.

[239] Center for Predictive Simulation of Functional Materials. "CPSFM: Center for Predictive Simulation of Functional Materials." https://cpsfm.ornl.gov/.

[240] Midwest Integrated Center for Computational Materials. "MICCo: Midwest Integrated Center for Computational Materials." http://www.miccom-center.org/.

[241] Center for Computational Material Spectroscopy and Design. "COMSCOPE: Center for Computational Material Spectroscopy and Design." https://www.bnl.gov/comscope/.

[242] Office of Science Programs at LLNL. "Center for Non-Perturbative Studies of Functional Materials Under Non-Equilibrium Conditions." https://sc-programs.llnl.gov/basic-energy-science-at-llnl/npneq.

[243] Center for Hierarchical Materials Design. "CHiMaD: Center for Hierarchical Materials Design." https://chimad.northwestern.edu/.

[244] The Molecular Sciences Software Institute. "MolSSI: The Molecular Sciences Software Institute." https://molssi.org/.

[245] National Science Foundation. "Award # 2136142 - S2I2: Impl: The Molecular Sciences Software Institute." https://www.nsf.gov/awardsearch/showAward?AWD_ID=2136142.

[246] Science Gateways Community Initiative. "Science Gateways Community Initiative." https://sciencegateways.org/.

[247] Network for Computational Nanotechnology. "Network for Computational Nanotechnology." https://nanohub.org/groups/ncn/.

[248] Engineered nanoBIO. "Engineered NanoBIO." https://nanohub.org/groups/nanobio.

[249] Nanomanufacturing. "NanoMFG." https://nanohub.org/groups/nanomfg.

[250] Energy Act of 2020. U.S. Congress. 12/2020. https://science.house.gov/imo/media/doc/Energy%20Act%20of%202020.pdf.

[251] U.S. Geological Survey. "U.S. Geological Survey Releases 2022 List of Critical Minerals." https://www.usgs.gov/news/national-news-release/us-geological-survey-releases-2022-list-critical-minerals.

[252] Government Accountability Office. "Critical Minerals: Building on Federal Efforts to Advance Recovery and Substitution Could Help Address Supply Risks." https://www.gao.gov/products/gao-22-104824.

[253] Executive Office of the President. "Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth: 100-Day Reviews Under Executive Order 14017." The White House, Washington DC, June 2021. https://www.whitehouse.gov/wp-content/uploads/2021/06/100-day-supply-chain-review-report.pdf.

[254] Naresh, C., P. S. C. Bose, and C. S. P. Rao. "Shape Memory Alloys: A State of Art Review." *IOP Conference Series: Materials Science and Engineering* 149, no. 1 (2016): 12054. https://doi.org/10.1088/1757-899X/149/1/012054. https://iopscience.iop.org/article/10.1088/1757-899X/149/1/012054.

[255] U.S. Food and Drug Administration. "3D Printing Medical Devices at the Point of Care: Discussion Paper." December 10, 2021. https://www.fda.gov/medical-

devices/3d-printing-medical-devices/3d-printing-medical-devices-point-care-discussion-paper.

[256] Cohen, Jennifer, and Yana Meulen van der Rodgers. “Contributing Factors to Personal Protective Equipment Shortages During the COVID-19 Pandemic.” *Preventive Medicine* 141 (2020): 106263. https://doi.org/10.1016/j.ypmed.2020.106263. https://www.sciencedirect.com/science/article/pii/S0091743520302875.

[257] U.S. Department of Commerce. “A Federal Strategy to Ensure Secure and Reliable Supplies of Critical Minerals.” https://www.commerce.gov/data-and-reports/reports/2019/06/federal-strategy-ensure-secure-and-reliable-supplies-critical-minerals.

[258] Department of Energy. “Supply Chain Risk Mitigation for Scientific Facilities and Tools.” 2022. https://science.osti.gov/-/media/bes/pdf/reports/2022/SC_Supply_Chain_rpt.pdf.

[259] Department of Energy. “The Quadrennial Technology Review.” 9/2015. https://www.energy.gov/quadrennial-technology-review-0.

[260] The Economist. “How Chinese Firms Have Changed Africa.” https://www.economist.com/special-report/2022/05/20/how-chinese-firms-have-changed-africa.

[261] Bureau of Industry and Security. “Fact Sheet: Biden-Harris Administration Announces Further Actions to Secure Rare Earth Element Supply Chain: Department of Commerce Findings and Recommendations Build on Progress to Secure Critical Supply Chain, Reduce Dependence on China.” https://www.bis.doc.gov/index.php/documents/section-232-investigations/3142-2022-09-fact-sheet-biden-harris-administration-announces-actions-to-secure-rare-earth-element/file.

[262] The White House. “Memorandum on Presidential Determination Pursuant to Section 303 of the Defense Production Act of 1950, as Amended.” https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/31/memorandum-on-presidential-determination-pursuant-to-section-303-of-the-defense-production-act-of-1950-as-amended/.

[263] United States Department of State. “Minerals Security Partnership - United States Department of State.” https://www.state.gov/minerals-security-partnership/.

[264] United States Department of State. “Minerals Security Partnership Convening Supports Robust Supply Chains for Clean Energy Technologies - United States Department of State.” https://www.state.gov/minerals-security-partnership-convening-supports-robust-supply-chains-for-clean-energy-technologies/.

[265] The European Commission. “Advanced Materials.” https://ec.europa.eu/info/research-and-innovation/research-area/industrial-research-and-innovation/key-enabling-technologies/advanced-materials-and-chemicals_en.

[266] The European Commission. *Materials 2030 Manifesto: Materials 2030 Manifesto*. Paris: OECD, 2022. https://doi.org/10.1787/9789264307452-en. https://ec.europa.eu/info/sites/default/files/research_and_innovation/research_by_area/documents/advanced-materials-2030-manifesto.pdf.

[267] O'Meara, Sarah. “Materials Science Is Helping to Transform China into a High-Tech Economy.” *Nature* 567, no. 7748 (2019): S1-S5.

https://doi.org/10.1038/d41586-019-00885-5. https://www.nature.com/articles/d41586-019-00885-5.

[268] UK Department for Business, Energy & Industrial Strategy. “UK Advanced Materials: Call for Evidence.” https://www.gov.uk/government/consultations/uk-advanced-materials-call-for-evidence/uk-advanced-materials-call-for-evidence.

[269] Gaur, Vishar, Gaiha, and Abinhav. “Building a Transparent Supply Chain.” https://hbr.org/2020/05/building-a-transparent-supply-chain.

[270] Department of Energy. “Critical Minerals and Materials: U.S. Department of Energy’s Strategy to Support Domestic Critical Mineral and Material Supply Chains (FY2021-FY2031).” January 20, 2021. https://www.energy.gov/sites/prod/files/2021/01/f82/DOE%20Critical%20Minerals%20and%20Materials%20Strategy_0.pdf.

[271] Government Accountability Office. “Trends Affecting Government and Society.” https://www.gao.gov/products/gao-22-3sp.

[272] National Academies of Sciences, Engineering, and Medicine. *Building America's Skilled Technical Workforce*. Washington DC: The National Academies Press, 2017. https://doi.org/10.17226/23472. https://nap.nationalacademies.org/catalog/23472/building-americas-skilled-technical-workforce.

[273] Subcommittee on Quantum Information Science under the Committee on Science of the National Science & Technology Council. “Quantum Information Science and Technology Workforce Development National Strategic Plan.” https://www.quantum.gov/wp-content/uploads/2022/02/QIST-Natl-Workforce-Plan.pdf.

Appendix M. Abbreviations

ACA	American COMPETE Act
AECA	Arms Export Control Act
AFFOA	Advanced Functional Fabrics of America
AFRL	Air Force Research Lab
AI	Artificial Intelligence
ALCF	Argonne Leadership Computing Facility
ALS	Advanced Light Source
AM	Additive Manufacturing
AMMTO	Advanced Manufacturing and Materials Technologies Office
ANL	Argonne National Laboratory
ANSI	American National Standards Institute
API	Application Programming Interface
APS	Advanced Photon Source
ARM	Advanced Robotics for Manufacturing
ARPA-E	Advanced Research Projects Agency-Energy
ASME	American Society of Mechanical Engineers
AWS	American Welding Society
BioMADE	Bioindustrial Manufacturing and Design Ecosystem
BIS	Bureau of Industry and Security
BNL	Brookhaven National Laboratory
C_TEC	Chamber of Commerce Technology Engagement Center
CCAM	Commonwealth Center for Advanced Manufacturing
CCCs	Carbon-Carbon Composites
CCL	Commerce Control List
CDRH	Center for Devices and Radiological Health
CECAM	Center of Excellence for Composites and Advanced Materials
CFN	Center for Functional Nanomaterials
CFTF	Carbon Fiber Technology Facility
CHiMaD	Center for Hierarchical Materials Design
CHRNS	Center for High Resolution Neutron Scattering
CINT	Center for Integrated Nanotechnologies
CMCs	Ceramic Matrix Composites
CMEDE	Center for Materials in Extreme Dynamic Environments
CMH-17	Composite Materials Handbook-17
CMS	Critical Minerals Subcommittee
CMSCs	Computational Materials Science Centers
CNM	Center for Nanoscale Materials
CNMS	Center for Nanophase Materials Sciences
CNST	Center for Nanoscale Science and Technology
COE	Center of Excellence
CoI	Community of Interest

CRADAs	Cooperative Research and Development Agreements
CREB	Center for Research in Extreme Batteries
CPSC	Consumer Product Safety Commission
DARPA	Defense Advanced Research Projects Agency
DMC	Defense Manufacturing Conference
DOD	Department of Defense
DOE	Department of Energy
DOS	Department of State
EERE	Energy Efficiency & Renewable Energy
EFRCs	Energy Frontier Research Centers
EMN	Energy Materials Network
EPA	Environmental Protection Agency
ESnet	Energy Sciences Network
FAA	Federal Aviation Administration
FCAB	Federal Consortium for Advanced Batteries
FDA	Food and Drug Administration
FHWA	Federal Highway Administration
FIMaR	Federal Interagency Materials Representatives
FRP	Fiber-reinforced Polymer
FMVSS	Federal Motor Vehicle Safety Standards
GAO	Government Accountability Office
GOALI	Grant Opportunities for Academic Liaison with Industry
HAMTC	Hypersonics Advanced Manufacturing Technology Center
HFIR	High Flux Isotope Reactor
HiCAM	Hi-Rate Composite Aircraft Manufacturing
IACMI	The Institute for Advanced Composites Manufacturing Innovation
ICME	Integrated Computational Materials Engineering
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
ISO	International Organization for Standardization
ITAR	International Traffic in Arms Regulations
JDMTP	Joint Defense Manufacturing Technology Panel
LANL	Los Alamos National Laboratory
LBNL	Lawrence Berkeley National Laboratory
LCLS	LINAC Coherent Light Source
LIFT	Lightweight Innovations for Tomorrow
M&MP	Materials & Manufacturing Processes
MATES	Multi-Agency Tissue Engineering Sciences
MDF	Manufacturing Demonstration Facility
MDIC	Medical Device Innovation Consortium
MDMA	Medical Device Manufacturers Association
MGI	Materials Genome Initiative
MIP	Materials Innovation Platform
ML	Machine Learning
MMCs	Metal Matrix Composites

MII	Materials Innovation Infrastructure
MMPDS	Metallic Materials Properties Development and Standardization
MOFs	Metal-Organic Frameworks
MolSSI	Molecular Sciences Software Institute
MRR	Materials Resource Registry
MRSEC	Materials Research Science and Engineering Center
NAMs	New and Advanced Materials
NASA	National Aeronautics and Space Administration
NASEM	National Academies of Sciences, Engineering, and Medicine
NCAME	National Center for Additive Manufacturing Excellence
NCAMP	National Center for Advanced Materials Performance
NCL	Nanotechnology Characterization Laboratory
NERSC	National Energy Research Scientific Computing Center
NHTSA	National Highway Traffic Safety Administration
NIAR	National Institute for Aviation Research
NIH	National Institutes of Health
NIOSH	National Institute for Occupational Safety and Health
NIST	National Institute of Standards and Technology
NNCI	National Nanotechnology Coordinated Infrastructure
NNI	National Nanotechnology Initiative
NQI	National Quantum Initiative
NQIA	National Quantum Initiative Act
NSF	National Science Foundation
NSLS-II	National Synchrotron Light Source II
NSRC	Nanoscale Science Research Center
NSTC	National Science and Technology Council
NTRC	National Transportation Research Center
OLCF	Oak Ridge Leadership Computing Facility
OPTIMADE	Open Databases Integration for Materials Design
ORNL	Oak Ridge National Laboratory
OSD	Office of the Secretary of Defense
OSHA	Occupational Safety and Health Administration
PEG	Polyethylene Glycol
PHMSA	Pipelines and Hazardous Materials Safety Administration
PET	Polyethylene Terephthalate
PPE	Personal Protective Equipment
PPPs	Public-Private Partnerships
QED-C	Quantum Economic Development Consortium
QIS	Quantum Information Science
QIST	Quantum Information Science and Technology
R&D	Research and Development
REMADE	Reducing Embodied-energy and Decreasing Emissions
RFI	Request for Information
SBIR	Small Business Innovation Research

SNL	Sandia National Laboratory
SNS	Spallation Neutron Source
SRM	Standard Reference Material
SSRL	Stanford Synchrotron Radiation Lightsource
STPI	Science and Technology Policy Institute
STTR	Small Business Technology Transfer
TAGs	Technical Advisory Groups
TCs	Technical Committees
TMF	The Molecular Foundry
TSCA	Toxic Substances Control Act
TWA	Technical Working Area
USDOT	U.S. Department of Transportation
USGS	U.S. Geological Survey
USML	United States Munitions List
VAMAS	Versailles Project on Advanced Materials and Standards
VTO	Vehicle Technologies Office
YSZ	Yttria-Stabilized Zirconia

Appendix N. NAMs and Other ACA Technologies

NAMs are connected to many of the other technologies named in the ACA, in particular additive manufacturing (AM), artificial intelligence (AI), Internet of Things (IoT) in manufacturing, uncrewed delivery services, blockchain, and quantum computing. This appendix discusses the ways in which NAMs overlap with these other ACA technology areas.

N.1. Additive Manufacturing

NAMs can be both a feedstock for AM and an output of additive manufacturing. Currently, most of the available feedstock powder for metal AM parts is not optimized for AM, resulting in parts that do not exhibit the same microstructure or properties as parts manufactured using more traditional processes such as casting or wrought processes (e.g., rolling or forging). Continued advancement of AM will be enabled by the optimization of feedstock materials for a given AM process or set of processes—e.g., laser powder bed fusion or directed energy deposition processes. Optimizing feedstock materials will also enable wider use of AM by ensuring repeatable fabrication and the production of quality parts. These materials therefore may be considered NAMs since they are tailored for use in AM to produce parts with desired, likely superior properties. In addition, the material that constitutes the additively-manufactured product has unique morphology and properties for its intended application, and therefore additively-produced materials may also have novel or enhanced properties for certain applications. NAMs produced using AM include, but are not limited to, functionally graded materials, multi-functional materials, and architected materials. Thus, the additive manufacturing process itself can be a way to produce NAMs. A detailed discussion of materials used in AM can be found in the corresponding chapter for that technology.

N.2. Artificial Intelligence/Machine Learning (AI/ML)

AI and ML are widely deployed by researchers and commercial entities to discover, design, simulate, and develop NAMs and to conduct materials research [78]. AI and ML are critical tools in the MGI toolbox, enabling vast quantities of materials data to be put to work predicting properties, learning new design strategies, optimizing manufacturing processes, and suggesting materials to synthesize and test. Natural language processing has been applied to materials science publications to suggest synthesis and processing routes, and ML models have been used to approximate complex, slower-running physics-based models. The value of the MII envisioned by the MGI is largely enabled by the ability of entities to use AI and ML tools to mine materials data and generate new knowledge. A key challenge of this material innovation infrastructure will be standards that enable materials data to be accessed, processed, and shared across systems and machines. Standards under development to govern AI more generally are covered in the AI chapter. However, standards development efforts that are specifically directed towards materials data are described in this chapter.

N.3. Internet of Things (IoT)

IoT may be used for the purpose of manufacturing NAMs, just as for many other products. IoT can be applied to quality assurance of NAMs manufacturing. For example, a manufacturer may be interested in using IoT equipment to collect real-time data of materials properties, processing temperatures, or other metrics during manufacturing to ensure that processing lines are operating correctly. Also, the microchips and sensors used by IoT devices may themselves incorporate NAMs, such as advanced semiconductors or optoelectronics. In that sense, IoT can be an application of NAMs, even as it is also an enabler of enhanced NAMs manufacturing.

N.4. Blockchain

Blockchain technologies will play an essential role in ensuring the provenance and security of data used in the digital engineering environment [79]. Data curation and secure data storage, exchange, and accessibility are essential for component/system design, advanced materials development and advanced manufacturing. The data from models, simulation, measurements and analytic tools used in advanced materials development, in component and system design and development, and in advanced manufacturing are part of the digital engineering environment for a component or system from concept to end-of-life [80]. The security of data throughout the digital engineering environment is critical. Blockchain may also play a role in improving supply chain management by increasing traceability of transactions and coordination among participants [81].

N.5. Quantum Computing

Quantum computing is a catalyst for NAMs development. Many of the devices proposed for use in quantum computing rely on materials with exquisite purity, in some cases including isotopic purity, as well as extraordinary crystalline quality and extremely precise positioning of atoms or other species within materials. Superconducting materials, semiconducting materials, 2D materials, and photonic materials are all key components of quantum computing technology, and each materials system has its own advantages and disadvantages [82]. Quantum computing as an industry is relatively new compared to the advanced materials industry, and can be seen as a current driver of advancements in materials purity, quality, and manufacturing precision.

N.6. Unmanned Delivery Services

Unmanned delivery services will take advantage of several NAMs, including NAMs contained in the energy storage devices these platforms use (i.e., batteries), NAMs that are used to build out the structures of these devices (i.e., lightweight structural materials), and NAMs that are integrated into the microchips and communications devices that are used to track their location and communicate their progress. Therefore, uncrewed delivery services may be viewed as technology that has been enabled in part by NAMs innovation.

Unmanned Delivery Services

Chapter Contents

List of Tables

List of Figures

6. Unmanned Delivery Services

Summary

The Consolidated Appropriations Act of 2021 (Act; Public Law 116-260) tasked the Secretary of Commerce, in coordination with other appropriate Federal agencies, to complete a series of studies on critical and emerging technologies. This chapter addresses one of the specified technologies—unmanned delivery services (UDS)—and provides analyses of current and long-term trends as well as risks, challenges, and opportunities.

For the purposes of this chapter and in keeping with provisions of the Act, UDS are defined based on a particular category of delivery[140]: "*unmanned (e.g., remotely operated, semi- to fully autonomous) delivery services (ground or aerial) that provide endpoint delivery—i.e., the last step of the delivery process when an item travels from a distribution point, such as a transportation hub or warehouse, to its final destination—of goods (e.g., groceries, meals, medications, disaster or emergency supplies).*"

Current Uses and Potential Applications

UDS have numerous potential applications in a variety of industry sectors, including wholesale and retail trade, medical and pharmaceutical supplies, agriculture and natural resource management, public safety, and disaster and emergency response. While most uses of UDS today have been limited to specific demonstrations and test cases, expanded and more complex operations can be expected as both experience and technologies mature.

Challenges to Development and Adoption

UDS rely on many new and emerging technologies, and therefore face many technical challenges, including: the ability to detect and avoid obstacles; improved capabilities for robust and reliable navigation and communication; Beyond Visual Line of Sight (BVLOS) operations; battery-limited payload capacity and range; road and air traffic management (e.g. Unmanned Traffic Management (UTM) framework); reliable and secure package transport and drop-off; operating in non-ideal weather; environmental conditions; and other operational domain considerations.

Other, technical challenges include the lack of UDS-specific infrastructure and logistics, integration into existing environments, and needs for further development of test methods and standards to assess safety and security, promoting public trust and acceptance of these systems, and establishing and harmonizing the heterogeneous regulatory frameworks that govern UDS operations.

[140] Various government and industry stakeholders are evaluating the whole sector of UDS, beyond endpoint delivery, but in response to legislative text NIST is solely focused on endpoint UDS.

Safety Risks Associated with UDS Adoption

Appropriate risk management and mitigation, including anticipating increased risks with more complex future deployments, will continue to be critical to the successful growth of the sector. These risks stem in part from the current state of knowledge of the technology and how it interacts with the operational environment—either airspace or sidewalks and roads—existing infrastructure, other vehicles, and people.

Cybersecurity risks are also a concern for UDS because malicious actors could gain illicit control of UDS. There are also broader security risks of malicious actors posing as legitimate UDS while conducting illicit activities. Both these security risks could potentially lead to acts of terrorism, delivering contraband, or other criminal activities.

Effect on Traffic

Currently, aerial and ground UDS have small effects on air and surface traffic congestion due to their limited deployment. As UDS are more widely adopted, the potential impact of UDS on traffic safety and congestion will depend on many factors, including operational designs (e.g., mode, scope, scale), local factors (e.g., population density, road design, geography, proximity to manned aircraft operations), and market factors (e.g., consumer demand or number of packages delivered). With growth in the aerial and ground UDS, industry predicts markets to reach as much as $3 billion by 2025 for aerial UDS and USD 349 million by 2026 for ground UDS. Consequently, traffic management concepts, logistics, and infrastructure will need to keep pace with predicted market growth.

U.S. Development and Manufacture of Related Software, Technology, and Infrastructure

While most U.S. UDS operators or their technology partners currently design and develop their own UDS hardware, software, and infrastructure, the underlying hardware and software systems and components come from a variety of domestic and international sources. With the U.S. UDS industry subject to many of the same foreign-source dependencies and supply chain risks as other information technology-centric sectors, successful growth of the UDS industry requires managing these risks.

Effect on U.S. Workforce

UDS workforce effects may be examined in the context of automation as experienced in other sectors. Generally, high-skill workers are more likely to be positively affected by automation while low- and middle-skill workers are more at risk of negative employment impacts due to labor displacement.

The current delivery services workforce consists of hundreds of thousands of workers, and job growth or displacement due to UDS is likely to differentially affect some sectors, job types, and localities. New research and continuing assessment of the delivery labor force are needed to address changes to the existing delivery workforce, predict the needs of the emerging workforce as UDS deployment expands, and inform and guide policies addressing an evolving delivery workforce.

UDS could spur specific job growth within the domestic workforce, with companies potentially hiring in UDS operation and piloting, research and development, maintenance, and management. However, these effects will depend largely on the rate of adoption, technological feasibility, cost, and policies for expanded UDS deployment.

Federal Activities and Federal Jurisdiction

While local, state, tribal, and territorial governments play essential roles in the UDS sector, this chapter responds to a legislative request focused on the Federal role. Federal agencies interact with UDS stakeholders and related technologies through their regulatory authorities, research and development activities, and operations. The Federal Aviation Administration (FAA) and Department of Transportation (DOT) have regulatory authority over aspects of UDS operations and systems. While development of deployable UDS technologies and platforms is primarily driven by the private sector, the Federal Government plays an important role in supporting the development of UDS standards. Regulatory and science-focused agencies such as FAA and the National Aeronautics and Space Administration (NASA) frequently collaborate on the development and evaluation of technologies that will help enable the safe integration of unmanned aircraft systems (UAS) technologies into U.S. airspace. The National Institute of Standards and Technology (NIST) collaborates with the National Highway Traffic Safety Administration (NHTSA) on concepts for automated driving systems safety and with the FAA and others on drone and robotics safe performance measurement methods. The National Science Foundation (NSF) supports research on the science and engineering needed to develop safe and effective hardware and software for UDS, as well as to develop education and training programs for a skilled UDS workforce. Continued coordination among Federal agencies is needed to facilitate growth of the UDS sector.

Risks Posed to the Market Place and Supply Chain

Liability, public perception, and an uncertain regulatory environment are potential risks for UDS developers and investors. For example, insuring emerging technologies like UDS carries inherent uncertainties due to a scarcity of data (e.g., insurance premiums are calculated conservatively to assume a worst-case scenario). This requires UDS operators to self-insure or acquire private insurance for their operations, which may limit the diversity of the UDS marketplace by preventing companies with fewer financial resources from entering. In addition to any financial repercussions, any incident involving UDS could have drastic consequences for public perception and acceptance of the technology.

Risks Posed to National Security, Including Economic Security

Domestic UDS deployment, or lack thereof, has the potential to affect the national security, including economic security,[141] of the United States. As with related technologies (e.g., automated vehicles [AVs]), direct competition between U.S.-based and foreign companies is expected in the UDS field. U.S. UDS companies may face economic risks if the market is slow to develop or supply chain issues make it difficult to meet market demand. Economic risks can also feed into national security risks, where foreign-controlled supply chains for UDS drones and AVs create vulnerabilities in defense- and homeland security-related uses of these technologies (e.g., adequate procurement, cybersecurity risk).

Emerging Risks and Long-term Trends

Nascent UDS technologies and operations are expected to mature and become more widespread in the coming years, although the extent of this growth will be driven and limited by policy, consumer demand, and public perception. Experts theorize that delivery enabled by UDS will continue to influence and increase overall growth of on-demand delivery services, in addition to replacing demand for delivery services performed through conventional modes of transportation. Widespread automation for UDS and transportation modes could lead to benefits for the environment, public safety, and operational efficiencies while decreasing risks associated with driver fatigue, distraction, or other unsafe driving behaviors.

Recommendations

The following recommendations stem from particular challenges and potential opportunities identified in this chapter and address:

- Advancing widespread adoption of UDS in the United States and in a global market;
- Mitigating current and emerging risks to the marketplace and supply chain; and
- Strengthening the role the United States plays in informing and establishing globally recognized norms and standards for UDS.

Challenge 1: *Increasing UDS deployments poses new risks to safety, security, and privacy.*

Recommendation 1a: Expand and strengthen existing coordinated efforts by DOT, NASA, DOL, and other Federal agencies—working in partnership with State and local entities, industry, and others—to develop operational frameworks that prioritize safety and accessibility for people while balancing the economic and societal benefits of UDS capabilities.

Recommendation 1b: Establish industry-wide best practices for security, privacy, and risk management. These can include examining and adapting existing frameworks and

[141] The Consolidated Appropriations Act of 2021 refers to "economic and national security," and economic security is understood to be part of national security for the purposes of authorities such as the Consolidated Appropriations Act of 2021 and Section 232 of the Trade Expansion Act of 1962 (Public Law 87-794).

best practices for implementation in the UDS sector, including NIST's risk management framework, privacy framework, and Internet of Things (IoT) cybersecurity guidance, OSTP's *Blueprint for an Artificial Intelligence (AI) Bill of Rights*, and NTIA's *Voluntary Best Practices for UAS Privacy, Transparency, and Accountability*.

Challenge 2: *Effective use by UDS systems of road networks and airspace requires integrating a range of policy, regulatory, and legal environments.*

Recommendation 2a: Undertake a study, led by stakeholder legal and regulatory experts/associations with engagement from existing State and local drone policy/legislation task forces, to develop consensus around the highest priority policy, regulatory, and legal barriers to growth of the UDS sector.

Recommendation 2b: Convene a series of joint task forces addressing each of the highest priority barriers for UDS. Task forces led by the DOJ and DOT should work in conjunction with other agencies, State and local attorneys general, legislative councils, and other relevant legal and regulatory stakeholders to identify best practices, Federal regulations, and consensus solutions for the removal of existing barriers.

Challenge 3: *The UDS sector operates at the leading edge of technologies and its continued growth relies on research and development for next generation capabilities.*

Recommendation 3a: Develop a Federal strategy for UDS research and development through an interagency task group with input from the commercial and academic sectors; convened by the Networking and Information Technology Research and Development (NITRD) program or similarly positioned agency.

Recommendation 3b: Strengthen and expand existing research, development, and standards programs in agencies such as NIST, NSF, NASA, DOL, DOT, Department of Energy (DOE), and others.

Challenge 4: *A lack of standards for interoperability, performance measurement, testing and certification, validation and verification, and other capabilities will inhibit innovation and the emergence of a competitive global UDS technologies market.*

Recommendation 4a: Convene private sector stakeholders to co-develop, with appropriate antitrust safeguards, a coordinated UDS strategy that identifies standards needs, gaps, and refinements essential to promoting UDS innovation and opportunities for market growth.

Recommendation 4b: Strengthen and extend existing programs that support basic and applied research, develop effective measurement methods, and document best practices and guidelines that provide the basis for effective development of prioritized, private sector-led UDS sector standards development.

Recommendation 4c: To promote broad adoption and maximize benefits of new standards, support programs for standards education and awareness and develop reliable and reproducible methods and protocols for testing and certification capabilities that support informed acquisition of innovative systems and technologies.

Challenge 5: *The workforce implications of UDS sector growth are complex with the pattern of workforce changes expected to vary by region with differences in the directions, pace, and scale of growth in this emerging sector.*

Recommendation 5a: Expand the collection and aggregation of openly accessible workforce data at local, State, and regional levels in UDS-relevant services, technologies, labor, and other jobs sectors.

Recommendation 5b: Support the development of education, training, and re-skilling programs in areas such as UDS operations, maintenance, management, and in areas such as complex systems integration and control. Develop, in cooperation with industry and academia, a resource for curricula and program options for a skilled UDS workforce suitable for tailoring to regional needs by local educators.

Challenge 6: *Enabling growth of the UDS sector requires coordination among a diverse group of stakeholders.*

Recommendation 6a: Strengthen and expand existing coordination efforts among relevant Federal agencies, including core agencies, such as the DOT, NASA, and the Federal Communications Commission (FCC)—and supporting agencies, such as NIST, NSF, NTIA, the Department of Homeland Security (DHS), the Department of Defense (DOD), the Department of Labor (DOL), the Department of Education (ED), and the Department of Justice (DOJ).

Recommendation 6b: Strengthen and expand existing coordination efforts among local, Tribal, State, and Federal agencies with roles in enabling UDS applications, including local planning entities, state departments of transportation, and public safety entities.

Recommendation 6c: Strengthen and expand existing coordination efforts linking the private sector and government entities at all levels, including technology developers, manufacturers and suppliers, service providers, and user and consumer groups.

Recommendation 6d: The FAA should continue efforts and work with Congress, which has defined ‘unmanned aircraft system’ in statute[142], to identify more inclusive, gender-neutral language to replace the term ‘unmanned.’

[142] 49 U.S.C. 44801, “Definitions.” https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title49-section44801&num=0&edition=prelim

6.1. Overview

6.1.1. Definition of “Unmanned Delivery Services”

“Unmanned delivery services” (UDS) is a term with a broad scope that can include a variety of different vehicle concepts (small delivery robots and aircraft systems to light- and medium-duty vehicles) and operating environments (e.g., sidewalks, roads, and low-altitude airspace). For the purposes of this chapter, it is helpful to use a definition of UDS focused on a specific category of delivery that uses certain types of UDS such as small unmanned aircraft systems (sUAS[143]) [1], personal delivery devices (PDD), and autonomous delivery vehicles (ADV):

> *unmanned (e.g., remotely operated, semi- to fully autonomous) delivery services (e.g., ground, aerial) that provide endpoint delivery—i.e., the very last step of the delivery process when an item travels from a distribution point, such as a transportation hub or warehouse, to its final destination—of goods (e.g., groceries, meals, medications, disaster or emergency supplies).*

This definition was developed with consideration of existing characterizations of UDS (e.g., [2], [3]) and the request in the Consolidated Appropriations Act of 2021 (Public Law 116-260).[144]

There are a number of potential benefits in furthering the broad adoption of UDS, including improved safety (e.g., reduced roadway injuries and fatalities), improved quality of life and access to goods, lower energy usage, and improved supply chain management [4]. Unfortunately, UDS typically responsible for endpoint delivery are relatively new and currently operate under regulatory exemptions and in limited numbers. This regulatory environment, or general lack thereof, challenges industry attempts to predict the potential market for UDS and limits the ability to communicate the advantages of the technology to the American public. In addition, the wide variety of parameters within operating environments, from rules of the road or low-altitude airspace to road-going infrastructure and available spectrum for communication, can potentially further complicate widespread adoption of current UDS technologies.

6.2. Background

The Consolidated Appropriations Act of 2021 (Public Law 116-260) directed the Secretary of Commerce, in coordination with other appropriate Federal agencies, to complete a series of studies on critical and emerging technologies. This chapter addresses one of the specified technologies—UDS—and provides analyses of current and long-term trends as well as risks, challenges, and opportunities. The topics as set out in the Appropriations Act and covered in this chapter are:

- industry sectors that implement and promote the use of UDS;

[143] sUAS are defined by the Federal Aviation Administration (FAA) as “unmanned aircraft weighing less than 55 pounds on takeoff,” i.e. 25 kg.

[144] Consolidated Appropriations Act, 2021 (Public Law 116-260). https://www.congress.gov/bill/116th-congress/house-bill/133/text.

- current uses and potential future applications of UDS;
- challenges to the development and adoption of UDS;
- the viability of UDS to deliver goods including groceries, meals, medications, and emergency response supplies;
- safety risks associated with the adoption of UDS on the ground and in the air;
- effect of UDS on traffic safety and congestion;
- extent of U.S.-based development and manufacture of UDS-related software, technology, and infrastructure;
- types of jobs that may be lost or created due to the development and adoption of UDS;
- the effect of the adoption of UDS on job quality for low-, middle-, and high-skilled workers;
- the breadth of Federal activity related to UDS, including a list of Federal agencies asserting jurisdiction over UDS sectors, a description of each agency's expertise regarding UDS, and the interagency activities focused on UDS;
- risks to UDS supply chains and marketplace;
- UDS-based risks to the national security, including economic security, of the United States; and
- long-term trends in UDS.

6.2.1. Approach

A targeted definition of UDS was developed for the purposes of this work given the breadth of types of and uses for UDS, and to be responsive to the congressional language in the bill text. Recent reports and scientific publications related to UDS were reviewed along with responses to the public request for information (RFI). Interviews with Federal employees, industry representatives, and current users of UDS were also carried out. Given the breadth of types of and uses for UDS, this chapter provides a representative snapshot of a facet of the UDS landscape rather than an exhaustive summary of every UDS platform in development or use.

For unmanned "endpoint" deliveries, the two main mechanisms of delivery in use today are deliveries via sUAS, also sometimes referred to as drones, and autonomous ground vehicles or robots traveling on the roads and/or sidewalks. In this chapter, deliveries via sUAS are referred to as "aerial UDS," and deliveries via autonomous ground vehicles or robots are referred to as "ground UDS."

6.2.1.1. Aerial UDS

Most aerial UDS generally consist of the following main components:

- Frame: The body of the aircraft, including fuselage, and landing gear.

- Motor(s): Generate thrust to propel the drone in flight.
- Battery/fuel: Provides power for drone flight and functions.
- Avionics: Onboard electronic systems that aid the drone in flight-control, navigation, and communications. This includes flight and speed controllers, inertial measurement units (IMU), radiofrequency (RF) transmitters and receivers, and global positioning system (GPS) modules.
- Optical and infrared cameras: Usually used as part of the drones' "visual" navigation system, to help detect and avoid obstacles, identify visual landmarks such as terrain features or landing zones, and navigate semi-autonomously using visual cues.
- Software: Includes firmware and operating system for basic drone functions, but also AI and machine learning (ML) and computer vision algorithms for advanced functions like sensor fusion, semi-autonomous navigation, terrain mapping, and object detection and avoidance.

Other sensors that are currently less common on aerial delivery drones, but are being used increasingly as the technology matures and the associated size, weight, and power (SWAP) requirements decrease, include radio detection and ranging (radar), light detection, and ranging (LIDAR), acoustic sensors, and multi-spectral cameras.

Aerial UDS also require mechanisms to transport and drop off the packages they are delivering. Currently, there are three main methods of delivery: 1) land and deposit the parcel, 2) hover while lowering the parcel with a cable, and 3) drop the parcel with or without a small parachute attached.

6.2.1.2. Ground UDS

Ground UDS can be divided into two categories: sidewalk delivery robots (sometimes referred to as "personal delivery devices [PDD]") and road delivery vehicles. Sidewalk delivery robots can weigh up to 50 kg and are designed to travel on sidewalks and pedestrian pathways, but not on roads and highways. Road delivery vehicles are larger, weighing more than 50 kg, and often more closely resemble autonomous (self-driving) passenger cars in size and form factor. Regardless of size, ground UDS, including both sidewalk and road delivery vehicles, generally consist of the following main components.

- Vehicle chassis and wheels: The frame of the vehicle, including storage areas for carrying delivery loads.
- Engine and motors: Provides power to and propels the vehicle (including high-voltage batteries in electric vehicles).
- Control and navigation system: Onboard electronic systems and sensors that enable vehicle functions such as navigation, steering and braking, and communications. These include accelerometers, Inertial Measurement Units (IMU), RF transmitters and receivers, and GPS modules.
- Vision system: These are systems that combine external sensors, used to provide information to the vehicle's computer vision, with perception software and

hardware to help the vehicle “see” and navigate in its environment. The sensors may include some combination of the following: optical and infrared cameras, radar, LIDAR, and acoustic and ultrasonic sensors.

- Software: Includes firmware and operating system for basic vehicle functions, including safety systems and fail-safe mechanisms, but also AI/ML and computer vision algorithms for perception, sensor fusion, navigation, route planning, and object detection and classification.

6.3. Observations

6.3.1. Industry Sectors That Develop, Build, Implement, and Use UDS

UDS have numerous applications in a variety of industry sectors. In order to categorize the UDS relevant industry sectors, the North American Industry Classification System (NAICS) was used [5].[145] In Table 1 the NAICS sectors where endpoint UDS have applications are listed, along with examples of how UDS are implemented in each sector.

[145] NAICS classifies business establishments by type of economic activity. NAICS is the standard system used by Federal agencies to classify businesses for data collected regarding the U.S. business economy.

Table 1. Examples of Endpoint UDS Implementation by Industry Sector

NAICS Code	Sector	Domain	Examples of UDS implementation in this sector
44–45	Retail Trade	Air and Ground	Delivery of retail goods directly to consumers
62	Health Care and Social Assistance	Air and Ground	Delivery of groceries, medications, and medical supplies
72	Accommodation and Food Services	Air and Ground	Delivery of meals, snacks, and beverages directly to consumers

Table 1 represents the relevant industry sectors within scope of endpoint UDS for the purposes of this chapter. However, there are additional applications of UDS beyond this scope; Table 2 details these sectors with examples of implementation.

Table 2. Examples of Other UDS Implementation by Industry Sector

NAICS Code	Sector	Domain	Examples of UDS implementation in this sector
11	Agriculture, Forestry, Fishing and Hunting	Air	Precision application of pesticides
42	Wholesale Trade	Air and Ground	Moving large-scale wholesale cargo
44–45	Retail Trade	Air and Ground	Beyond endpoint delivery of retail goods
48–49	Transportation and Warehousing	Air and Ground	Unmanned vehicles in warehouses and on roads; unmanned transportation of people
52	Finance and Insurance	Air	Use of vehicles to survey area to provide information for insurance needs
62	Health Care and Social Assistance	Air and Ground	Beyond endpoint delivery of groceries, medications, and medical supplies

NAICS Code	Sector	Domain	Examples of UDS implementation in this sector
71	Arts, Entertainment, and Recreation	Ground	Use of small robots within the hospitality industry

6.3.2. Current Uses of UDS

Companies have been developing and testing aerial and ground UDS for many years, but currently neither category of UDS is widely used across the United States. Current uses of UDS have been mostly limited to individual demonstrations and test cases, and/or limited deployment within small, localized areas. A representative list of these uses is presented in Table 3.

Table 3. Representative List of Current Uses of UDS

Delivery Category	Description	Domain	Example Use Cases
Food and beverage	Delivery of food and beverage by restaurants	Air	Flytrex drone food delivery from restaurants to customers in select communities[a]
		Ground	Starship robot food delivery from restaurants to customers in select communities and college campuses[b]
Retail goods	Delivery of retail goods and packages by logistics and retailer companies	Air	Wing drone delivery of packages in select cities[c]
		Ground	Nuro autonomous vehicle delivery of packages and groceries in select communities[d]
Medical aids	Delivery of medical supplies, medications, blood by healthcare and pharmaceutical companies, and/or humanitarian aid organizations	Air	Wingcopter drone delivery of medical supplies[e] Zipline drone delivery of blood in Rwanda[f]
		Ground	Nuro robot delivery of medical supplies[g]
Mail and Package Delivery	Delivery of mail and packages by postal service and logistics and retail companies	Air	Wing drone delivery of FedEx packages[h]
		Ground	U.S. Postal Service (USPS) pilot program employing autonomous robots in warehouses and sorting facilities[i]

[a] [6], [b] [7],[c] [8],[d] [9],[e] [10],[f] [11],[g] [12],[h] [13],[i] [14]

Although this chapter is focused on the delivery of goods and packages by UDS to consumers, there are other applications and use cases for unmanned systems that involve other forms of delivery (e.g., the delivery of information through the collection of data). Table 4 presents a representative list of notable applications that are well-suited for unmanned systems and may serve as entry points or pathways for UDS, enabling future growth and deployment (e.g., overcome some of the current technical and regulatory challenges).

Table 4. Other Notable Uses of UDS

Category	Description	Domain	Example Use Cases
Precision agriculture	Crop management including harvesting or delivery of insecticides, fertilizers, etc. by the agriculture industry and farmers	Air	Tevel Aerobotics Technologies drone harvesting system[a]; Rantizo drone crop spraying[b]
Industrial	Delivery of, for example, spare parts, tools, replacements parts, etc., by oil and gas, automotive, and energy and power industries	Air	Equinor drone delivery of spare parts to remote areas in Norway[c] Wingcopter drone delivery of spare parts to offshore wind farms in Germany[d]
		Ground	Starship robot delivery of spare parts, office equipment, and in-house mail[e]
Weapons and ammunition	Delivery of military cargo, supplies, weapons and ammunitions by the defense sector	Air	U.S. Army's use of drones to deliver ammunition directly to unit in field test[f]
		Ground	U.S. Army and Marine Corps use of semi-autonomous vehicles to deliver supplies to battlefield in field test[g]
Search and rescue	The use of unmanned systems to survey areas following emergencies or disasters to provide information to rescue teams and/or emergency supplies to victims	Air	Search and rescue organizations' use of drones to find lost or stranded hikers[h]
		Ground	First responders' use of robots to search for individuals in 2021 Florida building collapse[i]
Agricultural and industrial inspection and monitoring	The use of UAS to inspect and monitor crops, soil, power lines, critical infrastructure, and other areas that are difficult for humans to reach	Air	PrecisionHawk's use of drones to provide mapping and analytics for farmers and agricultural research firms[j]
Law enforcement	The use of UAS to provide mission situational awareness, surveillance and crowd monitoring, and aid in incident response	Air	Mountain View, California, Police Department[k]

[a] [15], [b][16], [c][17], [d][18], [e][19], [f][20], [g][21], [h][22], [i][23], [j][24], [k][25]

6.3.3. Future Applications of UDS

Potential near-term (i.e., ~5 years) future applications of small UDS may include the capability to navigate ever busier or more complex operating environments, such as delivering goods inside a high-rise office building or flying through congested low-altitude air space. Notably, the ability to autonomously navigate requires a significant number of hours-in-operation to train these systems and assess their safety and reliability. For ground-based UDS, operations in geographically restricted areas, whether inside buildings or within the confines of a college campus or municipality, potentially accelerates the pace at which these systems learn and increases their utility. Under the current regulatory regime, there could be limited growth of small aerial UDS operations in specific markets—such as remote or rural areas—where risk assessments are at an acceptable level to warrant operations. One challenge to widespread adoption of aerial UDS in the United States is FAA regulations that prohibit UAS pilots from operating BVLOS and over people. This aspect of operational capability may initially see growth and development via long-range surveillance of critical infrastructure (e.g., pipelines, rail ways, power grid) because, in part, they are typically not near population centers. As UDS reliability matures and regulations evolve, UDS may become more ubiquitous with larger platforms that can move passengers (e.g., air taxis) and cargo (e.g., hub-to-hub model, emergency response).

6.3.4. Challenges to Development of UDS

UDS rely on many new and emerging technologies, and therefore face many technical challenges as developers, engineers, and delivery service providers attempt to implement new models of endpoint delivery. To a certain degree, all unmanned or autonomous systems face similar challenges in their development, but there are some distinctions between the challenges for aerial and ground UDS.

6.3.4.1. Challenges for Aerial UDS

Payload Capacity and Endurance/Range

Currently, per FAA regulations, the maximum total weight of sUAS is 55 pounds (25 kg). This limits the payload capacity of most aerial UDS to around 10 pounds (4.5 kg), which limits the types and sizes of packages that aerial UDS can deliver [26]. The small size and payload capacities of sUAS also place a limitation on the lithium-ion or lithium-polymer batteries used by most aerial UDS. Using current battery technologies, aerial UDS are limited by the distances they can cover. Flight ranges are further reduced by increased battery energy usage in windy conditions or degraded battery energy capacity in extremely cold or hot temperatures.

While there are efforts to develop and employ other power sources, including hydrogen fuel cells and gas-powered engines, batteries remain the preferred power source for aerial UDS [27].

Sense and Avoid

As is true for any aircraft, crewed or unmanned, sUAS must be able to take off, fly, and land at the intended location and in an intended manner without colliding with any objects (e.g., trees, tall buildings, power lines, birds, kites, other crewed and unmanned aircraft, and humans) on the way. The challenge for sUAS is the ability to perform these tasks without a human operator on board. This capability, often referred to as "sense and avoid" technology, requires a combination of external sensors, to help the sUAS "see" its environment, and well-developed software algorithms that receive and interpret the inputs from the sensors, make decisions, and enable the drone to navigate safely throughout its flight [28].

Most aerial UDS rely primarily on electro-optical cameras to visualize their surroundings. While cameras are a fairly mature technology, they cannot ensure robust sensing performance against all potential objects a drone may encounter in flight, and often have difficulty in degraded-visibility conditions such as rain or fog. Many aerial UDS are beginning to incorporate other more advanced sensors, namely radar and LIDAR, into their sense and avoid technology. Radar has the advantage of providing an all-weather sensing capability, and LIDAR can produce detailed three-dimensional maps of an aerial UDS's surroundings to aid in terrain following and navigation. However, the SWAP requirements of radar and LIDAR are currently too large for the small airframes and limited battery power of most aerial delivery drones [28].

More important to the aerial UDS's sense and avoid capability are the software algorithms, which use AI/ML to process and interpret the data that come from its sensors and make decisions about the drone's actions [29]. This combination of sensors and AI/ML software allows aerial UDS to perform tasks such as detecting and classifying objects, avoiding obstacles, and identifying designated landing areas. While AI/ML is a large focus of UDS research and development, much remains unknown about AI/ML algorithms—in particular, how to develop and train algorithms to recognize objects and decide on a course of action quickly, and how to test them to assure their robustness and reliability across a wide range of conditions and environments [30].

Navigation and Communications

Aerial UDS rely on GPS [31] and wireless signals transmitted and received in the 2.4 GHz to 5.8 GHz frequency range for accurate geo-location, navigation, and communication [32]. Most sUAS do not have sufficient onboard processing power to perform all of the computing tasks required for navigation and sense and avoid. Instead, these data are transmitted over the wireless connections and processed in the cloud or on an off-board host processor [32]. Remote operators (currently required for all sUAS flights) also depend on wireless data transmission to ensure safe operation of the sUAS. Thus, strong and robust wireless data connections are critical for aerial UDS operations. In areas where the GPS and wireless signals are weak, or in high population density areas where there are numerous wireless devices competing for limited bandwidth, the aerial UDS operations can be affected [27].

Possible ways in which these effects can be mitigated include improved inertial navigation systems (INS) and increased onboard processing capabilities, such that the drone is less reliant on strong GPS or wireless signals to operate safely. The state of current technology for both INS and onboard processing capabilities is not mature enough to meet both the accuracy requirements and SWAP constraints of aerial UDS [33].

Air Traffic Management

To scale operations, aerial UDS must be safely integrated into the national airspace and deconflict with crewed aircraft and other commercial and recreational drone operators. This requires an air traffic management system with an effectiveness equivalent to that for the existing air traffic control (ATC) system used by the FAA for conventional aircraft. Such a system does not yet exist, but the FAA—in collaboration with NASA, other government agencies, and industry UAS stakeholders—has been working to develop the UAS Traffic Management (UTM) system [34]. This collaborative effort is working on developing concepts of operation and identifying services, roles and responsibilities, information architecture, data exchange protocols, software functions, infrastructure, and performance requirements to enable safe BVLOS drone operations in low altitude airspace. The envisioned UTM is complex and faces technical, policy, and regulatory challenges in its development and implementation [35].

Package Transport and Drop Off

To deliver packages to consumers, aerial UDS need the means to safely and securely carry and drop off an external payload without damaging its contents or losing control of the package either in flight or upon delivery. Designing such a system can be a challenge due to the small size and form factor of aerial drones—any mechanism to physically secure, protect and drop off the package must do so without adding significant weight to the system. Aerial UDS companies are actively working to expand upon and optimize methods and designs to carry and drop off packages, including land and deposit, lower with a cable, and drop with or without an attached parachute.

Weather and Environmental Conditions

Because of their small size, many aerial UDS have difficulty flying in windy conditions, and even more so in adverse weather conditions such as rain or snow [36]. This limits the distances that aerial UDS can cover and restricts the windows of opportunity (and, in some cases, the geographic locations) for delivery by aerial drones. The inability to operate in adverse weather is a significant consideration for many UDS applications, ranging from rapid package delivery services to critical medical supplies and urgent emergency and disaster response.

The low-altitude airspace environment (i.e., altitudes at or below 400 feet) in which most aerial UDS operate presents additional challenges for aerial UDS applications. UDS are more likely to encounter objects such as birds, trees, buildings, and power lines at these altitudes, thus underscoring the importance of effective “sense and avoid” solutions for aerial UDS (described above), as well as thorough environmental assessments in support of intended UDS areas of operation.

6.3.4.2. Challenges for Ground UDS

Sense and Avoid

Like aerial UDS, ground UDS need to be able to “see” the environment in which they are operating, so they can detect objects and obstacles and navigate safely from point A to B. However, for ground UDS, the environment in which they are required to operate involves complexities that are different than those for aerial UDS [37]. Ground UDS traveling on the roads or sidewalks must operate with other vehicles, pedestrians, and bicyclists, and follow and obey all traffic laws, including speed limits, lane markings, and traffic signals. Ground UDS rely on a combination of sensors to sense and perceive their environment, most commonly: visual cameras, LIDAR, and radar. Ground UDS are less constrained by SWAP requirements than aerial UDS, and thus are able to employ a wider variety and more combinations of sensors to aid in visualizing the environment.

Also similar to aerial UDS, ground UDS use AI/ML algorithms to process and interpret the data that come from their sensors and make decisions about the vehicle’s actions (e.g., braking or swerving to avoid an oncoming vehicle or pedestrian). However, the complexities of the road environment require that the sensors and AI/ML software work seamlessly to detect and classify objects with a required amount of certainty, make decisions, and take action, all in real-time, in order for the ground UDS to operate safely [38]. This places a high burden on AI/ML algorithms and increases the challenges associated with developing, training and testing these algorithms [37].

Navigation and Communications

Ground UDS also use GPS and wireless signals for navigation, and communication. Similar to aerial UDS, ground UDS operations can be affected in areas where the GPS and wireless signals are weak, or in high population density areas where there are numerous wireless devices competing for limited bandwidth. In addition, operating near the ground in areas of natural feature and built environment clutter makes navigation and communications more difficult for all UDS, although ground UDS are more subject to these difficulties due to their surface operational mode.

Because they usually have more space and power than aerial UDS, ground UDS can often perform more data processing onboard rather than needing to transmit data over wireless connections for off-board processing. However, ground UDS still rely on wireless data links for remote operation and applications like fleet management. The complexity of the environments in which ground UDS operate, along with the range of scenarios they may encounter, requires ground UDS to have access to fast (i.e., low-latency) data connections for the instances in which a remote operator needs to intervene or take control of the vehicle.

Limited Payload Capacity and Range (for personal delivery devices)

Ground UDS that travel on the sidewalks (i.e., PDDs) have size and weight limitations, which are prescribed in accordance with State and local regulations. These limitations can restrict the payload capacities and endurance of PDDs (due to the smaller batteries on these vehicles), which constrains the size of the packages PDDs can deliver and the distances they are able to travel.

6.3.5. Challenges to Adoption of UDS

Other challenges, which are less technical in nature, may not directly impact the development of UDS, but affect the widespread employment of UDS in both the air and ground domains. Representatives from government agencies and the UDS industry interviewed for this chapter described the following primary challenges to adoption of UDS.

6.3.5.1. UDS-specific Infrastructure and Logistics

Several of the technical challenges to the development of UDS discussed above are further exacerbated by a lack of infrastructure that, if implemented, could help to enable more widespread adoption of UDS. Aerial UDS could extend their delivery ranges by recharging their batteries en-route through the use of, for example, wireless charging stations. Aerial UDS can also benefit from designated take off, landing, and package drop-off areas. Analogously, ground UDS traveling on the roads and sidewalks can benefit from having clearly marked designated travel lanes and parking or drop-off areas [39]. Furthermore, both aerial and ground UDS would benefit from increased low-latency communications bandwidths and networked traffic management systems.

Since UDS are a nascent technology and new paradigm for endpoint deliveries, companies are still determining the most appropriate business and logistics models to economize the use of the technology (e.g., fleet management strategies, delivery route optimization, and aircraft/vehicle maintenance concepts). These logistical hurdles need to be overcome before UDS are more widely adopted by commercial industry.

6.3.5.2. Test Methods and Standards to Assess Safety and Security

Safety and security concerns related to UDS operations (discussed in more detail in Section 6.3.6) present a challenge to widespread adoption of UDS because many of the current regulations that place limitations on UDS operations stem in part from these concerns. For example, the FAA BVLOS restrictions for UAS come in part from a lack of assurance that UAS can travel safely on their own without colliding with any objects or obstacles they may encounter in their flight path. Addressing these safety and security concerns requires testing UDS against an established and accepted set of test methods and standards, including data collection standards.

Although companies developing UDS are actively conducting their own tests and government agencies are working to develop some of these test methods and standards, the technologies associated with UDS are still new and emerging, and as such, so are the test methods and standards. This is especially true when it comes to assessing the AI/ML algorithms, which are used in the UDS's computer vision and "sense and avoid" systems [40; 41]. Developing test methods to assess how these algorithms behave, learn, and make decisions in a wide range of scenarios and conditions is an active area of research.

6.3.5.3. Harms to People, and Associated Harms to Trust

Autonomous systems, whether operating in the air or on the roads, can pose risks to people. For example, aerial UDS could fall on people or cause property damage, and ground UDS could collide with pedestrians or other vehicles. High-profile incidents involving autonomous vehicles, such as the 2018 self-driving collision in Tempe, Arizona, have provided examples of this type of risk to people [42; 43]. Consequently, in some survey studies, consumers have expressed concerns about the safety of aerial and ground UDS [42; 44].

Airspace and privacy concerns, including owners' rights to the enjoyment or use of land and the airspace associated with it, are also relevant to public trust and acceptance of UDS. For endpoint delivery, UDS need to travel through neighborhoods and to places of residence, and there are potential privacy harms from aerial UDS equipped with cameras flying over homes and backyards [45].

6.3.5.4. Regulatory Frameworks that Affect UDS Operations

UAS are regulated by the FAA, which regulates all aspects of civil aviation in the United States. (Details on FAA activities related to aerial UDS can be found in section 6.3.10.) For aerial UDS, the FAA has several regulations that place restrictions on how these services may operate. The key rules affecting aerial UDS stipulate that aerial UDS must:

- Have a remote operator in control of one UAS at a time;
- Remain within visual line of sight of the remote operator; and
- Not be operated over non-participants who are not under a covered structure or in a stationary covered vehicle.

Operators seeking to conduct package delivery operations generally must operate under 14 CFR part 135 with regulatory relief and part 119 air carrier certification, which permit BVLOS flights and flights over people/vehicles under certain conditions. However, aerial UDS industry representatives have expressed concerns that the process for applying for these certifications is complex and opaque, often times interfering with companies' development and test efforts.

Ground UDS traveling on public roads are regulated at the Federal, State, and local level, while ground UDS operating on sidewalks (PDD) are regulated primarily by local authorities (details in section 6.3.10). The DOT's National Highway Traffic Safety Administration (NHTSA) issues the Federal Motor Vehicle Safety Standards (FMVSS), which ground UDS manufacturers must adhere to unless they apply for and receive certain exemptions. Ground UDS industry representatives have expressed concerns regarding the FMVSS exemption process in interviews, specifically, that the FMVSS were developed for standard vehicles (with human occupants) and need to be updated to accommodate autonomous vehicles and ground UDS.

There are no existing Federal laws governing the operation of ground PDD (i.e., sidewalk delivery robots).[146] State and local authorities regulate PDD operations, including the maximum weights of PDD and speeds at which they are permitted to travel. State and local regulations related to PDDs vary widely, with State law generally superseding local ordinances [46]. A number of States and local governments have passed laws enabling PDD operations within their borders under certain restrictions. Examples include the following.

- The city of San Francisco banned PDD entirely in 2017, before creating a process in which the city issues permits to eligible operators.
- Pennsylvania State law legalizes PDDs up to 500 lbs (227 kg, without cargo) and recognizes them as "pedestrians" but stipulates that they must yield right of way to humans [47].

The size and speed restrictions on PDD, and the variation of these regulations across different States and cities, impact the adoption and deployment of ground UDS that travel on sidewalks and pedestrian pathways.

While most goods considered for transportation by UDS are unregulated, some materials, including many household items such as cleaners, lithium batteries, paints, and medicines, are considered hazardous materials. The transportation of hazardous materials (or dangerous goods) is regulated by the Pipeline and Hazardous Materials Safety Administration (PHMSA). The Hazardous Materials Regulations (HMR) were developed for transportation in operations where human transportation workers are present. The regulations include operational controls and hazard communications that may need to be adjusted for UDS operations. Additionally, adjustments to the packaging requirements may be necessary for aerial UDS as a variety of delivery methods are being considered/used that go beyond the conditions considered when the HMR was developed. These include dropping via tether, delivery via parachute, or delivery via free-fall drop. The regulations are well-positioned, as PHMSA does have the authority to issue Special Permits (waivers) from the regulations that can allow these new operations prior to any needed regulatory changes.

6.3.6. Safety Risks Associated with the Adoption of UDS

6.3.6.1. In the Air

The major safety risks associated with the adoption of aerial UDS are injuries to people resulting from aerial UDS collisions with objects in flight, objects on the ground, or people directly [48]. These risks stem in part from the current state of knowledge of the technology and how it interacts with the airspace, existing infrastructure, other aircraft, and people. In particular, uncertainties exist regarding the airworthiness and reliability of sUAS and their "sense and avoid" capabilities.

[146] The Americans with Disabilities Act of 1990 (ADA) prohibits discrimination against people with disabilities and ensures equal opportunity and access for persons with disabilities with respect to the programs, services, and activities of public entities—including the provision of pedestrian facilities in the public right-of-way—and in access to places of public accommodation and commercial establishments.

Additionally, because sUAS have been used by malicious actors to conduct illicit activities and acts of terrorism, there is also a risk that the widespread adoption of aerial UDS will provide malicious actors with additional opportunities to conduct their activities [49; 50].

The key safety risks associated with the adoption of aerial UDS vary with the characteristics of the area of operations (e.g., population density) and include examples such as: [51]

- Collision with people causing bodily injury;
- Collision with property causing damage to assets and potential collateral injuries to surrounding people;
- Interference or collision with other crewed or unmanned aircraft;
- Loss of control of the sUAS, resulting in unexpected behaviors;
- Loss of control of the package being transported causing damage to property or bodily injury;
- Interference with radio signals causing communication or other critical hazards;
- Unauthorized trespassing or intrusion of privacy (e.g., using aerial UDS to take unauthorized pictures);
- Delivery to the wrong address or location, resulting in breach of privacy or medical risks if the goods being delivered are sensitive or health-critical (e.g., medications);
- Collection of sensitive information (e.g., use of aerial UDS to gain proximity to and collect sensitive data over wireless networks, gathering defense information for a foreign government);
- Hijacking of aerial UDS by malicious actors through hacking and/or spoofing of wireless signals; and
- Malicious actors posing as legitimate UDS companies to conduct, for example, explosive or chemical/biological attacks, or smuggle illegal items (e.g., drugs).

6.3.6.2. On the Road

The major safety risks associated with the adoption of ground UDS are injuries to people resulting from ground UDS collisions with pedestrians, vehicles, and other occupants of the roads and sidewalks. Similar to aerial UDS, these risks stem from the ongoing development of autonomous vehicle sensors and computer visions algorithms that form their "sense and avoid" capabilities [52]. Because ground UDS operate in a highly complex environment and will encounter more "objects" (compared to aerial UDS), uncertainties regarding the behaviors of ground UDS and their "sense and avoid" capabilities will magnify the safety risks. In addition, if these vehicles operate differently than other road users/sidewalk users, they may cause other vehicles to take unsafe actions. For example, passing a slow moving UDS could result in a collision between two other vehicles.

The key safety risks associated with the adoption of ground UDS vary with the characteristics of the operating area (e.g., foot and vehicle traffic density) and include examples such as:

- Collision with other occupants of the roads and sidewalks, including pedestrians, vehicles, and bicycles;
- Collisions between other occupants of the roads and sidewalks, including pedestrians, vehicles, and bicycles, caused by irregular behavior of ground UDS;
- Collision with property causing damage to assets and potential collateral injuries to surrounding people;
- Interference with emergency response vehicles and/or personnel;
- Interference with radio signals causing communication or other critical hazards;
- Unauthorized trespassing or intrusion of privacy;
- Delivery to the wrong address or location, resulting in breach of privacy or medical risks if the goods being delivered are sensitive or health-critical (e.g., medications); and
- Hijacking of ground UDS by malicious actors through hacking and/or spoofing of wireless signals.

6.3.7. Effect of UDS on Traffic Safety and Congestion

The effects of UDS on traffic safety and congestion depend on many factors, including operational designs (e.g., mode, scope, scale), local factors (e.g., population density, road design, geography), and market factors (e.g., consumer demand or number of packages delivered). Although existing U.S. UDS operations consist of pilot-scale demonstrations within designated locales, there was a broad consensus among interviewees and in literature that UDS platforms and operations will gradually expand beyond their current levels of deployment in the coming years and decades. This section is divided into subsections that briefly describe the effects of UDS on traffic safety and congestion for aerial and ground environments.

6.3.7.1. Air

At present, only a few companies have received the FAA Part 135 certification needed to perform commercial package delivery by drone; drone operations under Part 135 are restricted and cannot cross State lines. Wing and UPS Flight Forward have each received Part 135 certificates and intend to fly between approximately 16 to 100 deliveries per day in Christiansburg, VA, Winston-Salem, NC, Frisco and Little Elm, TX, and other locations [53; 54]. By comparison, Amazon shipped 4.5 billion packages to U.S. consumers in 2020, (averaging 12.3 million shipments per day) [55].

As existing U.S. delivery drone operations are highly restricted, relatively infrequent, and take place in less populated airspace, their effects on air traffic are likely small. Commercial delivery drones make up a small fraction of registered drones in the United States—as of 2022, there are 854,650 drones registered in the United States (of which 317,821 are registered for commercial use) [56]. General FAA sUAS collision reporting requirements only apply to incidents that result in serious injury or property damage over $500,[147] so sUAS collision data are limited (commercial aerial UDS operators have more stringent reporting requirements than recreational drones as a condition of their FAA certification). Although no fatalities due to sUAS operations have been recorded, the FAA collected 6,117 reports of instances of unsafe UAS behavior between 2014 and 2018, including one incident where an sUAS pilot flying BVLOS struck a helicopter, causing "minor damage to the helicopter's main rotor blade" [57; 58]. The majority of these anecdotal reports describe near misses that the FAA often attributes to unsafe and non-compliant pilot behavior.

Data describing effects of aerial UDS on surface vehicle traffic safety and congestion are also limited, as although it is possible some of the deliveries completed by drone replace and therefore reduce trips taken by commercial or privately-owned ground vehicles, current rates of replacement are unlikely to have a measurable effect on surface traffic congestion or safety.

If deployment and adoption of aerial UDS increase, their effects will be enhanced. As discussed previously, the intensity and scope of these effects depends on operational, local, and market factors. Researchers are developing models that consider the wide range of variability within these factors to predict potential effects. A 2020 study by researchers at Virginia Tech performed simulations of hypothetical aerial UDS operation at different levels of deployment for a few metropolitan centers (Christiansburg, VA; Austin, TX; Columbus, OH) to estimate effects such as hours of time saved per-person and reductions in cars on the road over a 5-year-period. Using these models, they estimate that drone deliveries could reduce 18.7–30.5 million vehicle miles annually in Christiansburg, preventing up to 46 car crashes per year by the fifth year of deployment (assuming all businesses delivering goods under 5 pounds (2.3 kg) adopt drone delivery by that time) [59]. This estimation could be applied to other cities where aerial UDS operate. Other studies have considered potential deployment models for drones and found that aerial congestion (e.g., number and density of drones in the airspace) depends on the number of drone delivery centers. Increasing the number of delivery centers decreases the distance traveled by each drone per trip [60].

6.3.7.2. Ground

Ground-based UDS generally fall into three categories: sidewalk delivery robots (often referred to as PDDs) that traverse pedestrian corridors, driverless or automated delivery vehicles that operate on roads and highways, and automated trucks capable of transporting goods over long distances. The focus of this chapter is on endpoint delivery, activities primarily conducted by sidewalk delivery robots and automated delivery vehicles (i.e., not automated long-haul transport of goods). Similar to computational methods used to estimate the effects of drone deployment, modeling tools can be used to consider potential externalities (e.g., sidewalk congestion, parking demand, curb space), of different hypothetical ground-based UDS operations [2].

The impact of ground-based automated delivery vehicles on traffic safety and congestion will depend on numerous variables that will change as software and hardware develop and automated delivery vehicles become more widely adopted. Some factors that will affect their

[147] 14 C.F.R. § 107.9 2022

impact on traffic flow include size, speed, driving behaviors, stop frequency, and trip duration. Automated vehicles that operate at very slow speeds could be an issue for slowing general traffic.

Sidewalk Delivery Robots

Sidewalk delivery robots travelling on pedestrian pathways should not add to vehicle traffic and may have the beneficial effect of reducing the number of conventional delivery vehicles on the road. However, they contribute to congestion on the sidewalks themselves, which vary in width and design between localities. Anecdotal statements from interviewees indicate that sidewalk delivery robots can create congestion in heavily trafficked pedestrian corridors as they sometimes become "stuck," or unable to proceed, when presented with novel environmental features or are surrounded by pedestrians they are programmed to yield to. A stuck UDS could create a collision- or trip-hazard for bicyclists or runners in addition to impeding the flow of the movement of people. In one incident, a sidewalk delivery robot blocked a curb ramp while a wheelchair user was in the crosswalk, preventing the person from safely accessing the sidewalk [61]. Sidewalk delivery robot deployment is still limited and largely confined to college campuses; interviewees report that ongoing operations collect data to optimize route-planning and avoid areas where robots are likely to encounter maneuverability issues. Improvements to the delivery robot's automation features should also reduce the frequency of such errors.

Automated Delivery Vehicles

The deployment of automated vehicles (AV) for delivery on roadways has immediate implications for traffic safety and may impact congestion. There is broad agreement that AVs could eventually greatly improve traffic safety and reduce traffic collisions and fatalities by reducing the rate of collisions caused by human error [62]. However, the introduction of AVs onto roads dominated by human drivers presents new dangers, especially during early and transitional phases of AV deployment.

Interviewees highlighted the need to better understand human-automated vehicle interaction to mitigate the potential risks of a mixed autonomy traffic environment. The AV's ability to anticipate and react to a human driver, and the human driver's perception and behavior around AVs, were both identified as challenges to autonomous vehicle deployment and adoption. One aspect identified by interviewees as challenging for AV developers is "roadsmanship," behaviors and norms widely accepted and practiced by human drivers (e.g., driving above the speed limit with the flow of traffic) that may deviate from traffic laws AV systems are programmed to strictly obey. Inflexibility in AV behavior may lead to congestion or human driver frustration if they encounter what they perceive as slow-moving AVs.

6.3.8. United States Development and Manufacture of Software, Technology, and Infrastructure for UDS

To describe U.S. development and manufacture of UDS, this section provides examples of U.S. companies in both the air and ground UDS sectors. Details of these companies are provided to give background on the state of their development and operations, and for reference of the current technology in use. Details are also provided on the design and manufacturing operations by company. In-house refers to activities that are carried out within the company, and by employees of the company. This section also briefly highlights the infrastructure required for air and ground UDS. Although there is no commonly agreed upon definition of infrastructure writ large used by the Federal Government, the term has generally been used to refer to capital-intensive and long-term systems and facilities. For the purpose of this section, the infrastructure discussed refers to the physical structures that might be required for or would facilitate the development and operation of UDS.

6.3.8.1. Air

Aerial UDS are still an emergent industry and have not reached widespread adoption. However, reports estimate the industry is estimated to widely expand in the coming decades. U.S. companies are cited as leading in the design capabilities behind aerial UDS. According to a 2021 economic report, the leading companies providing air-based delivery services are also predominantly based in the United States [27]. Table 5 provides a breakdown of examples of U.S. companies in endpoint unmanned air delivery services selected through review of recent media [27; 63]. A deeper look at these companies shows that almost all leading service providers design and manufacture their vehicles in house. No company yet has widespread adoption, and companies that do currently operate only do so in select locations. Although the specifications of each type of vehicle vary by company, all have a relatively similar small payload. However, this small payload is estimated to encompass the size of more than 80% of total packages that are shipped globally [27].

Table 5. Examples of U.S. Companies for Aerial UDS

Company	Operations Status	Drone Specifications	Regulation Status	Applications	Design and Manufacturing
Prime Air	Under development[b]	Packages up to 5 lbs (2.3 kg) in 25 km range Empty weight: 90 lbs (41 kg)	In 2020 received FAA part 135 certification to operate drone fleet[c]	E-commerce Industry	In house
Zipline	Limited operation in U.S. (Arkansas and North Carolina), other operations in Ghana and Rwanda	Packages up to 4 lbs (1.8 kg) in 80 km range Empty weight: 44 lbs (20 kg)	In 2022 received FAA part 135 certification and received FAA issuance of final airworthiness criteria under Title 14, Code of Federal Regulations (14 CFR) 21.17(b)[e]	Medical product delivery	In house[f]
Wing	Limited Operation: Helsinki, Finland; locations in U.S., including Christiansburg, VA; operations in Dallas-Fort Worth metroplex	Packages up to 2.6 lbs (1.2 kg) in 20 km range Empty Weight: 11.4 lbs[g] (5.2 kg)	In 2019 received FAA part 135 certification	Commercial delivery for a range of applications	In house[g]
UPS Flight Forward	Limited U.S. Operation (North Carolina)	Packages up to 4.4 lbs[k] (2 kg)	In 2019 received FAA part 135 certification[l]	Commercial delivery for range of applications	In house and collaboration with other companies[m]

Company	Operations Status	Drone Specifications	Regulation Status	Applications	Design and Manufacturing
Workhorse Group	Under development	Packages up to 10 lbs (4.5 kg) Empty Weight: 22.9 lbs (10.4 kg)	Currently pursuing type certification	Commercial contractor	In house[n]
FedEx	Under development, pilot program in Virginia[o]	See Wing entry above	See Wing entry above	Commercial delivery for range of applications	Use Wing drones

[a] [63], [b][64], [c][65], [d] [66], [e] [67], [f] [68], [g] [69], [h] [70], [I] [71], [j] [72], [k] [73], [l] [74], [m] [75], [n] [76], [o][13]

In addition to the endpoint applications of the companies listed in Table 5 there are efforts to implement unmanned delivery in larger aircraft services that deliver heavier cargo for longer distances. Companies such as Boeing are developing heavy lift delivery drones capable of lifting in the range of 230 kg of package weight over a range of about 33 km [27]. Longer-range applications to deliver goods from shores to cargo ships are also under development by Airbus [77]. These applications are outside of the scope of this chapter but might build on the same technology and involve similar key players in the field.

Regarding the physical infrastructure required for the unmanned aerial delivery services, there are not clearly defined requirements. These requirements will change as the technology develops, and as services reach more widespread deployment. However, initial physical infrastructure components include: vertiports and vertistops, which are helipads for landing and takeoff; charging stations, which could be part of the vertiports and vertistops; and ground control stations. The specific characteristics of the physical infrastructure will also differ based on the specific needs of the location. For example, urban and rural areas might have different considerations. The physical infrastructure needed will also depend on the growing demand of the e-commerce industry.

6.3.8.2. Ground

Similar to the aerial domain, ground-based UDS are an emergent industry. Companies are still in early stages of deployment and operate in a limited fashion. The design and manufacture for these vehicles also tend to occur in house. Table 6 provides information for examples of U.S. companies in the endpoint ground UDS domain. These companies were also selected through a review of relevant media [78; 2; 79]. These companies focus on sidewalk delivery, as this domain is the furthest developed and has the most advanced operations. These companies operate in select U.S. cities and have a focus on college campuses. They also sell their robots directly to a variety of consumers, individuals, small companies, and larger corporations to use their technologies to suit their businesses. However, for the purposes of this chapter the focus is on their application for delivery services. The robot specifications differ by company, and Table 6 specifies some of the unique features of each.

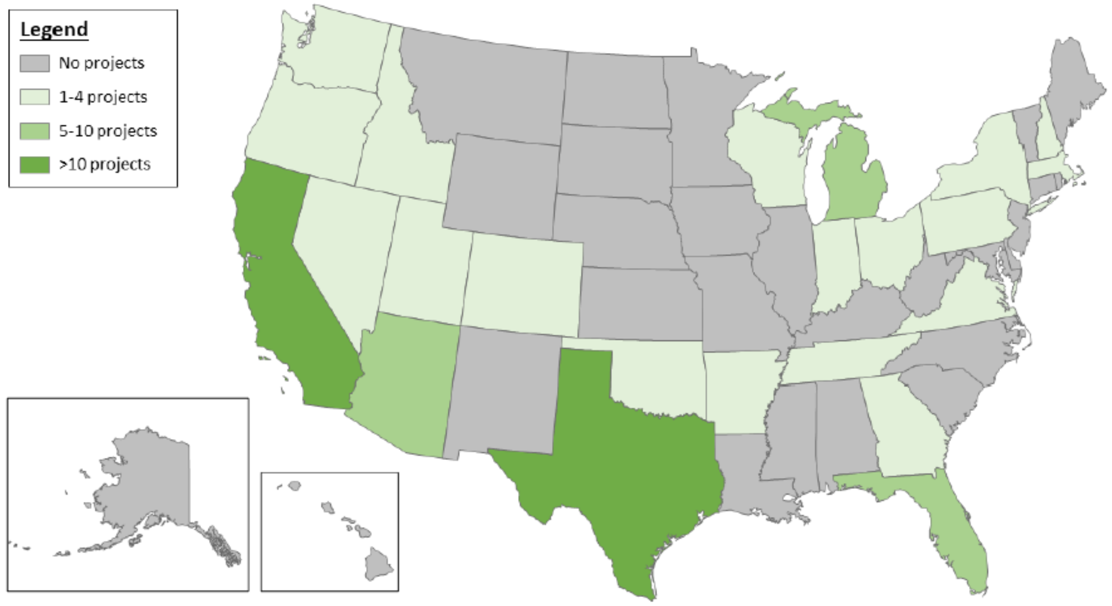
Table 6. Examples of U.S. Companies for Ground UDS

Company	Year Founded	Vehicle Type	Specifications	Technical Features	Design and Manufacture	Operation Status
Starship Technologies	2014	Sidewalk delivery	Payload of up to 22 lbs (10 kg) 1260 Wh Battery for over 12 hours of driving time[a]	Ultrasonic sensors, 12 cameras, radar, GPS, alarm system, reflectors, signal flag, TOF cameras	In house	Currently operate in select U.S. cities and college campuses Operate a fleet of over 1,700 robots daily
Nuro	2016	Road delivery	Payload of up to 419 lb (190 kg)	360° and thermal cameras, LIDAR	In house	First unmanned delivery vehicle to be granted self-driving exemption
Amazon Robotics	2003	Sidewalk delivery	Payload of up to 50 lb[b] (23 kg)		In house	Operating in select cities and college campuses
Robby Technologies	2016	Sidewalk delivery	Can travel 20 miles (32 km)on single battery[c]	LEDs serve both as signal and safety features	In house, specialize in design	Operating in select locations with a variety of commercial partners
Boston Dynamics	Company 1993, delivery robot 2016	Robotic developer and supplier	Payload of up to about 30 lb (14 kg), standard runtime of about 90 min.	5 cameras, field of view 360 degrees	In house	Partners with variety of commercial partners in industries such as food delivery, construction, public safety, etc.[d]
Robomart	2017	Road-based self-driving grocery store	Full-size cars adapted with self-driving software	"grab and go" checkout-free technology	In house	Began selected operations in California[e]
BoxBot	2018	Sidewalk and road-based delivery	Parcel delivery vans, and self-driving electric vehicles[f]		In house	Designs and manufactures a variety of robots in operation

Company	Year Founded	Vehicle Type	Specifications	Technical Features	Design and Manufacture	Operation Status
Kiwibot	2016	Sidewalk delivery	One cubic foot of cargo space, payload capacity unpublished	3 frontal cameras, a rear wide angle 180-degree camera, spot lights, various HD cameras, LTE, GPS, as well as sensors[g]	In house	Select U.S. cities and college campuses
Serve	2011	Sidewalk delivery	Payload of up to 50 Ib (23 kg), can travel for up to 30 min[h]	Electricity-powered robot contains Velodyne LIDAR sensors and a Nvidia Xavier processor	In house	Select U.S. cities, with variety of commercial partners
Piaggio Fast Forward	2015	Sidewalk delivery	Payload of up to 40 Ib[i] (18 kg)	Depth and color sensor, dynamic following technology	In house	Variety of commercial partners
Caterpillar (formerly Marble)	2015	Sidewalk delivery		Advanced sensors and use high-resolution 3D city maps to navigate efficiently	In house, specializes in robots and autonomous software	Variety of commercial partners, specifically meal delivery[j]
Cruise	2013	Road-based delivery	Full-sized vehicles[k]		In house designed software to adapt vehicles to self-driving delivery	Select pilot programs with Walmart

[a] [19], [b] [80], [c] [81], [d] [82], [e] [83], [f] [84], [g] [85], [h] [86], [I] [87], [j] [88], [k] [89]

Ground UDS operate in select locations across the country. These operations tend to be concentrated in certain areas. A 2020 U.S. DOT Volpe Center study cataloged the locations of these operations by State (Figure 1). California has the most operations, as a third of all ground UDS operations (as of 2020) occurred in the State. In addition, Arizona, Florida, Michigan, and Texas host a significant share of current operations as they are often cited as having favorable weather for UDS operation and supportive regulatory environments [2].



Source: USDOT Volpe Center 2020

Figure 1. Map of Identified Ground UDS Operations by State

In addition to the companies above, others specialize in supplying the individual components necessary for the production of ground UDS vehicles. These are the more granular level parts such as batteries, or sensors. For example, U.S.-based companies such as House of Battery and Ultralife Corporation supply batteries to robot manufacturers. The U.S.-based company Quanergy is a key supplier of LIDAR sensors [78]. These parts are not only used in UDS, but are also needed in a variety of industries. Some of the supply chain challenges associated with acquiring these parts are detailed in Section 6.4.

Regarding the physical infrastructure required for ground-based delivery services, as with the aerial domain, the infrastructure required will depend on the level and type of deployment. For example, at higher levels of deployment infrastructure for parking, storage and charging would need to be greatly expanded [90]. Interviews with representatives from industry noted business models are focusing on adapting their services to existing infrastructure dynamics—such as adapting to the layout and details of a certain neighborhood, city, or college campus where the vehicle operates. However, interviewees also mentioned that as these services become more widespread it might be advantageous to have more uniform physical infrastructure configurations for the vehicles to navigate.

Other companies are also developing efforts to introduce unmanned delivery to the long-haul ground delivery industry. For example, Waymo has started a partnership to implement autonomous delivery between UPS centers in Arizona [91]. These long-haul delivery efforts also include applications to the trucking industry. Applications involve both new truck designs specifically for unmanned delivery and adapting existing vehicles with the technology to support unmanned delivery. These efforts are outside of the scope of this chapter, as they support long-haul delivery and are not applicable to endpoint services.

6.3.9. Effects of UDS on the Workforce

The delivery services workforce consists of hundreds of thousands of workers who are tasked with facilitating exchange and delivering goods to millions of customers annually. Delivery service jobs range from the familiar delivery truck driver, to support and logistics roles filled by engineers and logisticians. Endpoint UDS intends to provide services similar to delivery drivers; however, workforce effects may be seen in other sectors of the economy as well, including areas such as agriculture, logging, and mining.

The Bureau of Labor Statistics (BLS) compiles information on a variety of delivery service workers, of which two larger categories that would be affected by UDS adoption are:

1. Light truck drivers
2. Driver/sales workers

Light Truck Drivers
BLS describes the task of light truck drivers:

> Light truck drivers, often called pickup and delivery (P&D) drivers, are the most common type of delivery driver. They drive small trucks or vans from distribution centers to delivery locations. Drivers make deliveries based on a set schedule. Some drivers stop at the distribution center once only, in the morning, and make many stops throughout the day. Others make multiple trips between the distribution center and delivery locations. Some drivers make deliveries from a retail location to customers [92].

There were over one million light truck drivers in May 2021. The median annual wage for light truck drivers was $38,280 in May 2021, similar to $38,920—the median annual wage of occupations typically requiring a high school diploma or equivalent (Table 7, Table 8) [93; 94].

Table 7. Employment Estimate and Mean Wage Estimates, Light Truck Drivers, May 2021

Employment	Employment RSE	Mean hourly wage	Mean annual wage	Wage RSE
1,010,040	0.7 %	$ 20.50	$ 42,630	0.3 %

[a] Source: [93]

Table 8. Percentile Wage Estimates, Light Truck Drivers, May 2021

Percentile	10%	25%	50% (Median)	75%	90%
Hourly Wage	$ 11.72	$ 14.59	$ 18.40	$ 23.46	$ 31.49
Annual Wage	$ 24,380	$ 30,350	$ 38,280	$ 48,790	$ 65,500

[a] Source: [93]

Light truck drivers provide services to a number of different industries, from traditional package deliveries to automotive parts delivery. A large plurality of workers in this field work in courier and express delivery services—these are delivery truck drivers that, for instance, may deliver packages also for online retailers. The mean annual wage for these workers employed by courier and express delivery services was $55,480 in May 2021, significantly higher than for other light truck drivers employed in other industries (Table 9).

Table 9. Industries with Highest Levels of Employment, Light Truck Drivers, May 2021

Industry	Employment	Percent of industry employment	Hourly mean wage	Annual mean wage
Couriers and Express Delivery Services	309,410	33.37	$ 26.67	$ 55,480
Local Messengers and Local Delivery	91,430	56.27	$ 18.70	$ 38,900
Automotive Parts, Accessories, and Tire Stores	67,110	12.37	$ 12.44	$ 25,880
Truck Transportation	57,460	3.85	$ 21.73	$ 45,200
Merchant Wholesalers, Durable Goods (4232, 4233, 4235, 4236, 4237, and 4239 only)[148]	39,800	2.90	$ 19.12	$ 39,770

[148] The merchant wholesalers, durable goods subsector consists of these industry groups: Motor Vehicle and Motor Vehicle Parts and Supplies Merchant Wholesalers (NAICS 4231); Furniture and Home Furnishing Merchant Wholesalers (NAICS 4232); Lumber and Other Construction Materials Merchant Wholesalers (NAICS 4233); Professional and Commercial Equipment and Supplies Merchant Wholesalers (NAICS 4234); Metal and Mineral (except Petroleum) Merchant Wholesalers (NAICS 4235); Electrical and Electronic Goods Merchant Wholesalers (NAICS 4236); Hardware, and Plumbing and Heating Equipment and Supplies Merchant Wholesalers (NAICS 4237); Machinery, Equipment, and Supplies Merchant Wholesalers (NAICS 4238); Miscellaneous Durable Goods Merchant Wholesalers (NAICS 4239) (Source: https://www.bls.gov/iag/tgs/iag423.htm)

[a] [93]

Light truck drivers are distributed widely across the United States, with positions available in all States. In May 2021, the States with the greatest number of light truck drivers were California, Texas, and Florida (Table 10).

Table 10. States with the Highest Employment Level, Light Truck Drivers, May 2021

State	Employment	Employment per thousand jobs	Location quotient[7]	Hourly mean wage	Annual mean wage
California	121,060	7.32	1.02	$ 22.28	$ 46,350
Texas	76,310	6.24	0.87	$ 20.19	$ 41,990
Florida	59,380	6.90	0.96	$ 18.84	$ 39,190
Illinois	57,470	10.23	1.43	$ 22.27	$ 46,320
New York	53,340	6.15	0.86	$ 21.31	$ 44,320

[a] Source: [93]

However, some States had a higher than average level of employment of light truck drivers when compared with the national average, such as Tennessee, Illinois, and Maryland in May 2021, as indicated by their respective location quotients (Table 11).[149]

Table 11. States with the Highest Concentration of Employment, Light Truck Drivers, May 2021

State	Employment	Employment per thousand jobs	Location quotient[7]	Hourly mean wage	Annual mean wage
Tennessee	35,220	11.79	1.64	$ 20.09	$ 41,780
Illinois	57,470	10.23	1.43	$ 22.27	$ 46,320
Maryland	25,190	9.89	1.38	$ 22.01	$ 45,780
Louisiana	16,850	9.40	1.31	$ 17.52	$ 36,430
South Dakota	3,940	9.36	1.31	$ 18.96	$ 39,440

[a] Source: [93]

Driver/sales workers

BLS describes the responsibilities of driver/sales workers as:

> Driver/sales workers are delivery drivers who also have sales responsibilities. They recommend products to businesses and solicit new customers. These drivers may have a regular delivery route and may be responsible for adding clients who are located along their route. For example, they may make regular

[149] The location quotient is the ratio of the area concentration of occupational employment to the national average concentration. A location quotient greater than one indicates the occupation has a higher share of employment than average, and a location quotient less than one indicates the occupation is less prevalent in the area than average.

> deliveries to a hardware store and encourage the store's manager to offer a new product. Some driver/sales workers use their own vehicles to deliver goods to customers, such as takeout food, and accept payment for those goods. Freelance or independent driver/sales workers may use smartphone apps to find specific delivery jobs [92; 95].

There were over 400,000 driver/sales workers in May 2021 (Table 12). The median annual wage for driver/sales workers was $29,280 in May 2021, lower than $38,290—the median annual wage of occupations typically requiring a high school diploma or equivalent (Table 13) [96; 97].

Table 12. Employment and Mean Wage Estimates, Driver/Sales Workers, May 2021

Employment	Employment RSE	Mean hourly wage	Mean annual wage	Wage RSE
477,020	2.4 %	$ 15.37	$ 31,970	0.8 %

[a] Source: [97]

Table 13. Percentile Wage Estimates, Driver/Sales Workers, May 2021

Percentile	10%	25%	50% (Median)	75%	90%
Hourly Wage	$ 8.83	$ 10.85	$ 14.08	$ 18.18	$ 23.01
Annual Wage	$ 18,360	$ 22,570	$ 29,280	$ 37,810	$ 47,850

[a] Source: [97]

Driver/sales employees are employed in a number of industries, including restaurants and nondurable goods delivery (Table 14). Nondurable goods (categories 4244 and 4248) include goods such as groceries and alcoholic beverages [98]. A large plurality of workers in this field work in restaurant delivery services. These workers may be employed by restaurants directly, or are freelance workers employed by third-party companies. The annual average wage for these workers employed in restaurants and other eating places was $24,900 in May 2021, which was lower than driver/sales workers employed in other industries.

Table 14. Industries with the Highest Levels of Employment, Driver/Sales Workers, May 2021

Industry	Employment	Percent of industry employment	Hourly mean wage	Annual mean wage
Restaurants and Other Eating Places	240,040	2.54	$ 11.97	$ 24,900
Merchant Wholesalers, Nondurable Goods (4244 and 4248 only)	80,370	8.66	$ 20.42	$ 42,470
Drycleaning and Laundry Services	19,280	8.35	$ 21.23	$ 44,160
Direct Selling Establishments	12,010	9.25	$ 20.34	$ 42,310
Automotive Parts, Accessories, and Tire Stores	9,100	1.68	$ 13.69	$ 28,460

[a] Source: [97]

Driver/sales workers are distributed across the United States, with most workers in Texas, California, and Ohio in May 2021 (Table 15).

Table 15. States with the Highest Levels of Employment, Driver/Sales Workers, May 2021

State	Employment	Employment per thousand jobs	Location quotient[7]	Hourly mean wage	Annual mean wage
Texas	45,680	3.74	1.10	$ 15.03	$ 31,250
California	41,480	2.51	0.74	$ 18.90	$ 39,320
Ohio	35,140	6.76	2.00	$ 14.20	$ 29,530
Florida	35,070	4.08	1.20	$ 13.59	$ 28,280
Illinois	19,810	3.53	1.04	$ 14.43	$ 30,010

[a] Source: [97]

However, some States had a higher than average level of employment of driver/sales employees when compared with the national average, such as Ohio, North Dakota, and Wyoming in May 2021, as indicated by their respective location quotients[7] (Table 16).

Table 16. States with the Highest Concentration of Employment, Driver/Sales Workers, May 2021

State	Employment	Employment per thousand jobs	Location quotient[7]	Hourly mean wage	Annual mean wage
Ohio	35,140	6.76	2.00	$ 14.20	$ 29,530
North Dakota	2,420	6.12	1.81	$ 22.48	$ 46,760
Wyoming	1,370	5.27	1.56	$ 12.97	$ 26,970
Missouri	14,070	5.16	1.52	$ 16.26	$ 33,820
Kentucky	9,280	5.05	1.49	$ 13.70	$ 28,490

[a] Source: [97]

6.3.9.1. Potential Job Losses

Workforce effects of UDS deployment are the result of a complex interplay between the labor market, technological advancement, costs of deploying UDS systems, and government policy. UDS workforce effects may be examined in the context of automation more generally. Understanding the effects of automation at the firm or sectoral level may be difficult, but broad trends can be observed [99–101]. Overall, automation tends to be neutral in its *net* impact on nationwide unemployment; no strong trends in either direction (either growth or decrease) of unemployment are typically seen. However, differential employment effects may be seen between different groups of workers. High-skill workers are more likely to be either positively or neutrally affected by automation, while low-skill or middle-skill workers are more at risk of negative employment impacts due to labor displacement. Aggregate trends of negative effects in the low-skill labor market do not necessarily generalize to all sectors, or all jobs, however. For instance, within an occupation a particular task may be at greater risk of automation—as Barbieri et al. note, when studies on employment impacts account for specific tasks, negative effects appear lessened [101].

Frey and Osborne calculated "computerisability" scores for 702 occupations in the U.S. economy to model the effect of automation on the workforce more broadly [102]. This study found that 47% of U.S. occupations are at risk for automation. It includes a computerisability probability estimate for light truck drivers (described in the previous section) of 0.69 on a scale from 0 (not computerisable) to 1 (computerisable). This places light truck drivers at rank 380 out of 702 of automatable occupations. This occupational category (53-3033) was included in the training data set, used to train the classification algorithm used in the study, and was hand-labelled as "computerisable" by the subjective assessment of the researchers. Arntz and others (2017) used a similar methodology as Frey and Osborne (2017), but arrived at different conclusions by including task-specific data within job categories [103]. After including this information, the automation risk to U.S. jobs drops down to 9%. This is largely due to the inherent variation of tasks within any given job that a worker performs—some of which are more easily automated than others.

The degree that automation may negatively affect the endpoint delivery workforce could largely depend on the extent to which routine tasks within these jobs can be automated, at a cost-effective rate. There are numerous technological, policy, and supply chain-related concerns that may be hurdles to both ground-based and drone-based UDS from competing with the traditional delivery workforce. However, at a high level, cost comparisons between UDS and current delivery services may provide some indication of which types of delivery jobs may be in greater competition with UDS in the coming years.

Doole et al. (2020) performed a cost analysis comparing e-bike meal deliveries in Paris, France with a hypothetical drone delivery service [104]. The study found that drone delivery was cost effective for "high potential" (multiple large delivery services incorporating drones into their delivery fleet with gradual acceleration in drone demand), and "high acceptability" (rapid growth in technology and full autonomy, which promote economies of scale) deployment scenarios. In the conservative scenario, where BVLOS flight is allowed but societal concerns limit delivery in certain areas of the city, drones were less cost effective. Notably, these scenarios assume fewer drone operators than delivery drivers in all scenarios. For each of the three scenarios, there are 1,455; 582; and 291 drone operators delivering food, whereas in all three cases there were 7,383 e-bike drivers delivering food. This would indicate an aggregate job loss if drones were to dominate the market for food delivery, all else equal. However, caution should be taken when examining these results—the study focused on a particular use-case in a foreign market and may not be reflective of U.S. domestic drone food delivery feasibility.

Tavares (2019) analyzed the cost effectiveness of drone UDS in three scenarios: biomedical sample delivery in Rouen, France; pizza delivery in London, England; and parcel delivery in Brussels, Belgium [105]. While the specific results of this study may have limited applicability to U.S. UDS employment effects due to their focus on non-U.S. markets and deployment environments, the work does provide useful general insights. Cost analyses showed that drone delivery would be most efficient for biomedical samples and food delivery, where the advantages of drone delivery are emphasized. The analysis also indicates that suburban drone delivery may be even more competitive than e-bikes for the food delivery market. The parcel delivery scenario showed an advantage for e-van delivery over drone UDS, due to the ability for vans to hold and deliver multiple packages.

Solutions have been proposed to aid the workers negatively impacted by automation. Programs such as the Trade Adjustment Assistance program [106] have been utilized by the U.S. Government in the past to mitigate negative effects of macroeconomic trends. Further study into workforce retraining and reemployment is needed to provide reliable solutions in this area (see [107] for example).

Overall, further analysis is needed to reach conclusions on potential negative workforce effects due to UDS. This is a nascent industry, with scarce economic impact and deployment outlook data, which makes it difficult to draw strong predictions on how workers may be impacted. Studies into the economics of drone delivery seem to indicate that food delivery workers, who fall under the definition of driver/sales workers in BLS statistics, may face competition due to UDS deployment. There are 240,000 workers employed directly by restaurants to deliver food (note that the total number of workers employed to deliver food from restaurants and similar establishments is likely much larger if third party and self-employed delivery drivers are included). Package delivery services by light truck drivers, such as couriers and express delivery drivers, may be at less risk of direct competition with UDS due to the cost per delivery of UDS compared with light truck drivers, as well as the types of deliveries handled by truck drivers (such as delivering multiple packages to a single location). In any case, UDS could be deployed to complement currently existing delivery jobs and used to complete more niche delivery tasks that are currently inefficient for human drivers or unfeasible with today’s technology.

6.3.9.2. Potential Job Creation

UDS could spur job growth in the U.S. domestic workforce. Direct employment in UDS operation/piloting, research and development, maintenance, and management at UDS development and operator companies may be seen alongside indirect employment effects, such as jobs created by the new demand that UDS brings for products, and from economic growth. However, these effects are largely dependent on the rate of adoption, technological feasibility, cost, and policy realities of UDS deployment.

Jenkins and Vasigh (2013) studied the total economic effect of commercial UAS technology in the United States. This study forecasted the total economic impact of UAS (across all sectors) to total around $82 billion, from 2015 to 2025. In addition, job creation was predicted to total over 100,000 new positions over the same time period. This early study into UAS technology predicted that agriculture and public safety would comprise over 90% of the market of UAS [108]. Though not all UAS activity in the U.S. economy is within the scope of endpoint delivery, this provides useful context for the potential economic impacts of UDS deployment, as an upper bound.

PricewaterhouseCoopers (PwC) in 2016 studied the total addressable market for drone usage in the transportation and logistics industry—meaning direct delivery of products, as well as services accompanying other forms of transportation [109]. According to this study, the addressable global market was around $13 billion for this sector. Applications of drone delivery included package delivery, medical transport, food delivery, and spare parts delivery.

A study by Jenkins et al. (2017) analyzed the economic effect of UAS deployment for package delivery as a disruptive technology [110]. This study estimated that the commercial UDS drone market will conduct between 8 million to 86 million package deliveries daily in the next 20 years. Additionally, these operations were estimated to save companies $2 billion to $10 billion in costs. However, certain conditions were required to achieve these numbers—for instance, BVLOS flights were a precondition to achieving disruptive economic activity.

Levitate Capital (2020) estimated that the drone logistics global market size will be $3.6 billion by 2025 [111]. By 2030, Levitate estimated that the market size will range from $7.1 billion to $47 billion by 2030, with a "base" case value of $33 billion. Various input parameters affect the logistics analysis in this study, including drone unit cost, maintenance costs, and operator-to-drone ratio.

Steer Group (2020) was commissioned by Nuro to perform an economic analysis of autonomous delivery services in the U.S., studying macroeconomic effects as well as effects on the workforce [112]. The study focused on endpoint UDS. This study analyzed three separate adoption scenarios—a conservative, a gradual shift, and a disruptive shift scenario. Under the gradual shift scenario, Steer expects to see a total economic impact of $4.1 trillion, comprising $3.4 trillion in direct economic impacts, and $0.7 trillion in wider economic impacts between 2025 and 2035.

Steer calculated a total employment effect of 34 million jobs generated from 2025 to 2035 in the gradual shift scenario, with 7 million and 43 million jobs created in the conservative and disruptive shift scenarios, respectively. The vast majority of these employees (over 20 million) were from the "pick and pack services/retail" sector—which consists of employees like retail workers (such as in grocery stores) who would be hired to pick out and pack goods to be delivered by UDS. Steer's forecasted economic impacts largely are a product of parameters chosen to input into their models. For instance, Steer models (depending on scenario) assume that a significant portion of vehicle miles traveled (VMT) in the United States would be replaced by UDS as consumers opt for delivery of groceries and other retail goods rather than going on errands. In these calculations, anywhere from 3.1% to 35.6% of in-scope VMTs were replaced by UDS. As with any modeled projections of job growth, these estimates are limited by the assumptions and models used in their generation.

Future job loss due to UDS deployment may be mitigated by overall job growth in the delivery sector. The Occupational Outlook Handbook of the BLS indicates that overall employment of delivery truck driver and driver/sales workers is projected to grow 11% from 2021 to 2031, much faster than the average for all occupations at 15% growth over the same period [92]. Over 174,200 jobs are expected to be added during this time frame (Table 17).

Table 17. Employment Projections Data for Delivery Truck Drivers and Drivers/Sales Workers, 2021-2031

Occupational Title	SOC Code	Employment, 2021	Projected Employment, 2031	Percent Change, 2021-31	Numeric Change, 2021-31	Employment by Industry
Delivery truck drivers and drivers/sales workers	—	1,640,600	1,814,800	11	174,200	—
Driver/sales workers	53-3031	531,000	594,500	12	63,500	Link[b]
Light truck drivers	53-3033	1,109,700	1,220,400	10	119,700	Link[c]

[a] Source: [92]

[b] https://data.bls.gov/projections/nationalMatrix?queryParams=53-3031&ioType=o

[c] https://data.bls.gov/projections/nationalMatrix?queryParams=53-3033&ioType=o

According to BLS, the continual growth of e-commerce will increase demand for delivery services. BLS also comments that drone delivery is expected to complement rather than replace most jobs—thus the downward employment impact of this technology may be reduced.

High-skill labor may benefit significantly from UDS adoption. UDS development is dependent on mechanical, electrical, robotics, and software engineers; computer scientists; technicians; logisticians, and other high-skill capabilities. If UDS are able to move from niche markets to serving the broader delivery market, job creation in these fields would be expected to increase, as is seen in other automation markets.

6.3.9.3. Potential Changes to Existing Jobs

Existing jobs could see substantial changes with the integration of UDS technology in the logistics fleet; however, the exact trajectory of job changes is difficult to predict. Two broad applications of drone-based systems are envisioned in multiple studies—drones delivering packages independently from a depot, and a delivery truck and drone working in tandem (often with a drone deployed from the truck) [113].

In the first case, drones could deliver packages from a depot to customers within their flight range, while standard delivery vehicles or ground-based UDS complete deliveries in harder to reach areas. Drone delivery and truck deliveries could be organized in tandem, so that optimal routes for both are chosen. This could utilize the advantages of both systems—for instance, drone delivery may be optimal for small packages to individual customers, while truck deliveries may be optimal for large packages and when delivering multiple packages to a single location such as an apartment building. In this case, truck drivers may experience little change in their day-to-day work. One possible change would be the routes a driver takes—for example, the driver may spend less time close to a central depot and more time servicing farther locations. Additionally, since small packages would be delivered by drone, the percentage of small packages delivered by a human could decrease—thereby increasing the average package weight that a truck driver must deliver.

The second scenario would see more changes to the job description of delivery drivers. Instead of delivering packages along a normal route by truck alone, the truck would act almost as a mobile depot for a drone UDS. Studies researching this scenario suggest that the truck would drive to a service area, then release a drone to deliver packages—meanwhile, the truck will continue driving along its own route and delivering packages as well. In this scenario, a driver would be tasked with not just operating their own vehicle, but also potentially (and separately while the vehicle is stopped) preparing and deploying the drone for delivery and recovering the drone after the delivery is complete. The driver may also be tasked with basic troubleshooting for drone issues—though for more complex issues, a dedicated maintenance team would be employed or contracted for the drones.

6.3.9.4. Potential Effects on Job Quality

Delivery service work typically requires a mixture of driving, walking, and carrying packages from a truck or car to its final destination. These tasks are performed in many different environments, in all four seasons, every year, and often on a time crunch as customers expect their packages to be delivered in a timely manner. In short, these jobs are physically demanding and stressful [92]. According to BLS data, the couriers and express delivery services industry had one of the highest injury and illness incidence rates in 2020 at 7.5 cases per 100 full-time workers, which was higher than the national rate for private industry of 2.7 [114]. These injuries can be sustained during lifting and carrying of heavy packages, and motor vehicle crashes.

As automation becomes more normalized in the delivery sector, there could be numerous changes to job quality. First, in the case of UDS with a human in the loop, such as a drone operator or observer, there is a shift from physically demanding and difficult outdoor jobs, to less demanding office-based jobs. If drone pilots or observers are able to operate offsite, the working environment for delivery workers could improve significantly. Additionally, UDS deployment could require significant numbers of technician-related positions. Technician jobs, while they may require work in the field, may not require the types of heavy lifting and driving that causes injury.

Automation could also bring improved job quality for the typical delivery driver in currently existing positions. For instance, drone plus truck combination delivery systems could reduce the amount of time on foot or walking distance of the delivery driver, as drones take care of lighter packages, delivered to potentially more distant areas—while the delivery driver is free to deliver more packages to a single location. Complementary roles between humans and drones or ground-based UDS could free up human labor to perform more productive and less strenuous tasks. On the other hand, if UDS are tasked with delivering lighter packages, it could be the case that a greater percentage of packages that humans hand deliver would be heavy.

6.3.10. Federal Activity Related to UDS

Federal agencies interact with UDS stakeholders and related technologies through their regulatory authorities; research, development, and standards activities, and operations. FAA and DOT have regulatory authority over aspects of UDS operations and systems. A larger number of agencies study, develop, or use technologies not explicitly designed for UDS applications but which are enabled by the same underlying technological capabilities such as unmanned aircraft or ground vehicles. Interagency efforts, both formal research collaborations and informal coordination, contribute to the development of technologies and inform regulations that will advance and govern the deployment of UDS systems.

6.3.10.1. Federal Agencies with Jurisdiction

Federal jurisdiction over UDS depends on the operating domain of the service. FAA has statutory authority over aviation safety and FAA rules apply to the U.S. National Airspace System, while DOT has statutory authority over safety for ground-based vehicles that operate on roads and highways.

A few agencies have jurisdictions that overlap with aspects of both aerial and ground-based UDS technologies. The National Transportation Safety Board (NTSB) is an independent agency tasked with investigating aviation and surface-based transportation accidents.[150] NTSB issues recommendations to Federal agencies and others based on their findings with the goal of helping to prevent accidents and saving lives [115]. The FCC regulates spectrum use, a limited resource underlying electronic communications infrastructure that may enable large-scale vehicle automation and navigation. Previous Administrations recommended reserving the 5.9 GHz "Safety Band" for the exclusive use of transportation safety applications [116; 117]. In November 2020, the FCC reallocated portions of the Safety Band for unlicensed Wi-Fi use over the objections of the NTSB [118].

Aerial UDS

All UAS must be registered with the FAA. UAS registration is valid for 3 years [119]. UAS operators may be required to apply for additional certifications or authorizations depending on the type of UAS, the flight path of the UAS, and the purpose of the flight. The FAA prohibits UAS operations within certain airspace, including over airports, military bases, nuclear power plants, and other critical infrastructure [120].

Existing FAA UAS rules and regulations use the principle of "operational segregation" between crewed and unmanned aircraft to ensure safety, but the FAA is working towards the integration of UAS into the NAS to enable safe UAS operation in airspace shared with crewed aircraft and to harmonize UAS operations with existing air traffic management systems and procedures [119].

Although the FAA is the Federal agency primarily responsible for aviation safety and the NAS, aircraft landing sites fall under the land use powers of State and local authorities. State, local, and Tribal governments and UAS operators and manufacturers participated in the DOT UAS Integration Pilot Program (IPP) that will inform the FAA's efforts to determine how to

[150] See NTSB authorizing language: https://www.govinfo.gov/content/pkg/USCODE-2014-title49/pdf/USCODE-2014-title49-subtitleII-chap11-subchapIII-sec1131.pdf

involve local communities and address local concerns related to UAS airspace integration. Commercial UAS operators and manufacturers also participated in the IPP, which concluded in October 2020. FAA's BEYOND program is a continuation of FAA's UAS integration efforts [121].

UAS operations occur primarily under 14 CFR parts 91 and 107, with package delivery occurring under part 135. Additional rules apply to certain types of UAS operations [122]. Developers of package delivery by drone services who participate in FAA's UAS integration program are moving towards proof-of-concept testing through FAA's existing Part 135 certification process for air cargo carriers. Small drone operators that intend to "carry the property of another for compensation beyond visual line of sight" must apply for Part 135 Air Carrier or Operating certificates; certificates are issued depending on the types of services the operator plans to provide and the location of their operations. The FAA grants exemptions to UAS applicants for specific Part 135 rules not applicable to UAS (e.g., requirements to keep flight manuals inside operational aircraft). Additional airspace authorizations and certificates may be required. The first single-pilot Part 135 certificate for a UAS was issued to Wing Aviation., and as of Fall 2021 the FAA was reviewing two UAS applications for part 135 certificates (all submitted by operators participating in IPP and FAA Partnership for Safety Plan participants) [123; 124; 74].

At the international level, FAA has working relationships with other Civil Aviation Authorities (CAAs) and international organizations. FAA participates in the International Civil Aviation Organization (ICAO) Remotely Piloted Aircraft System (RPAS) Panel and the Joint Authorities for Rulemaking on Unmanned Systems (JARUS)—another international body that develops recommended requirements for civil aviation authorities [122].

In August 2022, the NTSB finalized a rule amending its definition of "unmanned aircraft accident" to require notification of accidents involving UAS with an airworthiness certification requirement rather than the previous classification based on aircraft weight to allow the NTSB to "respond quickly to UAS events with safety significance, while not burdening the agency or public with unnecessary responses" [53].

Ground-based UDS

Ground-based UDS may eventually traverse pedestrian sidewalks, public and private roads, or highways. State and local authorities are typically responsible for issues pertaining to sidewalk construction, maintenance, and use—as mentioned previously, Federal authorities have limited jurisdiction over sidewalks beyond the Americans with Disabilities Act (ADA) design guidelines meant to ensure no new barriers to access are created—and design and maintenance can vary significantly within city limits [2]. Vehicles that operate on public roads are regulated at both the State and Federal level. State responsibilities include driver licensing, insurance, vehicle registration, and establishment of traffic laws, while the Federal Government is primarily responsible for motor vehicle and motor carrier safety.

A 2021 Congressional Research Service report, *Issues in Autonomous Vehicle Testing and Deployment*[151], provides a detailed summary of congressional legislation and White House policies related to the role of Federal Government in the development of autonomous vehicle

[151] See https://crsreports.congress.gov/product/pdf/R/R45985

technologies; this section will primarily focus on current Federal jurisdictional authorities for autonomous vehicles as they relate to UDS.

Vehicle and vehicle equipment manufacturers must adhere to the FMVSS issued by NHTSA applicable for its particular vehicle or equipment type. Conventional safety features such as seat belts are required for certain vehicles under FMVSS, but these components may be unnecessary in vehicles designed for unmanned operation. NHTSA can exempt automakers from specific FMVSS standards if automakers meet the statutory bases for such accommodations. In 2020, NHTSA approved a petition for temporary FMVSS exemptions filed by Nuro, a U.S. company developing self-driving delivery vehicles. Nuro was granted a 2-year exemption from specific standards to produce up to 2,500 vehicles per year over 2 years. The terms of the exemption give NHTSA additional oversight over Nuro's vehicle operations and establish a number of requirements to which Nuro must adhere [125]. In February 2022, General Motors applied for an exemption for its Cruise Origin—an electric, autonomous passenger vehicle designed for the commercial market [126]. In March 2022, NHTSA amended the FMVSS to resolve ambiguities and avoid unnecessary terminology not applicable to automated vehicles by defining terms like "manually operated driving controls" and excluding occupant-less vehicles from the 200-Series FMVSS whose objective is to protect a vehicle's occupants [127].

DOT has adopted the SAE International (formerly Society of Automotive Engineers) classification system for vehicle automation that defines six levels of automation based on vehicle capabilities, where Level 0 vehicles have no automation and Level 5 systems can drive the vehicle under all conditions. As of 2021, the most advanced commercially available vehicles were classified as Level 2, although Level 3 vehicles may soon become available. Standardized nomenclature will help facilitate effective communication between developers, regulators, and the public as vehicle automation technologies mature [117].

6.3.10.2. Interagency Activities – Research and Development

While development of deployable UDS technologies and platforms is primarily driven by the private sector, the Federal Government plays an important role in UDS research and development and standards development. Regulatory and science-focused agencies like FAA and NASA frequently collaborate on the development and evaluation of technologies that will help enable the safe integration of UAS technologies into U.S. airspace. NIST collaborates with NHTSA on concepts for automated driving systems safety and with the FAA and others on drone and robotics safe performance measurement methods. The National Science Foundation supports the development of education and training programs that prepare students for the FAA's UAS General Exam, Remote Pilot Certificate, and Field Technician Certificate. Examples of interagency research activities are highlighted below.

UAS Traffic Management and ATM-X

UAS Traffic Management (UTM) services are designed for sUAS typically flying under 400 feet and are separate but complementary to air traffic management for crewed aircraft. As part of UAS integration efforts, the FAA will begin field-testing the UTM system in 2022, which will help the FAA develop new policies and standards for beyond line of sight UAS operation [128; 129]. FAA and NASA developed a UTM Research Plan that details research objectives for UTM and have partnered with industry to form a Research Transition Team that coordinates on UTM activities [34]. DHS, NASA, and other agencies and industry partners also contribute to this effort [122].

NASA continues to work towards the integration of new types of aircraft into air space through the Air Traffic Management – eXploration (ATM-X) project in partnership with the FAA. ATM-X work is divided into four subprojects: Digital Information Platform; Urban Air Mobility Airspace Management, Pathfinding for Airspace with Autonomous Vehicles; and Extensible Traffic Management. As of June 2020, the ATM-X project has proceeded into Phase 2, which begins to address key technical challenges identified in Phase 1 [130].

UAS Test Site Program

Seven FAA-designated UAS Test Sites have been established since 2014 with the objective of providing "verification of the safety of public and civil UAS, operations, and related navigation procedures before their integration into the NAS." The UAS Test Site Program also helps support the FAA's "development of certification standards, air traffic requirements, coordinating research and other work with NASA, FAA NextGen, the Department of Defense, and other Federal agencies" [3].

Public aircraft operators and civil aircraft operators are eligible to participate in the program. Public aircraft operators focused on governmental activities (e.g., aeronautical research, search and rescue, public safety) work with public safety officials on training support, demonstrations, and integration of UAS technologies. The UAS Test Sites support civil operators by helping them develop concepts of operations and risk management plans, and assist them with flight-testing of their technologies. Part of this support includes assisting operators with certification or waiver processes needed to fly.

The UAS Test Sites conduct research and demonstration operations to support the advancement of technologies and capabilities such as: detect and avoid, BVLOS operations, and counter UAS [131].

6.3.10.3. Interagency Activities - Federal Coordination and Informal Collaboration

Informal conversations and established working relationships between Federal agencies increase awareness of the state of AV and UAS technologies and present opportunities for formal collaborations that address shared challenges. There are numerous interagency groups that coordinate on Federal use and integration of UAS technologies. A few of these interagency activities are described below; additional lists and descriptions can be found in the "Update of the FAA Comprehensive Plan and Unmanned Aircraft Systems (UAS) Program Alignment" [3]. Federal activities related to AV technologies are primarily conducted by agencies and offices within DOT, although a more comprehensive list of potential areas of Federal collaboration are described in a 2020 report published by NSTC and DOT, *Ensuring American Leadership in Automated Vehicle Technologies: Automated Vehicles 4.0 (AV 4.0)* [132].

Unmanned Aircraft Systems (UAS) Beyond Visual Line-of-Sight (BVLOS) Operations Aviation Rulemaking Committee (ARC)

The UAS BVLOS ARC consisted of members from industry, academia, and local, State, and Federal Government and was convened by FAA to "provide recommendations to the FAA for performance-based regulatory requirements to normalize safe, scalable, economically viable, and environmentally advantageous UAS BVLOS operations." The committee released its final report in March 2022, describing a list of recommendations to FAA including setting an acceptable level of risk consistent across types of operations, modifying right of way rules in low altitude areas, and creating a new remote pilot certification to cover BVLOS beyond the scope of Part 107 [133].

Interagency Unmanned Aircraft System (UAS) Program

The Interagency UAS Program enables coordination on fire UAS operations and consists of members of the National Interagency Fire Center (NIFC), including the Bureau of Land Management, U.S. Fish and Wildlife Service, Bureau of Indian Affairs, U.S. Forest Service, and National Park Service. The Interagency UAS Program website contains resources and information for Federal users of UAS services [134].

UAS Executive Committee (ExCom)

ExCom was established by Congress in 2009 to "serve as a focal point for resolution of policies and procedures relating to UAS access to the NAS" and supports "operational, training, developmental, and research requirements" for the DHS, DOC, DOD, DOE, DOI, DOJ, State, FAA, and NASA. Agency leadership involved in UAS integration meet quarterly [3].

Federal Fleet Policy Council (FEDFLEET)

FEDFLEET helps to coordinate Federal vehicle management programs and policies and analyzes the impacts of current and proposed Federal and international policies. Although the council is focused on federally owned vehicles, it may help to foster interagency coordination on issues related to AVs [134].

6.3.10.4. Other Federal Activities

Although few agencies are directly responsible for managing or regulating UDS technologies, numerous agencies use unmanned systems or fund research and economic development activities that encompass UAS or AV technologies related to UDS. This subsection provides descriptions of agency activities that could contribute to the development or adoption of UDS. Federal activities were identified through interviews and review of publicly available literature, primarily the following two reports: (1) *Standardization Roadmap for Unmanned Aircraft Systems*[152], published by the ANSI Unmanned Aircraft Systems Standardization Collaborative (UASSC), and (2) *Ensuring American Leadership in*

[152] See https://share.ansi.org/Shared%20Documents/Standards%20Activities/UASSC/ANSI_UASSC_Roadmap_V2_June_2020.pdf

Automated Vehicle Technologies Automated Vehicles 4.0[153], published by NSTC and DOT in 2020.

Department of Commerce (DOC)

NIST

NIST is a non-regulatory agency that "promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology." At present NIST does not develop UDS-specific test methods, but develops measurements and standards infrastructure for teleoperation and automation, sensing and perception, robotics, and other technical capabilities that underlie UDS systems. For example, NIST has produced a number of frameworks (e.g., the NIST Risk Management Framework, Privacy Framework, and IoT Cybersecurity Guidelines) that can be readily adapted by the UDS sector, including approaches that provide organizations with flexible, risk-based processes that help address associated security and privacy concerns [135–139].

Much of the UAS-related work conducted by NIST has focused on emergency responder and military applications. NIST research has led to the development of the ASTM International "Standard Test Methods for Response Robots" that provide test methods that have been used by the Federal Government to evaluate and procure aerial or terrestrial response robots. NIST has also funded research into the use of UAS for public safety applications (e.g., search and rescue, natural disaster management) [122].

NOAA

The National Oceanic and Atmospheric Administration (NOAA) uses unmanned aerial and maritime systems (UxS) to better monitor and understand the global environment to support its mission of "science, service, and stewardship." In 2021, NOAA released their Unmanned Systems Strategic Plan[154], which laid out the following goals:

- Goal 1: Coordinate and Support UxS Operations at an Enterprise Level.
- Goal 2: Expand UxS Applications Across NOAA's Mission Portfolio.
- Goal 3: Accelerate Transition of UxS Research to Applications.
- Goal 4: Strengthen and Expand UxS Partnerships.
- Goal 5: Promote Workforce Proficiency in UxS Use and Operations.

Although NOAA's strategic plans do not indicate any current or intended use of UxS for delivery applications, the agency "prioritizes strategic investments in unmanned systems applications and technologies that fuel innovation and strengthen operations, and accelerates and enhances capabilities through partnerships," work that may contribute to the development or optimization of technologies that underlie UDS [122].

[153] See https://www.transportation.gov/sites/dot.gov/files/2020-02/EnsuringAmericanLeadershipAVTech4.pdf
[154] See https://sciencecouncil.noaa.gov/Portals/0/NOAA%20Uncrewed%20Systems%20Strategic%20Plan%201.19.2021.pdf?ver=2021-01-22-134232-833

International Trade Administration (ITA)

The ITA is a DOC agency whose mission is to "Create prosperity by strengthening the international competitiveness of U.S. industry, promoting trade and investment, and ensuring fair trade and compliance with trade laws and agreements" [140]. ITA's Industry & Analysis (I&A) Aerospace Team facilitates connections between UAS industry members and Federal agencies (including FAA, TSA, NASA), and provides a representative to UAS EXCOM.

Bureau of Industry and Security (BIS)

The Bureau of Industry and Security (BIS) is involved in the management of export control issues that may affect UAS. Large UAS with a range over 300 km or a payload capacity greater than 500 kg are considered Category I items under the Missile Technology Control Regime, and as such "face a strong presumption of denial of export to anyone except allies." Many UAS components and systems require export licenses under the International Traffic in Arms Regulations (ITAR) process or Export Administration Regulations (EAR).

Department of Homeland Security (DHS)

DHS uses UAS technologies for remote monitoring and emergency response activities in pursuit of its mission to ensure national security. DHS supports the First Responder Robotic Operations System Test (FRROST) Small UAS for Search and Rescue project to assess how commercially available sUAS could be used for first responder missions [141]. Recognizing the potential for UAS to be used for nefarious purposes, DHS also works to protect the United States from UAS-based threats. DHS has statutory authority to "counter credible threats from unmanned aircraft systems (UAS) to the safety or security of a covered facility or asset" under the Preventing Emerging Threats Act of 2018 [122]. The DHS Cybersecurity and Infrastructure Agency (CISA) also produces standards and best practices for operating commercial UAS to help users protect their networks, information, and personnel [142].

DHS Science and Technology Directorate (S&T) test sites are used for demonstration, testing, and training of UAS. DHS S&T works with NIST to contribute to the development of standard test methods (published by ASTM International) that measure robot maneuverability, safety, autonomy, and other characteristics to ensure operator confidence [122].

Department of Justice (DOJ)

DOJ is working to understand and mitigate the risks posed by UAS and AVs. The DOJ UAS Working Group (chaired by DOJ Office of Legal Policy) is "responsible for coordinating and discussing matters relating to the use of UAS and efforts to counter the threat of malicious UAS." The working group includes many of the DOJ's investigative agencies (e.g., Federal Bureau of Investigation; Drug Enforcement Administration; Bureau of Alcohol, Tobacco, Firearms and Explosives) and attorney's offices (the Office of Legal Policy, the Office of Community Oriented Policing) [143]. The DOJ National Institute of Justice (NIJ) has provided funding to researchers working to identify and mitigate AV systems' vulnerabilities to cyberthreats [143].

Department of the Interior (DOI)

The DOI has become a major user of UAS due to its need for large amounts of remote sensing data. In FY18 DOI conducted over 10,000 flights through its UAS program, which aims to "maintain standardization of UAS platforms while building a variety of payloads" [123]. As discussed above, the Bureau of Land Management, U.S. Fish and Wildlife Service, and Bureau of Indian Affairs are all users of UAS services and are members of the Interagency UAS program that coordinates fire UAS operations [134].

NASA

NASA Ames Research Center led the UTM and ATM-X projects in collaboration with the FAA. NASA's goals for the UTM project, which concluded in May 2021, were to "create a system that can integrate drones safely and efficiently into air traffic that is already flying in low-altitude airspace" [144]. NASA's findings from the UTM project were transferred to the FAA, which is continuing to work on the implementation of a UTM system. Additional NASA projects and missions are developing aircraft automation technologies, including the Advanced Air Mobility mission, which includes the Integration of Automated Systems, a "multi-year test campaign that will focus on testing automation needed to enable scalable Urban Air Mobility (UAM)," and the Automated Flight and Contingency Management subproject that researches automation for "highly-integrated, vehicle and pilot interface systems" [145].

National Institute for Occupational Safety and Health (NIOSH)

NIOSH contributes to UDS research and development primarily through their Center for Motor Vehicle Safety (CMVS). CMVS collaborates with internal and external partners to conduct research and develop strategies to prevent work-related motor vehicle crashes and resulting injuries. The CMVS strategic plan for 2020 to 2029[155] includes goals related to addressing vehicle automation challenges (e.g., "Assess employee drivers' comprehension and use of advanced driver assistance systems (ADAS) and automated driving systems (ADS) in commercial motor vehicles" and "Develop and evaluate strategies to improve employee drivers' understanding of the capabilities of ADAS and ADS in commercial motor vehicles"). CMVS also participates in ANSI and the American Society of Safety Professionals (ASSP) subcommittees related to vehicle automation and has contributed to White House and National Safety Council reports on automated vehicles.

Office of Science and Technology Policy (OSTP)

The White House Office of Science and Technology Policy (OSTP) has developed extensive guidance for ensuring that automated systems work for the American people. In the Blueprint for an AI Bill of Rights, OSTP provides extensive guidance to ensure that automated systems are safe and effective and protect people's data privacy. The document comes with a

[155] NIOSH [2020]. NIOSH Center for Motor Vehicle Safety Strategic Plan, 2020–2029. By Pratt S, Retzer K, Rodríguez-Acosta R, Olsavsky R, Fosbroke D. Morgantown, WV: U.S. Department of Health and Human Services, Centers for Disease Control and Prevention, National Institute for Occupational Safety and Health, DHHS (NIOSH) Publication 2020–126, https://doi.org/10.26616/NIOSHPUB2020126

technical companion that provides specific technical steps that the developers of automated systems, including UDS, can take to build protections into their automated systems.

U.S. Department of Agriculture (USDA)

Forest Service

The Forest Service uses UAS to support forest conservation and management, and wide-ranging research activities (e.g., forestry, biological and physical science, socioeconomics). As part of these efforts, the Forest Service has partnered with NASA, DOD, and DOI to conduct "research to operations" activities to assess how UAS could be used for wildfire management and response. In 2020, the Forest Service released its *Forest Service Standards for UAS Operations*, outlining internal procedures that "promote safe, efficient and lawful operation of unmanned aircraft systems (UAS)" [146].

Agricultural Research Service

The Agriculture Research Service (ARS) uses sUAS to support research questions related to cropping and livestock systems in multiple locations across the country. ARS partners with universities and other federal agencies to conduct experimental research, which is often tied to developments in robotics, phenomics, precision agriculture, and the use of artificial intelligence. Additionally, ARS is engaged in research on ground-based unmanned devices and is exploring further partnerships to develop and deploy robotics and artificial intelligence to improve agricultural input delivery and research sampling including sample delivery to the researcher or lab facility.

National Institute of Food and Agriculture

The National Institute of Food and Agriculture (NIFA) funds projects that support the use of unmanned aerial and ground systems for precision agriculture, labor saving and assistive field operations, and wildfire management. In addition to two in-house Engineering programs and the Specialty Crops Research Initiative (SCRI), NIFA has partnered with the National Science Foundation on the National Robotics Initiative (now Foundational Research in Robotics), Cyber-Physical Systems, and Signals in the Soil programs to provide extramural funding for unmanned aerial and ground systems.

National Science Foundation

The National Science Foundation supports research to enable continued U.S. innovation and leadership in UAS technologies. This includes multidisciplinary research connecting computer science, engineering, and social sciences in use-inspired contexts such as geosciences and agriculture. This research aims to improve 1) the autonomy of these systems, allowing them to operate with minimal human control in unknown, dynamic environments; 2) their safety, enabling dependable operations in populated areas and in national airspace; and 3) their intelligence, enabling independent decision-making and adaptive behavior. Areas of research include communication, real-time control, autonomous decision-making, multi-vehicle coordination, task and path planning, ethics, and remote monitoring (e.g., for natural hazards and disaster reconnaissance). Relevant NSF programs include Foundational Research in Robotics, Cyber-Physical Systems, Smart and Connected Communities, and CIVIC Innovation Challenge. Inter-agency coordination is facilitated by the NITRD program, for example, through its working groups on Intelligent Robotics and Autonomous Systems and on Cyber-Enabled Networked Systems Physical Systems.

U.S. Postal Service (USPS)

The USPS conducts AV demonstration programs to assess how automation technologies could be used to improve the efficiency and safety of postal delivery services. They have partnered with university researchers on the Automated Rural Delivery Vehicle (Zippy) Program and completed a pilot program for an automated tractor-trailer proof-of-concept vehicle [134].

6.4. Marketplace and Supply Chain

6.4.1. Risks Posed to the Marketplace and Supply Chain

Liability, public perception, and an uncertain regulatory environment are potential risks for UDS developers and investors. Liability in the event of bodily harm or property damage requires UDS operators to self-insure or acquire private insurance for their operations. Insuring emerging technologies like UDS carries inherent uncertainties due to a scarcity of data; insurance premiums are calculated to assume a conservative worst case scenario so may be higher compared to other types of commercial insurance coverage. The need to self-insure or acquire specialty insurance can deter smaller companies, who can help to advance the technology but do not have the same financial resources as large tech companies, from entering the marketplace. This represents a risk to competition and diversity in the marketplace. Outside of the financial repercussions of a collision, any incident involving UDS could have drastic consequences for public perception and acceptance of the technology. In 2017, the USPS Office of Inspector General conducted an online survey to gauge public perception of driverless vehicles for long-haul trucking and endpoint delivery. They found that 40 percent of Americans thought self-driving delivery trucks would be less safe than human-driven delivery trucks, while only 24 percent thought they would be safer (23 percent said safety would be about the same and 12 percent were unsure). However, they found that knowledge of and exposure to information about self-driving vehicles correlated with a belief that self-driving delivery vehicles are safe [92]. A 2021 literature review of public acceptance studies surrounding AV's found little academic research has been done on how AV collisions affect public perceptions [147]. One study has sought to quantify the effects of a 2019 AV collision on public attitudes through semantic analysis on Twitter data. The authors conclude that after the crash there was a decrease in tweets expressing positive sentiments about AVs, while the number of negative tweets remained the same, which may indicate that people who previously expressed favorable views toward AVs no longer felt as positively toward AVs after the collision [148].

A slow-moving and opaque regulatory environment can be a market risk that threatens companies' commercial viability in the United States. Unlike other countries such as Germany, the United States does not yet have an established Federal policy governing the deployment and use of automated vehicles [149]. Work to strengthen U.S. policies on aerial UDS is a priority of the Administration, including addressing the danger of early monopolization of aerial UDS while promoting competition and economic opportunity [150]. Some UDS companies operate in other countries where they perceive regulations as being more favorable to the testing and development of UDS technologies. It typically takes many years to develop and establish new regulations in the United States—UDS operators said these timelines are often incompatible with a venture capital-backed startup's need to generate revenue and create returns for investors, in addition to managing business logistics challenges such as staffing and equipment production.

Industry highlighted market factors related to regulatory environments as presenting a major risk to their businesses and characterized supply chain risks as a less pressing issue. Potential supply chain risks include semiconductors and batteries as components that may be more challenging to source, especially if UDS companies scale up their operations and demand for delivery vehicles grows. UDS technologies share the same supply chain concerns that are becoming increasingly prevalent across industry domains. Semiconductors are critical components used for UDS power control, automation, and processing—and global supply chain shortages of these parts are widely reported. A 2021 report notes only 12% of global semiconductor manufacturing capacity is located in the United States [151]. The market for high-capacity batteries is also becoming increasingly competitive, as demand for energy storage capacity increases [152]. UDS technologies generally use lightweight, high-capacity batteries (most often Lithium-ion) to optimize the weight and range of the vehicles. However, U.S. facilities comprise only 6% of new lithium-ion battery manufacturing facilities currently planned or under construction [152].

6.4.2. Risks to the National Security, Including Economic Security, of the United States

Domestic UDS deployment, or lack thereof, has the potential to significantly impact the national security, including economic security, of the United States. As with related technologies, such as AVs [153], direct competition between U.S.-based companies and foreign companies is expected in the UDS field. U.S. UDS companies may face economic risks if the market is slow to develop or supply chain issues make it difficult to meet market demand. Economic risks can also feed into national security risks, where foreign-controlled supply chains for UDS drones and AVs create vulnerabilities to defense and homeland security (e.g., adequate procurement, cybersecurity risk, foreign control of UDS near sensitive facilities).

Economic risks relating to UDS could be seen if domestic UDS companies, both in manufacturing and logistics, have difficulty creating a market or meeting a market demand within the United States. A U.S. foothold in the UDS market would provide the basis for domestic investment and supply chains, which could result in international competition in favor of U.S.-based companies. On the other hand, if international markets become dominated by foreign-owned companies, domestic companies would be at risk of being outcompeted by more established foreign firms. The economic viability of U.S. UDS deployment is a key question that may determine the outcome of this international competition. Alongside workforce and supply chain-related issues of a primarily foreign nation dominating the UDS market, the issue of technological standards setting could be at risk—the U.S. market could become dependent on foreign standards setting rather than providing significant input into the international standards process. This could have follow-on effects on how well UDS integrates with other U.S. technologies and priorities. Traditionally, the United States has benefitted from being in a strong position for technological standards setting [46].

The economic risks feed into national security risks. Foreign-controlled supply chains for UDS drones and AVs could create supply chain insecurity for defense-related applications of these technologies. Foreign parts and construction introduce complications for procurement of these technologies for government functions. Additionally, foreign manufactured drones and AVs may pose a national security threat, particularly in the area of cybersecurity [154]. Foreign cybersecurity threats, coupled with other risks associated with UAS [155], could lead to heightened national security fears surrounding UDS technologies.

6.4.3. Emerging Risks and Long-term Trends in the Marketplace and Supply Chain

Nascent UDS technologies and operations are expected to mature and become more widespread in the coming years, although the extent of this growth will be driven and limited by policy, consumer demand, and public perception. A 2018 study estimates that by 2040 the United States will need between 300,000 and 1 million automated delivery vehicles [156]. This study assumes these vehicles will replace between 30% and 50% of projected deliveries based on historical increases of e-commerce shopping.

Experts theorize that on-demand delivery enabled by UDS has the potential to increase overall consumer demand for delivery services, in addition to replacing demand for delivery services performed through conventional modes of transportation. As delivery becomes faster and more convenient, consumers may order goods in smaller quantities and more frequently, replacing trips to the grocery store with e-commerce orders [156].

Widespread automation for UDS and transportation modes could lead to benefits for the environment, public safety, and operational efficiencies by decreasing the number of human drivers on the road. Although experts agree that a fully automated transportation network is not possible in the near future, higher levels of automation could reduce traffic, lower emissions, and decrease fatality rates [1; 58].

6.5. Recommendations

The following recommendations are based on review of publicly available academic articles and grey literature, responses to the public request for information, and conversations with Federal employees, representatives from the UDS industry, and users of UDS from local government and businesses. The recommendations stem from particular challenges and potential opportunities identified throughout the course of preparing this chapter and address:

- Advancing widespread adoption of UDS in the United States and in a global market;
- Mitigating current and emerging risks to the marketplace and supply chain; and

- Strengthening the role the United States plays in informing and establishing globally recognized norms and standards for UDS.

Challenge 1: *Increasing UDS deployments poses new risks to safety, security, and privacy.*

A strategy based on existing best practices and extending to large-scale deployments is needed to enable effective risk-based management of UDS implementations.

Recommendation 1a: Expand and strengthen existing coordinated efforts by DOT, NASA, DOL, and other Federal agencies—working in partnership with State and local entities, industry, and others—to develop operational frameworks that prioritize safety and accessibility for people while balancing the economic and societal benefits of UDS capabilities.

Recommendation 1b: Establish industry-wide best practices for security, privacy, and risk management. These can include examining and adapting existing frameworks and best practices for implementation in the UDS sector, including NIST's risk management framework, privacy framework, and IoT cybersecurity guidance, OSTP's *Blueprint for an AI Bill of Rights*[156], and NTIA's *Voluntary Best Practices for UAS Privacy, Transparency, and Accountability*[157].

Challenge 2: *Effective use by UDS systems of road networks and airspace requires integrating a range of policy, regulatory, and legal environments.*

A strategy for cooperation, coordination, and conflict resolution across policy, regulatory, and legal stakeholders at local, State, Tribal, territorial, and Federal levels is needed to resolve new issues posed by UDS in areas such as privacy, property rights, jurisdiction, liability, and other elements.

Recommendation 2a: Undertake a study, led by stakeholder legal and regulatory experts/associations with engagement from existing State and local drone policy/legislation task forces, to develop consensus around the highest priority policy, regulatory, and legal barriers to growth of the UDS sector.

Recommendation 2b: Convene a series of joint task forces addressing each of the highest priority barriers for UDS. Task forces led by the DOJ and DOT should work in conjunction with other agencies, State and local attorneys general, legislative councils, and other relevant legal and regulatory stakeholders to identify best practices, Federal regulations, and consensus solutions for the removal of existing barriers.

Challenge 3: *The UDS sector operates at the leading edge of technologies and its continued growth relies on research and development for next generation capabilities.*

UDS technologies and operational concepts are intrinsically multi-technology, multi-sector, and multi-disciplinary. A coordinated strategy for Federal research and development investments is needed to link together the range of agencies and programs needed to catalyze progress in the UDS field in areas such as communications, autonomous systems, safety measurement, and others.

[156] https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf
[157] https://www.ntia.doc.gov/files/ntia/publications/uas_privacy_best_practices_6-21-16.pdf

Recommendation 3a: Develop a Federal strategy for UDS research and development through an interagency task group with input from the commercial and academic sectors; convened by the Networking and Information Technology Research and Development (NITRD) program or similarly positioned agency.

Recommendation 3b: Strengthen and expand existing research, development, and standards programs in agencies such as NIST, NSF, NASA, DOL, DOT, DOE, and others.

Challenge 4: *A lack of standards for interoperability, performance measurement, testing and certification, validation and verification, and other capabilities will inhibit innovation and the emergence of a competitive global UDS technologies market.*

Open, consensus-based, voluntary, private sector-led, and science- and engineering-informed standards enable innovation in products and services development; interoperability across systems and devices; open and competitive national and global markets; and efficient and precise acquisition processes.

Recommendation 4a: Convene private sector stakeholders to co-develop, with appropriate antitrust safeguards, a coordinated UDS strategy that identifies standards needs, gaps, and refinements essential to promoting UDS innovation and opportunities for market growth.

Recommendation 4b: Strengthen and extend existing programs that support basic and applied research, develop effective measurement methods, and document best practices and guidelines that provide the basis for effective development of prioritized, private sector-led UDS sector standards development.

Recommendation 4c: To promote broad adoption and maximize benefits of new standards, support programs for standards education and awareness and develop reliable and reproducible methods and protocols for testing and certification capabilities that support confident acquisition of innovative systems and technologies.

Challenge 5: *The workforce implications of UDS sector growth are complex with the pattern of workforce changes expected to vary by region with differences in the directions, pace, and scale of growth in this emerging sector.*

A strategy that is responsive to market dynamics and technology change, while cognizant of the needs of different regions, is needed to enable effective management of the workforce implications of UDS sector growth. The workforce strategy must connect information to decision makers in government, industry, and educational sectors and provide options for an effective response.

Recommendation 5a: Expand the collection and aggregation of openly accessible workforce data at local, State, and regional levels in UDS-relevant services, technologies, labor, and other jobs sectors.

Recommendation 5b: Support the development of education, training, and re-skilling programs in areas such as UDS operations, maintenance, management, and in areas such as complex systems integration and control. Develop, in cooperation with industry and academia, a resource for curricula and program options for a skilled UDS workforce suitable for tailoring to regional needs by local educators.

***Challenge 6:** Enabling growth of the UDS sector requires coordination among a diverse group of stakeholders.*

A broad coordination strategy, focused specifically on addressing challenges 1–5 enumerated above and implemented as set out in recommendations 6a–d below, is needed to spur UDS innovation and enable a vibrant marketplace.

Recommendation 6a: Strengthen and expand existing coordination efforts among relevant Federal agencies, including core agencies, such as DOT, NASA, and the FCC—and supporting agencies, such as NIST, NSF, NTIA, DHS, DOD, DOL, ED, and DOJ.

Recommendation 6b: Strengthen and expand existing coordination efforts among local, Tribal, State, and Federal agencies with roles in enabling UDS applications, including local planning entities, state departments of transportation, and public safety entities.

Recommendation 6c: Strengthen and expand existing coordination efforts linking the private sector and government entities at all levels, including technology developers, manufacturers and suppliers, service providers, and user and consumer groups.

Recommendation 6d: The FAA should continue efforts and work with Congress, which has defined 'unmanned aircraft system' in statute[158], to identify more inclusive, gender-neutral language to replace the term 'unmanned.'

[158] 49 U.S.C. 44801, "Definitions." https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title49-section44801&num=0&edition=prelim

References

[1] sUAS Operations. 14 CFR Part 107. Federal Aviation Administration. Accessed May 26, 2022. https://www.faa.gov/air_traffic/publications/atpubs/foa_html/chap19_section_6.html.

[2] Cregger, Joshua, Elizabeth Machek, Alexander Epstein, Tracy Lennertz, Jingsi Shaw, Kevin Dopart, Molly Behan, and John A. Volpe National Transportation Systems Center. "Emerging Automated Urban Freight Delivery Concepts: State of the Practice Scan." FHWA-JPO-20-825, United States. Department of Transportation. Intelligent Transportation Systems Joint Program Office, November 20, 2020. https://rosap.ntl.bts.gov/view/dot/53938.

[3] Federal Aviation Administration. "Report to Congress: Update of the FAA Comprehensive Plan and Unmanned Aircraft Systems (UAS) Program Alignment: FAA Reauthorization Act of 2018 (Pub. L. No. 115-254) – Section 342." 2022. https://www.faa.gov/sites/faa.gov/files/2022-02/PL_115-254_Sec_342_UAS_Comprehensive_Plan_and_Program_Alignment.pdf.

[4] Congressional Research Service. "Issues in Autonomous Vehicle Testing and Deployment." 2021. Accessed May 18, 2022. https://sgp.fas.org/crs/misc/R45985.pdf.

[5] U.S. Census Bureau. "Economic Census: NAICS Codes & Understanding Industry Classification Systems." Accessed May 18, 2022. https://www.census.gov/programs-surveys/economic-census/guidance/understanding-naics.html.

[6] Flytrex. "Flytrex - Drone Delivery." Accessed May 19, 2022. https://www.flytrex.com/.

[7] Starship. "Starship." Accessed May 19, 2022. https://www.starship.xyz/.

[8] Wing. "Wing - Drone Delivery." Accessed May 19, 2022. https://wing.com/.

[9] Nuro. "Nuro - on a Mission to Better Everyday Life Through Robotics." Accessed May 19, 2022. https://www.nuro.ai/.

[10] Daleo, Jack. "Wingcopter Inks $16M Deal with Spright for US Medical Drone Deliveries." *FLYING Magazine*, January 25, 2022. Accessed May 19, 2022. https://www.flyingmag.com/wingcopter-inks-16m-deal-with-spright-for-us-medical-drone-deliveries/.

[11] Ackerman, Evan. "In the Air with Zipline's Medical Delivery Drones." *IEEE Spectrum*, April 30, 2019. Accessed May 19, 2022. https://spectrum.ieee.org/in-the-air-with-ziplines-medical-delivery-drones.

[12] Hawkins, Andrew J. "Nuro Is Using Delivery Robots to Help Health Care Workers Fighting COVID-19." *The Verge*, April 22, 2020. Accessed May 19, 2022. https://www.theverge.com/2020/4/22/21231466/nuro-delivery-robot-health-care-workers-food-supplies-california.

[13] FedEx. "Drone Package Delivery Pilot Program Launched | FedEx." Accessed May 18, 2022. https://www.fedex.com/en-us/sustainability/wing-drones-transport-fedex-deliveries-directly-to-homes.html.

[14] USPS Office of Inspector General. "Autonomous Mobile Robots and the Postal Service." Accessed May 19, 2022. https://www.uspsoig.gov/reports/white-papers/autonomous-mobile-robots-and-postal-service.

[15] Tevel. "Technology." Accessed November 2, 2022. https://www.tevel-tech.com/technology/.

[16] Rantizo. “Drone Crop Spraying | Rantizo - Elevating Precision Ag.” Accessed May 19, 2022. https://www.rantizo.com/.

[17] O'Neal, Bridget. “Equinor Uses Offshore Drone Delivery for 3D Printed Spare Parts.” *3DPrint.com*, September 4, 2020. Accessed May 19, 2022. https://3dprint.com/272565/equinor-3d-prints-obsolete-parts-to-be-delivered-offshore-drone/.

[18] Mircea, Cristina. “Wingcopter's Flexible, All-Weather Drones Will Deliver Spare Parts for Offshore Wind Farms.” Accessed May 19, 2022. https://www.autoevolution.com/news/wingcopter-s-flexible-all-weather-drones-will-deliver-spare-parts-for-offshore-wind-farms-185408.html.

[19] Starship Deliveries. “Industry - Starship Deliveries.” Accessed May 18, 2022. https://starshipdeliveries.com/industry/.

[20] Cox, Matthew. “Autonomous Drones Proved Themselves in Army Ammo Resupply Tests. Now, the XVIII Airborne Wants in.” *Military.com*, March 15, 2021. Accessed May 19, 2022. https://www.military.com/daily-news/2021/03/15/autonomous-drones-proved-themselves-army-ammo-resupply-tests-now-xviii-airborne-wants.html.

[21] Thompson, Maureena. “Utilizing Semi-Autonomous Resupply to Mitigate Risks to Soldiers on the Battlefield.” Accessed May 19, 2022. https://www.army.mil/article/251476/utilizing_semi_autonomous_resupply_to_mitigate_risks_to_soldiers_on_the_battlefield.

[22] Schwartz, Dan. “Why Drones Are the Future of Outdoor Search and Rescue.” *Outside*, October 4, 2021. Accessed May 19, 2022. https://www.outsideonline.com/outdoor-adventure/exploration-survival/drones-search-rescue/.

[23] Brown, Dalvin. “Throwable Military Robots Sent to Assist with Florida Condo Collapse.” *The Washington Post*, June 30, 2021. Accessed May 19, 2022. https://www.washingtonpost.com/technology/2021/06/30/throwable-robot-florida-condo-collapse/.

[24] PrecisionHawk. “Agriculture: Drone Mapping and Analytics.” Accessed May 19, 2022. https://www.precisionhawk.com/agriculture.

[25] Forestieri, Kevin. “Mountain View Council Swiftly Approves Drone Policy for City Staff Use.” Accessed May 19, 2022. https://www.mv-voice.com/news/2019/09/05/mountain-view-council-swiftly-approves-drone-policy-for-city-staff-use.

[26] Frachtenberg, Eitan. “Practical Drone Delivery.” *Computer* 52, no. 12 (2019): 53–57. https://doi.org/10.1109/MC.2019.2942290.

[27] Markets and Markets. “Drone Package Delivery Market: Global Forecast to 2030.” https://www.marketsandmarkets.com/Market-Reports/drone-package-delivery-market-10580366.html.

[28] Skowron, Michal, Witold Chmielowiec, Karolina Glowacka, Magdalena Krupa, and Adam Srebro. “Sense and Avoid for Small Unmanned Aircraft Systems: Research on Methods and Best Practices.” *Proceedings of the Institution of Mechanical Engineers, Part G: Journal of Aerospace Engineering* 233, no. 16 (2019): 6044–62. Accessed May 18, 2022. https://doi.org/10.1177/0954410019867802. https://journals.sagepub.com/doi/pdf/10.1177/0954410019867802.

[29] Bisen, Vikram Singh. “How AI Based Drone Works: Artificial Intelligence Drone Use Cases.” *Medium*, February 5, 2020. Accessed May 18, 2022.

https://medium.com/vsinghbisen/how-ai-based-drone-works-artificial-intelligence-drone-use-cases-7f3d44b8abe3.

[30] Lee, Thomas, Susan Mckeever, and Jane Courtney. "Flying Free: A Research Overview of Deep Learning in Drone Navigation Autonomy." *Drones* 5, no. 2 (2021): 52. https://doi.org/10.3390/drones5020052. https://www.mdpi.com/2504-446X/5/2/52.

[31] Cast, Nick. "How Drone GPS Navigation Works?" *Remote Flyer*, November 25, 2020. Accessed May 18, 2022. https://www.remoteflyer.com/how-drone-gps-navigation-works/.

[32] Abdalla, Aly Sabri, and Vuk Marojevic. "Communications Standards for Unmanned Aircraft Systems: The 3GPP Perspective and Research Drivers." *IEEE Commun. Standards Mag*, 2021. Accessed May 18, 2022. https://arxiv.org/pdf/2009.03533.pdf.

[33] Givens, M. W., and C. Coopmans. "A Survey of Inertial Sensor Fusion: Applications in SUAS Navigation and Data Collection." In *2019 International Conference on Unmanned Aircraft Systems (ICUAS)*, 1054–60., 2019.

[34] Federal Aviation Administration. "Unmanned Aircraft System Traffic Management (UTM)." Accessed May 18, 2022. https://www.faa.gov/uas/research_development/traffic_management/.

[35] U.S. Government Accountability Office. "GAO-20-165, Unmanned Aircraft Systems: FAA Could Strengthen Its Implementation of a Drone Traffic Management System by Improving Communication and Measuring Performance." 2021. https://www.gao.gov/assets/gao-21-165.pdf.

[36] Wolfe, Leslie. "5 Challenges That the Drone Delivery System Should Overcome." *InterDrone*, January 15, 2018. Accessed May 18, 2022. https://interdrone.com/news/5-challenges-that-the-drone-delivery-system-should-overcome/.

[37] Martínez-Díaz, Margarita, and Francesc Soriguera. "Autonomous Vehicles: Theoretical and Practical Challenges." *Transportation Research Procedia* 33 (2018): 275–82. https://doi.org/10.1016/j.trpro.2018.10.103. https://www.sciencedirect.com/science/article/pii/S2352146518302606.

[38] McDermid, John. "Autonomous Cars: Five Reasons They Still Aren't on Our Roads." Accessed May 18, 2022. https://theconversation.com/autonomous-cars-five-reasons-they-still-arent-on-our-roads-143316.

[39] Ramey, Jay. "The Delivery Robot Revolution Is Not Quite Ready for Primetime." *Autoweek*, July 20, 2020. Accessed May 18, 2022. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1400/RR1478/RAND_RR1478.pdf.

[40] Liu, Zhixiang, Youmin Zhang, Chi Yuan, Laurent Ciarletta, and Didier Theilliol. "Collision Avoidance and Path Following Control of Unmanned Aerial Vehicle in Hazardous Environment." *Journal of Intelligent & Robotic Systems* 95, no. 1 (2019): 193–210. https://doi.org/10.1007/s10846-018-0929-y. https://link.springer.com/article/10.1007/s10846-018-0929-y.

[41] Nidhi Kalra, Susan M. Paddock. "Driving to Safety: How Many Miles of Driving Would It Take to Demonstrate Autonomous Vehicle Reliability?," 2016. Accessed May 18, 2022. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1400/RR1478/RAND_RR1478.pdf.

[42] National Transportation Safety Board. "Docket No. DOT-NHTSA-2020-0106." Accessed October 28, 2022. https://www.ntsb.gov/Advocacy/safety-topics/Documents/2021-Comments-to-NHTSA-Framework-for-ADS-Safety-ANPRM.pdf.

[43] Wakabayashi, Daisuke. "Self-Driving Uber Car Kills Pedestrian in Arizona, Where Robots Roam." *The New York Times*, March 19, 2018. Accessed May 18, 2022. https://www.nytimes.com/2018/03/19/technology/uber-driverless-fatality.html.

[44] NTSB. "Collision Between Vehicle Controlled by Developmental Automated Driving System and Pedestrian, Tempe, Arizona, March 18, 2018." 2019. Accessed November 1, 2022. https://www.ntsb.gov/investigations/AccidentReports/Reports/HAR1903.pdf.

[45] Eißfeldt, Hinnerk, and Albert End. "Investigating Attitudes Towards Drone Delivery." *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 64, no. 1 (2021): 169–73. https://doi.org/10.1177/1071181320641042.

[46] Winkler, Stephanie, Sherali Zeadally, and Katrine Evans. "Privacy and Civilian Drone Use: The Need for Further Regulation." *IEEE Security & Privacy* 16, no. 5 (2018): 72–80. https://doi.org/10.1109/MSP.2018.3761721.

[47] Shivakumar, Sujai. "Securing Global Standards for Innovation and Growth." 2022. Accessed May 18, 2022. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220127_Shivakumar_Securing_Global_Standards.pdf?RxVe0c96Njjy24Af_R8kcoDkW8MhSYsi.

[48] Deto, Ryan. "Pennsylvania Legalizes Autonomous Delivery Robots, Classifies Them as Pedestrians." *Pittsburgh City Paper*, December 2, 2020. Accessed May 18, 2022. https://www.pghcitypaper.com/pittsburgh/pennsylvania-legalizes-autonomous-delivery-robots-classifies-them-as-pedestrians/Content?oid=18482040.

[49] Namian, Mostafa, Mohammad Khalid, George Wang, and Yelda Turkan. "Revealing Safety Risks of Unmanned Aerial Vehicles in Construction." *Transportation Research Record: Journal of the Transportation Research Board* 2675, no. 11 (2021): 334–47. https://doi.org/10.1177/03611981211017134.

[50] Tingle, Anthony, and David Tyree. "The Rise of the Commercial Threat: Countering the Small Unmanned Aircraft System." Accessed May 18, 2022. https://ndupress.ndu.edu/Media/News/Article/1130654/the-rise-of-the-commercial-threat-countering-the-small-unmanned-aircraft-system/.

[51] Lacher, A., J. Baron, M. Balazs, and J. Rotner. "Small Unmanned Aircraft: Characterizing the Threat." 2019. Accessed May 18, 2022. https://www.mitre.org/sites/default/files/publications/pr-18-3852-small-uas-characterizing-threat.pdf.

[52] Editorial. "Potential Risks and Dangers in Drone Delivery." *RoboticsBiz*, February 2, 2020. Accessed May 18, 2022. https://roboticsbiz.com/potential-risks-and-dangers-in-drone-delivery/.

[53] Federal Aviation Administration. "Package Delivery by Drone (Part 135)." Accessed May 18, 2022. https://www.faa.gov/uas/advanced_operations/package_delivery_drone/.

[54] Salvini, Pericle, Diego Paez-Granados, and Aude Billard. "Safety Concerns Emerging from Robots Navigating in Crowded Pedestrian Areas." *International Journal of Social Robotics* 14, no. 2 (2022): 441–62. https://doi.org/10.1007/s12369-021-00796-4. https://link.springer.com/article/10.1007/s12369-021-00796-4.

[55] Federal Aviation Administration. “UPS Flight Forward Drone Package Delivery Operations Wake Forest Baptist Health (WFBH) Routes, Winston-Salem, NC - EA & ROD.” 2021. https://www.faa.gov/sites/faa.gov/files/uas/advanced_operations/nepa_and_drones/UPS_Flight_Forward_Winston_Salem_NC-EA_and_record_of_decision.pdf.

[56] Davis, Joshua. “The Crypto-Currency: Bitcoin and Its Mysterious Inventor.” *The New Yorker*, October 3, 2011. https://www.newyorker.com/magazine/2011/10/10/the-crypto-currency.

[57] Federal Aviation Administration. “Drones by the Numbers.” Accessed May 18, 2022. https://www.faa.gov/uas.

[58] Greenwood, Faine. “How to Solve the Problem of Missing Drone Crash Data.” *Brookings*, September 28, 2021. Accessed May 18, 2022. https://www.brookings.edu/techstream/how-to-solve-the-problem-of-missing-drone-crash-data/.

[59] Wallace, Ryan, Kristy Kiernan, Tom Haritos, John Robbins, and Godfrey D'souza. “Evaluating Small UAS Near Midair Collision Risk Using AeroScope and ADS-B.” *International Journal of Aviation, Aeronautics, and Aerospace*, 2018. Accessed May 18, 2022. https://doi.org/10.15394/ijaaa.2018.1268. https://commons.erau.edu/cgi/viewcontent.cgi?article=1268&context=ijaaa.

[60] Lyon-Hill, Sarah, Melissa Tilashalski, Kimberly Ellis, and Elli and Travis. “Measuring the Effects of Drone Delivery in the United States_September 2020.” 2020. Accessed May 18, 2022. https://www.newswise.com/pdf_docs/160018187481745_Virginia%20Tech%20%20Measuring%20the%20Effects%20of%20Drone%20Delivery%20in%20the%20United%20States_September%202020.pdf.

[61] Lohn, Andrew J. “What's the Buzz? The City-Scale Impacts of Drone Delivery.” 2017. Accessed May 18, 2022. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1718/RAND_RR1718.pdf.

[62] Lavallee, Elise. “Pitt Pauses Testing on Food Delivery Robots Following Reports of Impeded Accessibility.” *Pittsburgh City Paper*, October 23, 2019. Accessed May 18, 2022. https://www.pghcitypaper.com/pittsburgh/pitt-pauses-testing-on-food-delivery-robots-following-reports-of-impeded-accessibility/Content?oid=16050658.

[63] NHTSA. “2020 Fatality Data Show Increased Traffic Fatalities During Pandemic.” Accessed May 18, 2022. https://www.nhtsa.gov/press-releases/2020-fatality-data-show-increased-traffic-fatalities-during-pandemic.

[64] Emergen Research. “Drone Package Delivery Industry Top Companies | Drone Package Delivery Market Top Players by 2028.” Accessed May 18, 2022. https://www.emergenresearch.com/blog/top-10-companies-in-the-drone-package-delivery-industry.

[65] James Gelinas. “Amazon Prime Air Plans to Start Autonomous Drone Delivery Within Months.” https://www.komando.com/shopping/look-up-in-the-sky-its-my-package-amazon-to-start-drone-delivery-within-months/571255/.

[66] Palmer, Annie. “Amazon Wins FAA Approval for Prime Air Drone Delivery Fleet.” *CNBC*, August 31, 2020. Accessed May 18, 2022.

https://www.cnbc.com/2020/08/31/amazon-prime-now-drone-delivery-fleet-gets-faa-approval.html.

[67] Federal Aviation Administration. “Draft Environmental Assessment Zipline International Inc. Drone Package Delivery Operations Kannapolis, NC and Surrounding Area.” 2022. https://www.faa.gov/sites/faa.gov/files/uas/advanced_operations/nepa_and_drones/SIGNED_FONSI_ROD_Final_EA_Zipline_Kannapolis_NC.pdf.

[68] Federal Aviation Administration. “Airworthiness Criteria: Special Class Airworthiness Criteria for the Zipline International Inc. Zip UAS Sparrow Unmanned Aircraft.” https://www.federalregister.gov/documents/2022/02/25/2022-03864/airworthiness-criteria-special-class-airworthiness-criteria-for-the-zipline-international-inc-zip.

[69] Engineering For Change. “Zipline: Zipline Uses Fixed Wing Drones to Remotely Deliver Vaccines Medicines and Supplies.” Accessed May 18, 2022. https://www.engineeringforchange.org/solutions/product/zipline/.

[70] Wing. “How It Works – Wing.” Accessed May 18, 2022. https://wing.com/how-it-works/.

[71] SPEEDA Edge. “SkyDrop (Flirtey) - SPEEDA Edge.” Accessed May 18, 2022. https://sp-edge.com/companies/153041.

[72] Flirtey. “Flirtey Announces New Brand SkyDrop.” *PR Newswire*, January 25, 2022. Accessed May 18, 2022. https://www.prnewswire.com/news-releases/flirtey-announces-new-brand-skydrop-301468330.html.

[73] Federal Aviation Administration. “Wing Aviation Drone Package Delivery Operations Christiansburg, Virginia: Finding of No Significant Impact/Record of Decision for Environmental Assessment for Wing Aviation Drone Package Delivery Operations Christiansburg, Virginia.” Accessed May 18, 2022. https://www.faa.gov/sites/faa.gov/files/uas/advanced_operations/nepa_and_drones/Wing_Christiansburg-record_of_decision.pdf.

[74] SkyDrop. “SkyDrop | Real-Time Delivery by Flying Robots.” Accessed May 18, 2022. https://getskydrop.com/.

[75] Federal Aviation Administration. “U.S. Transportation Secretary Elaine L. Chao Announces FAA Certification of UPS Flight Forward as an Air Carrier | Federal Aviation Administration.” https://www.faa.gov/newsroom/us-transportation-secretary-elaine-l-chao-announces-faa-certification-ups-flight-forward.

[76] United Parcel Service. “UPS Flight Forward and Wingcopter to Develop Versatile New Drone Fleet | About UPS.” Accessed May 18, 2022. https://about.ups.com/sg/en/newsroom/press-releases/customer-first/ups-flight-forward-and-wingcopter-to-develop-versatile-new-drone-fleet.html.

[77] Workhorse. “Workhorse | HorseFly.” Accessed May 18, 2022. https://workhorse.com/horsefly.html.

[78] Airbus. “Airbus’ Skyways Drone Trials World’s First Shore-to-Ship Deliveries.” Accessed May 18, 2022. https://www.airbus.com/en/newsroom/press-releases/2019-03-airbus-skyways-drone-trials-worlds-first-shore-to-ship-deliveries.

[79] Markets and Markets. “Delivery Robot Market with COVID-19 Impact: Global Forecast to 2026.” Accessed 5/182022. https://www.marketsandmarkets.com/Market-Reports/delivery-robot-market-263997316.html.

[80] Ueland, Sig. “10 Autonomous Robots for Last-Mile Deliveries.” *Practical Ecommerce*, June 28, 2021. Accessed May 18, 2022. https://www.practicalecommerce.com/10-autonomous-robots-for-last-mile-deliveries.

[81] Dimensions. “Amazon Scout Dimensions & Drawings.” Accessed May 18, 2022. https://www.dimensions.com/element/amazon-scout.

[82] Pallone, Tony. “Robby Is a Robot That Delivers.” Accessed May 18, 2022. https://electronics360.globalspec.com/article/10864/robby-is-a-robot-that-delivers.

[83] Boston Dynamics Support. “Spot Specifications.” Accessed May 18, 2022. https://support.bostondynamics.com/s/article/Robot-specifications.

[84] Robomart. “Platform.” Accessed May 18, 2022. https://platform.robomart.co/.

[85] Robotics Business Review Staff. “Boxbot Launches Last-Mile, Self-Driving Parcel Delivery System.” Accessed May 18, 2022. https://www.roboticsbusinessreview.com/supply-chain/boxbot-launches-last-mile-self-driving-parcel-delivery-system/.

[86] Dimensions. “KiwiBot Dimensions & Drawings.” Accessed May 18, 2022. https://www.dimensions.com/element/kiwibot.

[87] Mcclure, Olivia. “10 Robotics Delivery Companies in San Francisco Embracing a New World.” *Built In San Francisco*, February 9, 2020. Accessed May 18, 2022. https://www.builtinsf.com/2019/12/19/robotics-delivery-companies-san-francisco.

[88] My Gita. “How It Works - Piaggio Fast Forward.” Accessed May 18, 2022. https://mygita.com/how-it-works.

[89] MarketLine. “Marble Acquisition Will Drive Caterpillar’s Automation Strategy.” *Verdict*, June 18, 2020. Accessed May 18, 2022. https://www.verdict.co.uk/marble-robot-caterpillar/.

[90] Cruise. “Cruise Technology.” Accessed May 18, 2022. https://www.getcruise.com/technology.

[91] Balać, Miloš, Amedeo R. Vetrella, and Kay W. Axhausen. “Towards the Integration of Aerial Transportation in Urban Settings.” ETH Zurich, 2018. https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/193150/ab1266.pdf.

[92] AUVSI News. “UPS, Waymo Partner to Begin Picking up Packages Using Autonomous Vehicles in Phoenix.” Accessed May 18, 2022. https://www.auvsi.org/industry-news/ups-waymo-partner-begin-picking-packages-using-autonomous-vehicles-phoenix.

[93] Bureau of Labor Statistics. “Usual Weekly Earnings of Wage and Salary Workers First Quarter 2022.” Accessed May 23, 2022. https://www.bls.gov/news.release/pdf/wkyeng.pdf.

[94] United States Postal Service Office of Inspector General, and Risk Analysis Research Center. “Summary Report: Public Perception of Self-Driving Technology for Long-Haul Trucking and Last-Mile Delivery.” 2017. Accessed May 20, 2022. https://www.uspsoig.gov/reports/white-papers/public-perception-self-driving-technology-long-haul-trucking-and-last-mile.

[95] Bureau of Labor Statistics. “Occupational Employment and Wages Light Truck Drivers.” Accessed May 23, 2022. https://www.bls.gov/oes/current/oes533033.htm.

[96] Bureau of Labor Statistics. “Occupational Employment and Wages Driver/Sales Workers.” Accessed May 23, 2022. https://www.bls.gov/oes/current/oes533031.htm.

[97] U.S. Bureau of Labor Statistics. “Delivery Truck Drivers and Driver/Sales Workers: Occupational Outlook Handbook.” Accessed November 3, 2022.

https://www.bls.gov/ooh/transportation-and-material-moving/delivery-truck-drivers-and-driver-sales-workers.htm#tab-2.

[98] U.S. Bureau of Labor Statistics. “Employment, Wages, and Projected Change in Employment by Typical Entry-Level Education.” Accessed November 1, 2022. https://www.bls.gov/emp/tables/education-summary.htm.

[99] Bureau of Labor Statistics. “Industries at a Glance: Merchant Wholesalers, Nondurable Goods: NAICS 424.” Accessed May 23, 2022. https://www.bls.gov/iag/tgs/iag424.htm.

[100] Ramaswamy, K. “Technological Change, Automation and Employment: A Short Review of Theory and Evidence.” *International Review of Business and Economics* 2, no. 2 (2018). https://digitalcommons.du.edu/irbe/vol2/iss2/1.

[101] Terzidis, Nikos, Steven Brakman, and Raquel Ortega-Argilés. “Labour Markets, Trade and Technological Progress: A Meta-Study.” *SSRN Electronic Journal*, 2019. https://doi.org/10.2139/ssrn.3421146.

[102] Barbieri, Laura, Chiara Mussida, Mariacristina Piva, and Marco Vivarelli. “Testing the Employment Impact of Automation, Robots and AI: A Survey and Some Methodological Issues.” *SSRN Electronic Journal*, 2019. https://doi.org/10.2139/ssrn.3457656.

[103] Frey, Carl Benedikt, and Michael A. Osborne. “The Future of Employment: How Susceptible Are Jobs to Computerisation?” *Technological Forecasting and Social Change* 114 (2017): 254–80. https://doi.org/10.1016/j.techfore.2016.08.019. https://www.sciencedirect.com/science/article/pii/S0040162516302244.

[104] Arntz, Melanie, Terry Gregory, and Ulrich Zierahn. “Revisiting the Risk of Automation.” *Economics Letters* 159 (2017): 157–60. https://doi.org/10.1016/j.econlet.2017.07.001. https://www.sciencedirect.com/science/article/pii/S0165176517302811.

[105] Doole, Malik, Joost Ellerbroek, and Jacco Hoekstra. “Estimation of Traffic Density from Drone-Based Delivery in Very Low Level Urban Airspace.” *Journal of Air Transport Management* 88 (2020): 101862. https://doi.org/10.1016/j.jairtraman.2020.101862. https://www.sciencedirect.com/science/article/pii/S0969699719304004.

[106] Tavares, T. “Comparing the Cost-Effectiveness of Drones V Ground Vehicles for Medical, Food and Parcel Deliveries.” 2019.

[107] U.S. Department of Labor. “Trade Adjustment Assistance for Workers | U.S. Department of Labor.” Accessed May 24, 2022. https://www.dol.gov/agencies/eta/tradeact.

[108] Guth, J., and J. Lee. “Evaluations of the Trade Adjustment Assistance Program for Workers: A Literature Review.” https://www.usitc.gov/publications/332/executive_briefings/ebot_taaevaluationsguthlee.pdf.

[109] Jenkins, D., and B. Vasigh. “The Economic Impact of Unmanned Aircraft Systems Integration in the United States.” *The Association for Unmanned Vehicle Systems International (AUVSI)*, 2013. https://www.auvsi.org/our-impact/economic-report.

[110] PricewaterhouseCoopers. “Clarity from Above PwC Global Report on the Commercial Applications of Drone Technology.” n.d. Accessed May 24, 2022. https://www.pwc.pl/pl/pdf/clarity-from-above-pwc.pdf.

[111] D Jenkins, B Vasigh, C Oster, and T Larsen. "Forecast of the Commercial UAS Package Delivery Market." *Academia*, 2017.

[112] Levitate Capital. "The Future of the Drone Economy.."

[113] Steer Group. "Economic Impacts of Autonomous Delivery Services in the US." Accessed May 24, 2022. https://www.steergroup.com/sites/default/files/2020-09/200910_%20Nuro_Final_Report_Public.pdf.

[114] Benarbia, Taha, and Kyandoghere Kyamakya. "A Literature Review of Drone-Based Package Delivery Logistics Systems and Their Implementation Feasibility." *Sustainability* 14, no. 1 (2022): 360. https://doi.org/10.3390/su14010360. https://www.mdpi.com/2071-1050/14/1/360.

[115] Harper, Corey D., Chris T. Hendrickson, and Constantine Samaras. "Cost and Benefit Estimates of Partially-Automated Vehicle Collision Avoidance Technologies." *Accident; analysis and prevention* 95, Pt A (2016): 104–15. https://doi.org/10.1016/j.aap.2016.06.017. https://pubmed.ncbi.nlm.nih.gov/27423430/.

[116] Canis, Bill. "Issues in Autonomous Vehicle Testing and Deployment." Accessed May 20, 2022. https://sgp.fas.org/crs/misc/R45985.pdf.

[117] NTSB. "History of the National Transportation Safety Board." Accessed May 20, 2022. https://www.ntsb.gov/about/history/Pages/default.aspx.

[118] U.S. Department of Transportation. "The Safety Band #SafetyBand." Accessed May 20, 2022. https://www.transportation.gov/content/safety-band.

[119] Federal Communications Commission. "Use of the 5.850-5.925 GHz Band." Accessed May 20, 2022. https://www.federalregister.gov/documents/2021/05/03/2021-08802/use-of-the-5850-5925-ghz-band.

[120] Federal Aviation Administration. "Unmanned Aircraft Systems (UAS)." Accessed May 18, 2022. https://www.faa.gov/uas/.

[121] Federal Aviation Administration. "Critical Infrastructure and Public Venues." Accessed May 18, 2022. https://www.faa.gov/uas/critical_infrastructure/.

[122] Federal Aviation Administration. "BEYOND." Accessed May 18, 2022. https://www.faa.gov/uas/programs_partnerships/beyond/.

[123] ANSI Unmanned Aircraft Systems Standardization Collaborative. "ANSI UASSC Standardization Roadmap for Unmanned Aircraft Systems." 2020. https://share.ansi.org/Shared%20Documents/Standards%20Activities/UASSC/ANSI_UASSC_Roadmap_V2_June_2020.pdf.

[124] Federal Aviation Administration. "Partnership for Safety Plan (PSP) Program." Accessed May 18, 2022. https://www.faa.gov/uas/programs_partnerships/psp/.

[125] Federal Register. "Amendment to the Definition of Unmanned Aircraft Accident." Accessed October 26, 2022. https://www.federalregister.gov/documents/2022/07/14/2022-14872/amendment-to-the-definition-of-unmanned-aircraft-accident.

[126] National Highway Traffic Safety Administration. "NHTSA Grants Nuro Exemption Petition for Low-Speed Driverless Vehicle." Accessed May 20, 2022. https://www.nhtsa.gov/press-releases/nhtsa-grants-nuro-exemption-petition-low-speed-driverless-vehicle.

[127] Grant, Rob. "Seeking NHTSA Review of the Origin - Cruise." Accessed May 20, 2022. https://getcruise.com/news/blog/2022/seeking-nhtsa-review-of-the-origin/.

[128] Federal Aviation Administration. "FAA Begins New Phase of Testing to Safely Integrate Drones into the National Airspace | Federal Aviation Administration." Accessed May 18, 2022. https://www.faa.gov/newsroom/faa-begins-new-phase-testing-safely-integrate-drones-national-airspace.

[129] U.S. Department of Transportation. "Occupant Protection for Vehicles with Automated Driving Systems: 49 CFR Part 571 Docket No. NHTSA-2021-0003 RIN 2127-AM06." 2022. https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-03/Final-Rule-Occupant-Protection-Amendment-Automated-Vehicles.pdf.

[130] Federal Aviation Administration. "UTM Field Test (UFT)." Accessed May 18, 2022. https://www.faa.gov/uas/research_development/traffic_management/field_test/.

[131] Hoover, Rachel. "What Is the Air Traffic Management EXploration?" *NASA*, September 27, 2021. Accessed May 20, 2022. https://www.nasa.gov/ames/atmx.

[132] National Science and Technology Council, and U.S. Department of Transportation. "Ensuring American Leadership in Automated Vehicle Technologies: Automated Vehicles 4.0." 2020. https://www.transportation.gov/sites/dot.gov/files/2020-02/EnsuringAmericanLeadershipAVTech4.pdf.

[133] Unmanned Aircraft Systems Beyond Visual Line of Sight Aviation Rulemaking Committee. "Final Report." 2022. https://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/UAS_BVLOS_ARC_FINAL_REPORT_03102022.pdf.

[134] Interagency Unmanned Aircraft System (UAS) Program. "Interagency UAS Program." Accessed May 20, 2022. https://uas.nifc.gov/.

[135] Fagan, Michael, Jeffrey Marron, Kevin Brady, Barbara Cuthill, Katerina Megas, Rebecca Herold, David Lemire, and Brad Hoehn. "IoT Device Cybersecurity Guidance for the Federal Government." 2021. https://csrc.nist.gov/publications/detail/sp/800-213/final.

[136] Joint Task Force Interagency Working Group. "Risk Management Framework for Information Systems and Organizations." NIST, 2018. https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final.

[137] NIST. "Privacy Framework." n.d. https://www.nist.gov/privacy-framework.

[138] NIST. "NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management." 2020. https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf.

[139] NIST CSRC. "About the RMF - NIST Risk Management Framework | CSRC | CSRC." Accessed June 28, 2022. https://csrc.nist.gov/projects/risk-management/about-rmf.

[140] International Trade Administration. "About Us." Accessed May 20, 2022. https://www.trade.gov/about-us.

[141] U.S. Department of Homeland Security. "First Responder Robotic Operations System Test (FRROST) Small UAS for Search and Rescue." Accessed May 20, 2022. https://www.dhs.gov/science-and-technology/saver/st-small-unmanned-aircraft-systems-search-and-rescue-frrost.

[142] Cybersecurity and Infrastructure Security Agency. "Cybersecurity Best Practices for Operating Commercial Unmanned Aircraft Systems (UASs)." Accessed October 26, 2022.

https://www.cisa.gov/sites/default/files/publications/CISA%20Cybersecurity%20Best%20Practices%20for%20Operating%20Commerical%20UAS%20%28508%29.pdf.

[143] U.S. Department of Justice. “Unmanned Aircraft Systems.” Accessed May 20, 2022. https://www.justice.gov/olp/unmanned-aircraft-systems.

[144] Blake, Tiffany. “What Is Unmanned Aircraft Systems Traffic Management?” News release. June 6, 2018. Accessed May 20, 2022. https://www.nasa.gov/ames/utm.

[145] National Aeronautics and Space Administration. “Advanced Air Mobility Looks Ahead to Automation.” Accessed August 1, 2022. https://www.nasa.gov/centers/armstrong/features/aam-looks-toward-automation.html.

[146] U.S. Department of Agriculture, and U.S. Forest Service. “Forest Service Standards for UAS Operations.” 2020. Accessed May 20, 2022. https://www.fs.usda.gov/sites/default/files/2020-07/Forest%20Service%20Standards%20for%20UAS%20Operations%2007012020.pdf.

[147] Othman, Kareem. “Public Acceptance and Perception of Autonomous Vehicles: A Comprehensive Review.” *AI and Ethics* 1, no. 3 (2021): 355–87. https://doi.org/10.1007/s43681-021-00041-8. https://link.springer.com/article/10.1007/s43681-021-00041-8.

[148] Jefferson, Jacelyn, and Anthony D. McDonald. “The Autonomous Vehicle Social Network: Analyzing Tweets After a Recent Tesla Autopilot Crash.” *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 63, no. 1 (2019): 2071–75. Accessed May 19, 2022. https://doi.org/10.1177/1071181319631510. https://journals.sagepub.com/doi/pdf/10.1177/1071181319631510.

[149] The Library of Congress. “Germany: Road Traffic Act Amendment Allows Driverless Vehicles on Public Roads.” Accessed May 19, 2022. https://www.loc.gov/item/global-legal-monitor/2021-08-09/germany-road-traffic-act-amendment-allows-driverless-vehicles-on-public-roads/.

[150] The White House. “Fact Sheet: Biden-Harris Administration Actions to Attract STEM Talent and Strengthen Our Economy and Competitiveness.” *The White House*, January 21, 2022. Accessed November 21, 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/21/fact-sheet-biden-harris-administration-actions-to-attract-stem-talent-and-strengthen-our-economy-and-competitiveness/.

[151] SIA. “2021 SIA State of the Industry Report.” 2021. Accessed May 19, 2022. https://www.semiconductors.org/wp-content/uploads/2021/09/2021-SIA-State-of-the-Industry-Report.pdf.

[152] U.S. Department of Energy. “Energy Storage Grand Challenge Energy Storage Market Report.” 2020. Accessed May 19, 2022. https://www.energy.gov/sites/default/files/2020/12/f81/Energy%20Storage%20Market%20Report%202020_0.pdf.

[153] The White House. “Building Resilient Supply Chains, Revitalizing American Manufacturing and Fostering Broad-Based Growth.” 2021. Accessed May 19, 2022. https://www.whitehouse.gov/wp-content/uploads/2021/06/100-day-supply-chain-review-report.pdf.

[154] Lewis, James A. “National Security Implications of Leadership in Autonomous Vehicles.” 2021. Accessed May 19, 2022. https://csis-website-prod.s3.amazonaws.com/s3fs-

public/publication/210628_Lewis_National_Security_AVs.pdf?WJN5SSLvZl8ofCfoavKu6Ot0rCaHZalC.

[155] Cadell, Cate. "Drone Company DJI Obscured Ties to Chinese State Funding, Documents Show." *The Washington Post*, February 1, 2022. Accessed May 19, 2022. https://www.washingtonpost.com/national-security/2022/02/01/china-funding-drones-dji-us-regulators/.

[156] KPMG. "Autonomy Delivers: An Oncoming Revolution in the Movement of Goods." 2018. Accessed May 19, 2022. https://advisory.kpmg.us/content/dam/advisory/en/pdfs/2018/autonomy-delivers-final-secured-web.pdf.

Appendix O. Abbreviations

ADA	Americans with Disabilities Act
ADAS	Advanced Driver Assistance Systems
ADV	Autonomous Delivery Vehicles
AI	Artificial Intelligence
ARC	Aviation Rulemaking Committee
ASSP	American Society of Safety Professionals
ATC	Air Traffic Control
ATM-X	Air Traffic Management – eXploration
AV	Automated Vehicles
BIS	Bureau of Industry and Security
BLS	Bureau of Labor Statistics
BVLOS	Beyond Visual Line of Sight
CAA	Civil Aviation Authorities
CISA	Cybersecurity and Infrastructure Agency
CMVS	Center for Motor Vehicle Safety
DHS	Department of Homeland Security
DOC	Department of Commerce
DOD	Department of Defense
DOE	Department of Energy
DOI	Department of the Interior
DOJ	Department of Justice
DOL	Department of Labor
DOT	Department of Transportation
ED	Department of Education
FAA	Federal Aviation Administration
FCC	Federal Communications Commission
FEDFLEET	Federal Fleet Policy Council
FMVSS	Federal Motor Vehicle Safety Standards
FRROST	First Responder Robotic Operations System Test
GPS	Global Positioning System
HMR	Hazardous Materials Regulations
ICAO	International Civil Aviation Organization
IMU	Inertial Measurement Units
INS	Inertial Navigation Systems
IoT	Internet of Things
IPP	DOT UAS Integration Pilot Program
ITA	International Trade Administration
JARUS	Joint Authorities for Rulemaking on Unmanned Systems
LIDAR	LIght Detection, and Ranging
ML	Machine Learning
NAICS	North American Industry Classification System
NASA	National Aeronautics and Space Administration
NHTSA	National Highway Traffic Safety Administration
NIFA	National Institute of Food and Agriculture
NIFC	National Interagency Fire Center

NIJ	DOJ National Institute of Justice
NIOSH	National Institute for Occupational Safety and Health
NIST	National Institute of Standards and Technology
NITRD	Networking and Information Technology Research and Development
NOAA	National Oceanic and Atmospheric Administration
NSF	National Science Foundation
NTIA	National Telecommunications and Information Administration
NTSB	National Transportation Safety Board
OSTP	White House Office of Science and Technology Policy
P&D	Pickup and Delivery
PDD	Personal Delivery Devices
PHMSA	Pipeline and Hazardous Materials Safety Administration
Radar	RAdio Detection and Ranging
RF	Radiofrequency
RFI	Request For Information
RPAS	Remotely Piloted Aircraft System
S&T	Science and Technology
SCRI	Specialty Crops Research Initiative
sUAS	Small Unmanned Aircraft Systems
SWAP	Size, Weight, and Power
UAM	Urban Air Mobility
UAS	Unmanned Aircraft Systems
UASSC	Unmanned Aircraft Systems Standardization Collaborative
UDS	Unmanned Delivery Services
UPS	United Parcel Service
USDA	U.S. Department of Agriculture
USPS	U.S. Postal Service
UTM	Unmanned (UAS) Traffic Management
UxS	Unmanned Aerial and Maritime Systems

Additive Manufacturing
& Three-Dimensional Printing

Chapter Contents

List of Tables

List of Figures

7. Additive Manufacturing & Three-Dimensional Printing

Summary

In the Consolidated Appropriations Act of 2021, Congress tasked the National Institute of Standards and Technology (NIST) to prepare a series of studies on critical and emerging technologies, including *three-dimensional printing* (3DP) or *additive manufacturing* (AM), and their impact on the U.S. economy. This chapter addresses:

- industry sectors that implement and promote the use of AM,
- public-private partnerships (PPPs) focused on promoting adoption of AM,
- industry-based bodies developing and issuing standards for AM,
- the status of mandatory and voluntary standards related to AM, both Federal and industry-based,
- Federal agencies with expertise and jurisdiction in industry sectors implementing AM,
- Federal interagency activities relevant to AM,
- Federal regulations, guidelines, mandatory standards, voluntary standards, and other policies concerning AM implemented by Federal agencies and industry-based bodies,
- Federal resources that exist for consumers and small businesses to evaluate the use of AM,
- risks to AM supply chains and marketplace,
- AM-based risks from foreign actors or third parties to the national security, including the economic security,[159] of the United States, and
- long-term trends in AM.

AM is a family of processes that uses a wide variety of materials—typically polymers, metals, or ceramics, but also more exotic substances, like biomaterials containing live cells—to create an object by incrementally adding material based on a digital model. AM has a number of traits that, in combination, make it an exceptionally flexible technology potentially capable of changing manufacturing practices in numerous different industries:

- it is capable of making uniquely complex objects, for example, objects with internal cavities or gradients in physical properties;
- it can produce objects using less material than other manufacturing processes, reducing waste and costs;
- it is able to produce many different objects simply by changing the digital model without substantial adjustment or modification of 3D printing equipment or the need to redeploy a production line, which makes it uniquely well suited to:

[159] The Consolidated Appropriations Act of 2021 refers to "economic and national security," and economic security is understood to be part of national security for the purposes of authorities such as the Consolidated Appropriations Act of 2021 and Section 232 of the Trade Expansion Act of 1962 (Public Law 87-794).

- produce highly personalized or specialized objects in small batches; and
- respond to sudden increases in demand for a product.

Industry Sectors and Public-Private Partnerships

AM technology is used in numerous industries including aerospace, automotive, biomedicine (primarily medical devices, but also pharmaceuticals and biologics), consumer products (including jewelry and sporting goods), energy, printed electronics, construction, and heavy equipment. In May 2022, the White House announced the launch of *Additive Manufacturing Forward* (AM Forward), an initiative focused on using AM technology to strengthen supply chains, grow small- and medium-sized companies, overcome coordination challenges in growing the industries of the future, and expand regional manufacturing ecosystems. AM Forward pledges the U.S. Government to commit resources and work with large manufacturers to help smaller, U.S.-based suppliers adopt new AM capabilities, train workers and provide technical assistance on new AM technologies, and engage in common standards development and certification for AM products. In addition to AM Forward, a number of PPPs support research, development, and innovation of AM technologies in many industry sectors, including America Makes, the Additive Manufacturing Consortium, the ASTM Additive Manufacturing Center of Excellence, the National Center for Additive Manufacturing Excellence, and the Alliance for the Development of Additive Processing Technologies. Moreover, numerous PPPs whose focus is on specific industrial sectors also promote the advancement of AM technology and applications within those sectors.

Industry-Based Standards

In the United States, the American National Standards Institute and America Makes launched the Additive Manufacturing Standardization Collaborative (AMSC) in 2016 with support from NIST, the Department of Defense, and other Federal agencies. The AMSC facilitates interaction among participants—which include private industry, original equipment manufacturers, material suppliers, standards development organizations (SDOs), academia, and government organizations—to develop and maintain an AM standards roadmap. The most recent version—*AMSC Standardization Roadmap for Additive Manufacturing (Version 2.0)*—is a detailed summary of the status of AM-related standards in the United States, including existing standards, standards under development within SDOs, and gaps in standards development. The AM community anticipates Version 3.0 of the AMSC Standardization Roadmap which will be available in the summer of 2023. This substantial update will address the many new and revised AM standards released since the prior version. Among the most active SDOs touching multiple industrial sectors are the American Society of Mechanical Engineers, ASTM International, and the International Organization for Standardization, although sector-specific SDOs, such as SAE International, also address the use of AM for particular applications. In addition to AM-specific standards, the materials, processes, and objects used in or created by AM technology are also covered by product-specific standards.

Federal Standards and Regulations

In the arena of Federal regulations, guidelines, and standards, no single agency oversees all AM processes and uses, and each agency's jurisdiction is generally constrained to the particular sectors covered by its mission and authority. Many agencies participate in, actively contribute to, or enforce industry-based AM standards developed by SDOs, and several agencies have developed or are in the process of developing standards for AM parts and products, including the Department of Defense, the Food and Drug Administration, and the National Aeronautics and Space Administration. In all industrial sectors, existing and new AM products are governed by all appropriate Federal rules and guidelines that apply to analogous products made using non-AM processes.

Interagency Interactions

Federal agencies conducting and/or supporting AM research and development (R&D) or with oversight authority over AM processes or products interact with one another through both formal and informal mechanisms. The Interagency Writing Team on Performance and Reliability of Advanced Manufactured Parts was established in 2021 by the National Science and Technology Council's Subcommittee on Advanced Manufacturing and Subcommittee on the Materials Genome Initiative to identify opportunities for research and development that will improve the quality and reduce the cost of AM parts and processes in sensitive, high-reliability, and safety-critical applications. A number of formal interagency research activities—like 4D Bio^3 (a biomedical research initiative that aims to adapt biotechnology for warfighter benefit) and the Materials Genome Initiative (an effort aimed at expediting the development and deployment of advanced materials, including for AM)—include AM but do not focus on it exclusively. Lastly, agencies interact bilaterally through a variety of mechanisms, both formal (for example, memoranda of agreement) and informal (for example, conferences, working groups, and interpersonal interactions), allowing them to support one another's efforts and stay informed on aspects of AM that are of mutual interest.

Federal Government Resources for Small Businesses to Evaluate and Adopt Additive Manufacturing Technology

The Federal Government provides numerous resources for consumers and small businesses to develop, evaluate, and responsibly adopt AM technology. The Small Business Innovation Research and Small Business Technology Transfer programs provide Federal funding to conduct research that stimulates technological innovation and meets Federal needs, including AM. In addition, several of the Manufacturing USA Institutes—including America Makes, LIFT, BioFabUSA, IACMI, and MxD—make AM-related resources available to small businesses through various mechanisms. Although not limited to AM, NIST's Manufacturing Extension Partnership is a PPP that supports the advancement of AM through a national network of technical and business experts that can support company growth, business improvement, and risk mitigation efforts of small- and medium-sized manufacturers. NIST laboratories conduct measurement science research in AM to provide new measurement capabilities and form the technical basis for new standards. NIST also maintains the Additive Manufacturing Materials Database through its Configurable Data Curation System, which provides a forum for data sharing and open data access for the AM community. The NIST Metals-Based Additive Manufacturing Grants Program has provided dedicated funding for growth of this industry since 2017. Lastly, three of the Department of Energy's National Laboratories—Oak Ridge, Lawrence Livermore, and Sandia—offer state-of-the-art AM R&D capabilities to private-sector entities.

Supply Chain Risks

The AM supply chain consists of two parts: AM equipment and AM materials (which consists of both raw material commodities and AM-ready feedstock). Since AM is a family of manufacturing processes employed very differently in many economic sectors, its impact on markets and supply chains depends on the particular circumstances of its application.

The manufacturer base for industrial AM equipment is large, geographically diverse, and growing; the United States is a major supplier of industrial AM systems. With respect to desktop 3D printers, there was a significant increase in supply to the United States and Europe from Chinese manufacturers in 2020 (likely in response to COVID-19 supply chain disruptions). Overall, however, no major vulnerabilities to the U.S. supply chain for AM systems were identified through reviews of literature or interviews with technical experts.

Materials used in AM processes include polymers, metals, ceramics, and various composites that come in the form of filaments, wires, pellets, sheets, liquids, or powders. The supply chain for each of the different raw materials and AM-ready feedstocks is distinct and depends on the specific AM process, post-processing, and the desired properties of the final product.

The raw materials of AM—particularly metals and polymers, which are the most widely used materials for commercial applications—are common commodities and do not face immediate supply chain concerns, although numerous metals used in AM alloys are listed as critical materials for economic growth and national security and are closely monitored by various government agencies.

In contrast to raw materials, where potential issues involve sourcing, the primary concern facing AM feedstock is a lack of sufficient production capacity (e.g., atomization of metal powder). This concern is expected to be exacerbated as AM is increasingly used to support manufacturing of final products at higher volumes.

Potential for Market Disruption

Overall, the effect of AM on a market depends on the product and sector. Although other manufacturing processes may be better choices for particular products or under particular circumstances, AM has the potential to disrupt markets for a number of reasons:

- AM equipment can be rapidly redeployed to produce very different objects in response to sharp changes in demand;
- the per-unit cost to produce an AM item is independent of its complexity or the number of times a fabrication operation is performed (although additional complexity may require additional validation and quality control);
- AM can be used to produce single parts that replace multi-part assemblies, thereby reducing the number of processes, suppliers, and steps in production; and

- AM products can be quickly and cost-effectively customized by adjusting the digital model rather than the production equipment.

When producing large quantities of the same objects at scale, conventional manufacturing technologies are typically more cost effective than AM due to economies of scale and savings stemming from the increased production volumes. However, even when per-item production costs are higher than alternative manufacturing technologies, AM can still be cost effective and reduce the time to market if it reduces transportation costs or the need to stock inventory by allowing production of parts and other items at the time and location of need. In addition, AM can be incorporated into production lines by creating jigs, tools, and fixtures for use in more efficient machining, casting, or injection molding process and to simplify production lines by replacing multi-part assemblies that require multiple suppliers or many steps to put together.

AM's flexibility, customization, and ease of access present challenges when trying to secure and enforce intellectual property rights for AM software, physical products, and processes or to assign legal liability in the event of product failure. The accessibility and affordability of desktop 3D printers that enable consumers to make objects from polymer and polymer-based materials and the relative ease with which some products can be copied and shared as digital files could lead to cases of intellectual property infringement that are difficult to detect or deter. In addition, companies may need to strengthen their cybersecurity practices and infrastructure to protect digital files needed in AM to avoid theft, illegal copying, and sabotage.

National Security, Including Economic Security

AM is considered vulnerable to three types of threats: (1) theft of technical data, (2) sabotage of AM design files, and (3) manufacturing of illegal products. The digital nature of AM design and process files exposes them to cyber-attacks, either to steal or to modify. In particular, tiny modifications to AM design files can result in compromised parts that are very difficult to detect after they have been produced. In the arena of national defense, use of AM—in both deployed and expeditionary contexts—is particularly relevant to the maintenance and sustainment of equipment, and AM is increasingly used to fabricate parts when replacements or spares are no longer readily available. AM technology and know-how that can be used to fabricate products critical to or that threaten national defense as well as sensitive equipment that includes one or more AM parts are subject to U.S. export controls.

Long-Term Trends

The future of AM builds on its ability to fabricate a wide variety of objects using the same equipment with little or no retooling. Although this characteristic is not unique to AM as a manufacturing technology, it allows manufacturers with AM capabilities to respond rapidly to sudden increases in demand, as they did when faced by the urgent need for personal protective equipment and nasal swabs during the COVID-19 pandemic.

The economic value generated by AM across all sectors is expected to grow by more than 20 % annually from $10.7 billion in 2020 to $34.8 billion in 2026, and in the long term, AM's integration into manufacturing is expected to expand by 50 times its current footprint.

Despite its rapid growth, however, AM should be seen as a means of extending and enhancing established manufacturing capabilities rather than replacing them, primarily as part of the expansion of the modern digital manufacturing and distribution ecosystem.

In addition to streamlining and extending the capabilities of production lines, AM is also expected to encourage the expansion of distributed, localized manufacturing. The flexibility of AM is well-suited for rapid production of small numbers of specialized objects at or near the point of use, which allows firms to both reduce the need to maintain a large inventory as well as decrease the time and expense of transporting and delivering products over long distances.

Recommendations

The U.S. Government is uniquely positioned to convene the full diversity of AM stakeholders, including vocational schools, universities, research labs, standards development organizations, small enterprises, and large corporations, to:

- grow the U.S. economy through the secure and safe development of AM;
- strengthen U.S. global competitiveness through faster and broader adoption of AM;
- mitigate current and emerging risks to the AM marketplace, supply chain, and workforce; and
- advance AM's adoption where there is advantage and opportunity to be gained.

The following recommendations address five broad areas of investment in AM by the U.S. Government and the private sector.

Ensure that AM is Fully Integrated into the Modern Digital Manufacturing Environment

Recommendation 1a. Expand Federal resources to accelerate development and adoption of technical standards, common file formats, and guidance to promote and facilitate more rapid qualification and insertion of new AM technologies into the digital manufacturing environment.

Recommendation 1b. The U.S. Government should continue to support the efforts of the Manufacturing USA institutes to develop multi-institute collaborative projects to advance the integration of AM technologies into the manufacturing environment.

Identify and Mitigate Vulnerabilities in the Supply Chain of AM Feedstock

Recommendation 2a. The U.S. Government should carry out a full assessment of both the capability and capacity of domestic AM material supply chains to meet national security, including economic security, needs and to be prepared to respond to future crises.

Recommendation 2b. The assessment of AM capability and capacity should be used to formulate a Federal strategy to diversify the materials that can be responsibly used for AM to mitigate potential material supply chain disruptions.

Recommendation 2c. The U.S. Government should assess the need for R&D, standards development, and other efforts to facilitate reclaiming and safe use of recycled materials for AM as a potential source of feedstock materials and support such activities accordingly.

Coordinate and Support Investment in AM Research and Development Across the Federal Government

Recommendation 3a. Assess the need for a Federal AM R&D interagency body with the mission of coordinating agency and cross-agency efforts to accelerate the advancement of AM technology by:

- identifying gaps in the U.S. AM R&D portfolio,
- identifying and minimizing redundancy in AM R&D among different agencies,
- encouraging and facilitating cross-fertilization of AM R&D across agencies and industrial sectors, and
- developing guidelines and sharing best practices for the strategic development, purchase, and responsible use of AM technology that enable the Federal Government to be a smart buyer of leading-edge AM systems.

Recommendation 3b. Ensure adequate Federal investments are dedicated to address high priority R&D gaps by conducting precompetitive research and transferring results to the AM community.

Support the Expansion of AM by Manufacturers Across Industrial Sectors and the Adoption of AM by Small Businesses and Manufacturers

Recommendation 4a. The U.S. Government should increase support through the SBIR/STTR programs for small businesses and entrepreneurs developing and applying AM technology.

Recommendation 4b. The U.S. Government should commit the resources needed to advance the objectives of AM Forward: encouraging increased participation of small businesses in the AM supply chain, providing capital and delivering technical assistance to small- and medium-sized manufacturers seeking to adopt AM, setting industry standards, and investing in the AM workforce.

Expand Technical Training and Workforce Development in AM

Recommendation 5a. The U.S. Government should continue to encourage cooperation among AM stakeholders (universities, community colleges, industry, standards development organizations, and professional societies) to develop and adopt certifications and credentials for AM operations.

Recommendation 5b. The U.S. Government should identify and address high-priority gaps in vocational and university education programs aimed at expanding the AM workforce.

7.1. Overview

7.1.1. Definition of "Additive Manufacturing"

Additive manufacturing (AM), the more general and industry-preferred term for 3DP, is the "process of joining materials to make parts from 3D model data, usually layer upon layer, as opposed to subtractive manufacturing and formative manufacturing technologies" [2]. In effect, AM is a family of processes (Table 1) that create an object by incrementally adding material based on a digital model, which distinguishes it from other fabrication methods, like machining, casting, injection molding, or joining [3]. A wide variety of materials can be used for AM, ranging from the familiar, like polymers, metals, and ceramics, to the exotic, like biomaterials containing live cells.

Table 1. Additive Manufacturing Process Categories

Process	Definition
Material jetting	liquid material (for example, wax, thermoplastic, or a metal alloy) is deposited through a jet or nozzle
Binder jetting	an adhesive is deposited through a jet or nozzle to bind solid material, usually powdered
Material extrusion	material is continuously dispensed through an orifice
Directed energy deposition	energy (for example, a high-power laser) is focused to melt and fuse material
Powder bed fusion	part of a layer of powder is selectively fused to build up a three-dimensional object; during fabrication the object resides within and is supported by the accumulated unfused material
Sheet lamination	thin sheets (paper, plastic, or metal) are cut to shape and successively bonded together
Vat photopolymerization	uses directed light to cure polymers layer-by-layer

a Source: [2]

The main original (and still common) use of AM in industry was to make prototypes of objects during design and testing. More recently, the technology is increasingly being used to make finished products [4]. AM has a number of characteristics that in combination give it the potential to disrupt a variety of manufacturing sectors. First, it is capable of making objects whose internal complexity is beyond the capabilities of other fabrication technologies. For example, AM is well suited for items with internal cavities or with gradients in physical properties like density, porosity, and strength. Second, the same AM machinery can be used to produce many different objects simply by changing the digital model (i.e., the instructions for creating the object) without substantial adjustment or modification of the equipment (i.e., retooling) or the need to incur the expense of redeploying a production line. Although other fabrication technologies can be similarly redirected, AM is particularly flexible in the range of items it can produce, making it ideal for creating small batches or even single examples of highly personalized or specialized objects that would not be cost effective using conventional mass production. AM's flexibility also allows it to respond to sudden increases in demand for a product, as was seen in the rapid ramp-up of 3D-printed personal protective equipment and nasal swabs during the early months of the COVID-19 pandemic [5; 6].

AM is perhaps most publicly visible through the increasing availability of affordable desktop 3D printers, which allow hobbyists and small manufacturers to take advantage of the technology. However, AM is becoming increasingly integrated into many different economic sectors. For example, the aerospace industry was an early adopter of AM, initially using it for prototyping, but increasingly using it to fabricate lighter, stronger, and more complex components for aircraft and spacecraft. For similar reasons, AM is seeing increasing application in the automotive sector, where an additional challenge is scaling up production for the large number of parts needed. In the field of biomedicine, AM is already being used to make patient-specific implants (for example, jaw replacements) and prosthetics, and ongoing research and development (R&D) is focused on using AM to create personalized pharmaceuticals and produce living, 3D-printed tissues for transplants. Advances in 3D-printed electronics allow solid-state components to be integrated into the body of a device rather than requiring a separate circuit board. In the construction industry, builders are beginning to produce 3D-printed structures that can be erected quickly where needed. And in the area of consumer products, athleticwear firms are taking advantage of AM's flexibility to produce lightweight sports and safety equipment uniquely customized to fit individual athletes.

In 2020, AM generated an estimated economic value of $10.7 billion, a modest drop in value from 2019 reflecting the effects of the COVID-19 pandemic (Table 2). However, based on market surveys and the pre-pandemic cumulative annual growth rate, AM is forecasted to generate $34.8 billion in all economic sectors in 2026 (Table 2).

Table 2. Past and Anticipated Size of Additive Manufacturing by Economic Sector (in millions of U.S. dollars).

Sector	2017	2018	2019	2020	2021	2022	2024	2026	CAGR[160]
Aerospace	1,372	1,664	2,002	1,654	1,958	2,390	3,450	4,738	19.3 %
Automotive	994	1,260	1,582	1,351	1,655	2,176	3,628	5,963	29.2 %
Biomedicine	957	1,175	1,429	1,748	1,913	2,393	3,633	5,297	22.6 %
Consumer Products	1,443	1,812	2,256	1,959	2,370	3,022	4,765	7,209	24.9 %
Energy	367	447	541	481	560	689	1,008	1,414	20.4 %
Printed Electronics	198	236	278	240	272	327	456	603	17.3 %
Construction	325	396	478	424	494	610	900	1,274	20.9 %
General Industrial[161]	1,517	1,847	2,230	1,836	2,229	2,738	3,997	5,411	19.4 %
Other Sectors[162]	777	944	1,138	1,001	1,170	1,431	2,077	2,884	19.8 %

[160] CAGR = compound annual growth rate used to estimate value of each sector after 2020

[161] "General Industrial" includes applications of AM technologies like foundry, forging, tooling, special machinery manufacturing, and robotics.

[162] "Other sectors" includes education, food and culinary, and offshore marine that are not specifically covered in this chapter.

Sector	2017	2018	2019	2020	2021	2022	2024	2026	CAGR[160]
Total	7,950	9,781	11,934	10,694	12,621	15,776	23,914	34,793	22.5 %

a Source: [7]

In addition to increasing efficiency and expanding capabilities in manufacturing chains, AM is well suited to enhancing distributed, localized production by lowering start-up costs, by making small-scale manufacturing of complex parts economically feasible, and by allowing parts to be made near their site of use, reducing the costs of transportation and maintaining inventory. Lastly, product changeover—i.e., switching from making one product to another—using AM requires less setup cost in the form of time, labor, and tooling than other manufacturing technologies, because it only requires changing the digital design and machine control files and ensuring that the correct material is used rather than retooling or modifying the fabrication equipment. This relatively easy changeover process gives firms the flexibility to respond rapidly to shifts in demand.

Although AM differs from other fabrication processes in important ways, its products and materials are subject to the same standards, guidelines, and regulations governing the production and sale of conventionally manufactured materials and products. In situations where AM is used to make highly personalized products (for example, patient-specific surgical implants), guidance and regulations intended for mass production of large numbers of identical items may need to be modified or extended. Similarly, most of the raw materials needed for AM are subject to similar marketplace and supply chain issues facing the same materials when they are used in other manufacturing methods. However, AM-ready feedstocks (for example, AM-ready metal alloy powders) are often available from only a limited number of providers or facilities, which can lead to supply chain or sourcing challenges.

In May 2022, the White House identified AM as a high priority technology with the launch of *Additive Manufacturing Forward*, an initiative focused on using AM technology to strengthen supply chains, grow small- and medium-sized companies, overcome coordination challenges in growing the industries of the future, and expand regional manufacturing ecosystems [8]. AM Forward is a voluntary compact between the U.S. government and large manufacturers to help their smaller, U.S.-based suppliers adopt new AM capabilities by committing to purchase AM-produced parts from U.S.-based suppliers, train their suppliers' workers and provide technical assistance on new AM technologies, and engage in common standards development and certification for AM products. In addition to coordinating with the private-sector, the Federal Government will act to support the initiative by providing access to capital for small- and medium-sized enterprises, delivering technical assistance to both large and small manufacturers, investing in expanding the AM workforce, and working with the full complement of stakeholders to set technical standards for AM processes and materials [8; 9].

Overall, AM is a rapidly maturing technology that has already been widely integrated in some individual sectors but remains in the R&D stage in others. It is particularly well suited for the manufacture of highly complex parts and individually customized objects and for addressing supply chain issues such as single-source constraints and parts obsolescence. In addition, it is rapidly being integrated into the digital manufacturing ecosystem.

Opportunities to expand the application of AM lie in advancing analytical and modeling capabilities to evaluate performance of AM parts, expanding the variety of well-characterized materials compatible with AM, furthering capabilities to monitor AM processes in-situ as well as evaluate AM products non-destructively, and developing public-domain standards and material databases [10]. Although some AM-ready feedstocks are only available from a relatively small number of suppliers and sources, supply chain constraints are expected to diminish as the technology gains more widespread use in a greater variety of applications and third-party providers enter the market. Although AM will not replace conventional manufacturing, it is expected to play a central role in ensuring American manufacturing competitiveness in the short- and long-term future [11].

7.2. Background

As part of the Consolidated Appropriations Act of 2021 [1] (under the title "American Competitiveness of a More Productive Emerging Tech Economy Act" or the "American COMPETE Act"), Congress mandated studies on eight critical and emerging technologies, including *three-dimensional printing* (3DP). These studies were delegated to be completed by the Secretary of Commerce and, in some cases, the Federal Trade Commission (FTC), in coordination with the heads of other appropriate Federal agencies; within the Department of Commerce (DOC), the National Institute of Standards and Technology (NIST) was selected to lead these inquiries. The mandated study of each technology area was to address four requirements: (1) an overview of the topic area in general with a focus on Federal Government activities and industry impact on the U.S. economy, (2) a marketplace and supply chain review, (3) recommendations to develop policy and legislative proposals, and (4) a written report.

NIST worked with the Science and Technology Policy Institute (STPI) to prepare the mandated reports and specifically requested the following topics be addressed:

- industry sectors that implement and promote the use of each technology,
- public-private partnerships (PPPs) focused on promoting adoption of each technology,
- industry-based bodies developing and issuing standards for each technology,
- the status of mandatory and voluntary standards, both Federal and industry-based,
- Federal agencies with expertise and jurisdiction in industry sectors implementing each technology,
- Federal interagency activities relevant to each technology,
- Federal regulations, guidelines, mandatory standards, voluntary standards, and other policies implemented by Federal agencies and industry-based bodies,
- Federal resources that exist for consumers and small businesses to evaluate the use of each technology,
- risks to the supply chains and marketplace of each technology,
- risks from foreign actors or third parties to the national security, including the economic security, of the United States concerning each technology, and

- long-term trends for each technology.

To address each of these topics, STPI relied on publicly available literature and documents as well as conversations with representatives of relevant Federal agencies.[163] The organization of this chapter addresses each of the requested topics listed above as it relates to 3DP and matches the structure of the reports for the other technology areas mandated by the American COMPETE Act.

7.3. Observations

7.3.1. Industry Sectors that Implement and Promote the Use of AM

The AM family of manufacturing processes is used in a wide variety of industrial sectors to make products as diverse as rocket engine parts, jewelry, buildings, and medical implants. This section reviews the current state of development, application, PPPs, and technical standards relevant to AM in general and in the specific industry sectors where the technology is currently driving important innovations or is anticipated to have substantial impact in the foreseeable future. Although the sectors described here are those where AM is being most actively pursued, this is not an exhaustive list and future development of the technology is expected to be widespread.

7.3.2. Cross-Sectoral AM

Although much R&D, application, and regulation of AM technology is sector-specific, there are a number of PPPs and organizations working to promote and standardize AM processes and materials across industrial sectors. This section focuses on those overarching initiatives and programs; the subsequent sections describe sector-specific development, implementation, promotion, PPPs, and technical standards.

7.3.2.1. AM Public-Private Partnerships and Consortia (Cross-Sectoral)

There is no established, binding definition of a "public-private partnership" used across the Federal Government [12]. Nevertheless, a PPP is commonly understood to be a collaborative working relationship between Federal and non-Federal actors to achieve stated goals and in which the roles and responsibilities of each partner are mutually determined [12]. The PPPs included in this chapter specifically focus on collaborations that promote R&D, technology transfer, and commercialization of AM technology through a variety of mechanisms, including consortia, membership organizations, and other comparable associations. To constrain the scope of this chapter, the focus on PPPs both across and within industry sectors is on efforts intended to broadly buoy AM technology or its use in an industrial sector rather than addressing particular research or technical questions. For this reason, individual research grants for specific projects, contracts for vendor services, and individual Federal grants and loans to support small business growth have not been counted as PPPs in this document.

[163] All online citations were most recently accessed March 22, 2022.

Table 3 summarizes some current PPPs and consortia supporting the advancement of AM technology across industrial sectors. In addition, many regional PPPs are working to develop and promote AM (for example, State-based PPPs).

In addition to PPPs, there are a number of regularly occurring conferences, workshops, and technical sessions with the objective to advance AM technology development and use across industrial sectors. These include the Additive Manufacturing Users Group (AMUG) conference [13], RAPID +TCT Conference sponsored by SME and Rapid News Publications [14], and the Solid Freeform Fabrication Symposium (SFFS) [15].

Table 3. Cross-Sectoral Public-Private Partnerships and Consortia in Additive Manufacturing.

Name	Description
AM Forward	AM Forward is a newly formed PPP, announced May 2022, where large OEMs commit to support AM adoption by their suppliers consisting mainly of small- to medium-sized manufacturers. The OEMs will support their suppliers by purchasing AM parts, providing technical assistance to their suppliers, training their workers, and engaging in AM standards development and certification activities [16].
America Makes	America Makes was launched in 2012 as the first Manufacturing USA institute and is the largest PPP for AM research, development, and innovation in the United States. America Makes focuses on AM technology and education and strives to accelerate the adoption of AM to advance U.S. manufacturing competitiveness [17].
Additive Manufacturing Consortium (AMC)	AMC was established in 2010 by EWI (previously known as Edison Welding Institute) to advance the manufacturing readiness of metal AM by acting as a collaboration platform across industry, government, and academia. Consortium activities include executing pre-competitive research projects, providing technical and other forums for consortium members, and partnering on government-funded research opportunities [18].
ASTM Additive Manufacturing Center of Excellence (AM CoE)	AM CoE is a partnership among ASTM International and representatives from government, academia, and industry. This partnership advances AM standards by conducting coordinated, strategic R&D intended to accelerate the development and adoption of AM technologies [19].
National Center for Additive Manufacturing Excellence (NCAME)	NCAME is a PPP hosted by Auburn University that fosters collaboration among industry, government, academia, non-profit organizations, and ASTM committees to advance AM by closing standards and workforce development gaps [20].
Alliance for the Development of Additive Processing Technologies (ADAPT)	ADAPT is an industry-academia consortium and research center based at the Colorado School of Mines focused on characterization technologies and data informatics to advance qualification and optimization of AM processes and parts [21].

7.3.2.2. AM Standards Bodies and Current State of Industry-Based Standards (Cross-Sectoral)

The U.S. Office of Management and Budget's Circular No. A-119 establishes policies regarding the role of the U.S. Government in the development and use of standards [22]. By establishing uniform engineering or technical criteria, methods, processes, and practices through an accredited consensus process, technical standards (1) improve the safety and reliability of products, materials, and processes; (2) encourage compatibility and interoperability; and (3) establish expectations for users and consumers. Standards developed by Federal agencies or voluntary consensus bodies are commonly cited in regulations and guidance issued by Federal agencies, and adherence to cited standards can be mandatory. In addition, non-binding agency guidelines, which aim to provide information and to indicate current recommended practices, may also cite Federal and other standards.

In the United States, the American National Standards Institute (ANSI) and America Makes launched the Additive Manufacturing Standardization Collaborative (AMSC) in 2016, which does not develop standards itself but supports and coordinates standards development activities. AMSC participants are stakeholders in AM and include private industry, original equipment manufacturers (OEMs), material suppliers, standards development organizations (SDOs), academia, and government organizations [23].

Bodies involved in developing AM standards include SDOs, engineering and technical societies, and government agencies, and much of their activity involves international cooperation and coordination (Fig. 1). Table 4 lists SDOs that touch all or multiple industrial sectors impacted by AM; industry-specific SDOs and bodies within general SDOs are listed separately in the following sections reviewing specific industry sectors.

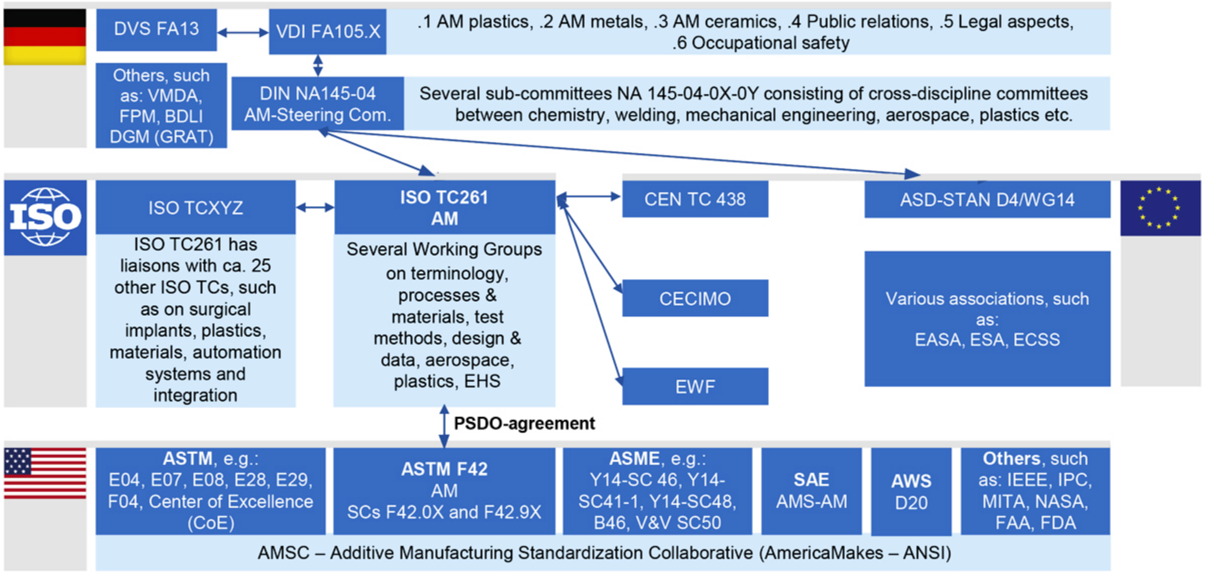

DVS FA13
VDI FA105.X
.1 AM plastics, .2 AM metals, .3 AM ceramics, .4 Public relations, .5 Legal aspects, .6 Occupational safety
Others, such as: VMDA, FPM, BDLI DGM (GRAT)
DIN NA145-04 AM-Steering Com.
Several sub-committees NA 145-04-0X-0Y consisting of cross-discipline committees between chemistry, welding, mechanical engineering, aerospace, plastics etc.
ISO
ISO TCXYZ
ISO TC261 has liaisons with ca. 25 other ISO TCs, such as on surgical implants, plastics, materials, automation systems and integration
ISO TC261 AM
Several Working Groups on terminology, processes & materials, test methods, design & data, aerospace, plastics, EHS
CEN TC 438
CECIMO
EWF
ASD-STAN D4/WG14
Various associations, such as: EASA, ESA, ECSS
PSDO-agreement
ASTM, e.g.: E04, E07, E08, E28, E29, F04, Center of Excellence (CoE)
ASTM F42 AM SCs F42.0X and F42.9X
ASME, e.g.: Y14-SC 46, Y14-SC41-1, Y14-SC48, B46, V&V SC50
SAE AMS-AM
AWS D20
Others, such as: IEEE, IPC, MITA, NASA, FAA, FDA
AMSC – Additive Manufacturing Standardization Collaborative (AmericaMakes – ANSI)

Figure 1. The International Network of Relationships among Selected Additive Manufacturing SDOs

Source: [24].

Table 4. Additive Manufacturing Standards Development Organizations.

Name	Description
Association for the Advancement of Medical Instrumentation (AAMI)	AMMI develops standards for medical devices that cover the design and manufacture of medical devices. AAMI is exploring guidance for applying existing standards to AM and developing new standards as needed.
American Concrete Institute (ACI) Committee 564 - 3-D Printing with Cementitious Materials	The Committee's mission is to develop and report information on three-dimensional printing (3-D) printing, or additive manufacturing with inorganic cementitious materials. Their goals include the development of publications related to AM with cement-based materials, collaboration with ACI committees and other technical organizations (for example, ISO, ASCE, ASTM) on information sharing, and development of guidelines for evaluation of AM materials and technology [24].
American Society of Mechanical Engineers (ASME)	ASME is a professional organization that facilitates knowledge exchange, skill development, and collaboration across all engineering disciplines [25] ASME standards are developed by technical committees within ASME [26]. Several ASME committees are involved in developing AM-related standards: ASME Y14 Subcommittee 46 on Product Definition for Additive Manufacturing; ASME Y14 Subcommittee 41.1 on 3D Model Data Organization Schema; ASME Y14 Subcommittee 48 on Universal Direction and Load Indicators; ASME B46 Project Team on Additive Manufacturing; ASME V&V Subcommittee 50 on Verification and Validation of Computational Modeling for Advanced Manufacturing; ASME Committee on Manufacturing and Advanced Manufacturing (MAM); ASME Board Pressure Technology Codes and Standards (BPTCS)/Board on Nuclear Codes and Standards (BNCS) Special Committee on Use of Additive Manufacturing for Pressure Retaining Equipment; ASME Y14 Subcommittee 41 on Digital Product Definition Data Practices; ASME B89 Project Team 4.23, CT Measuring Machines; ASME Y14.5 on Dimensioning and Tolerancing.
ASTM International (ASTM)	ASTM is an SDO whose committees are involved in developing AM-related standards [27]: ASTM committee F42 on AM Technologies [28]; ASTM committee B09 on Metal Powder & Metal Powder Products [29]; ASTM Committee E04 on Metallography [30]; ASTM Subcommittee E07.10 on Specialized NDT Methods [31]; ASTM Committee E08 on Fatigue and Fracture [32]; ASTM Committee E28 on Mechanical Testing [33]; ASTM Committee E29 on Particle and Spray Characterization [34]; ASTM Subcommittee F04.12 on Metallurgical Materials [35]. In addition to these committees, ASTM has signed a partner SDO (PSDO) agreement with the International Organization for Standardization (ISO) to develop joint AM standards via collaboration between ASTM F42 on AM Technologies and ISO Technical Committee (ISO TC) ISO/TC 261 on AM.

Name	Description
American Welding Society (AWS)	AWS is a professional society that facilitates knowledge exchange, skill development, and collaboration in areas regarding the science, technology, and use of welding, joining, and cutting processes [36]. AWS formed the D20 committee to develop standards related to AM of metal components, since many AM processes are basically welding or joining processes (for example, directed energy deposition and some applications of powder bed fusion). AWS D20 has several task groups active in AM standards development.
Institute for Electrical and Electronics Engineers (IEEE)	IEEE is a professional society that has the goal to advance technology in the areas of electrical, engineering, electronics, communications, and computer engineering as well as computer science [37]. The IEEE Standards Association (IEEE-SA) includes boards or committees that have activities relevant to AM, including: the IEEE Computer/Standards Activity Board; the IEEE Consumer Electronics Society/Standards Board; and the IEEE Engineering, Medicine and Biology Society/Standards Committee. In addition to these boards and committees, IEEE established an Industry Standards and Technology Organization (IEEE ISTO) that is a group of member cooperative programs that support technology standard development and technology adoption by industry. Relevant to AM standard development, the IEEE ISTO Printer Working Group (PWG) is chartered to make printers and associated devices, applications, and operating systems work better together.
Association Connecting Electronics Industries (IPC)	IPC is a trade association for electronics manufacturing that develops standards, provides certification, delivers education and training, develops innovative solutions, and provides advocacy for all members of the electronics industry [38]. IPC Printed Electronics committees involved in developing AM-related standards and guidance include: the Printed Electronics Committee (D-60); the Design Subcommittee (D-61); the Functional Materials Subcommittee (D-63); the Final Assembly Subcommittee (D-64); the Terms and Definitions Task Group (D-64a); the Test Method Development and Validation Subcommittee (D-65); the Processes Subcommittee (D-66); and the 3D Printed Electronics Processes Task Group (D-66a).
International Organization for Standardization (ISO)	ISO is an organization that develops and publishes standards that are accepted worldwide [39]. ISO established technical committee (TC) 261 on AM (ISO/TC 261). A PSDO agreement was signed between ISO and ASTM that established formal collaboration between ISO/TC 261 and ASTM F42 on the development and maintenance of AM standards. Several joint groups exist between ISO/TC 261 and ASTM F42 to develop joint ISO/ASTM standards for AM. Also, ISO has established Joint Working Group (ISO/TC 261/JWG 5) that fosters cooperation among ISO technical committees and ISO/TC 261 on AM-related standards development. Other ISO technical committees (e.g., ISO/TC 184 on Industrial Data) have also developed standards related to AM.

Name	Description
Metal Powder Industries Federation (MPIF)	MPIF is an organization made up of six trade associations, each focusing on various aspects of powder metallurgy [40], including: the Powder Metallurgy Parts Association (PMPA); Metal Powder Producers Association (MPPA); Powder Metallurgy Equipment Association (PMEA); Metal Injection Molding Association (MIMA); Refractory Metals Association (RMA); and the Association for Metal Additive Manufacturing (AMAM). The federation also includes corporate members involved in powder metal (PM) parts design, materials, and products.
MTConnect Institute (MTConnect)	MTConnect is an SDO for the MTConnect standard, which establishes a semantic vocabulary for manufacturing equipment—machines, software, and systems—that provides structured, contextualized data formats that are not proprietary [41]. The MTConnect standards include data from production equipment, sensor packages, and other hardware. The MTConnect Institute established a working group on AM to address development or revision of MTConnect standards for AM.
National Electrical Manufacturers Association (NEMA)	NEMA is an SDO for the electronics industry that facilitates interactions among and involves electrical experts, business leaders, scientists, engineers, and technicians in forums and in the standards development process for electrical and medical imaging standards [42; 43]. The Medical Imaging & Technology Alliance (MITA) is a division of NEMA that develops standards for medical imaging equipment. MITA may develop standards for imaging and verification testing related to the use of AM in medicine. Digital Imaging and Communication in Medicine (DICOM) is the recognized standard for medical images and related information. MITA established a DICOM standard committee to develop and revise the DICOM standard [44].
SAE International (SAE)	SAE is an association of engineers and technical professionals in the aerospace, automotive, and commercial-vehicle industries [45]. SAE is the largest aerospace SDO with over 8,500 aerospace technical standards in use across industry, government, and research organizations. SAE established SAE AMS-AM, which is an AM technical committee in its Aerospace Materials Systems Group. SAE AMS-AM develops aerospace material and process practices, specifications, standards, and other documents covering materials; processing-related, nondestructive testing; and quality assurance documentation. In 2015, the Federal Aviation Administration (FAA) requested SAE develop AM specifications to support FAA guidance materials for AM certification. Other SAE technical committees with interests in AM include, AMS Committee B, Finishes, Processes & Fluids; AMS Committee G-8, Aerospace Organic Coatings; AMS Committee K, Nondestructive Methods & Processes; SMC G-33, Configuration Management Committee; SMC G-41, Reliability Committee; SMC LCLS, Life Cycle Logistics Supportability Committee; and the G-11M, Maintainability, Supportability & Logistics Committee.

7.3.2.3. Status of Industry-Based Mandatory or Voluntary Standards (Cross-Sectoral)

The AMSC facilitates interaction among its participants to support the development of AM-related standards within the United States. As a part of its *Standardization Roadmap for Additive Manufacturing (Version 2.0, June 2018)*, AMSC published a supplement providing a comprehensive view of the status of AM-related standards across all developers and identified whether each standard was AM-specific [46].

When preparing the roadmap to advance future development and revision of AM standards, AMSC worked with AM stakeholders to identify gaps in existing standards and specifications that would advance the adoption of AM if the gaps were addressed. In addition to the identification of gaps, the roadmap provides priorities for standards and specification development, indicates where additional R&D is needed, and identifies the organization(s) that could perform the work. A total of 93 gaps were identified in 8 areas that correspond to AMSC working groups: (1) design, (2) precursor materials, (3) process control, (4) post-processing, (5) finished material properties, (6) qualification and certification, (7) nondestructive evaluation, and (8) maintenance and repair [23]. A "gap" indicates no published standard or specification addresses the particular issue. Of the 93 gaps, 18 were assigned as high priority (needing standard development within 2 years), 51 were medium priority (needing attention within 5 years), and the remaining 24 were low priority.

In April 2022, AMSC published an update to its *Standardization Roadmap for Additive Manufacturing (Version 2.0, June 2018)* that summarizes standard development activities since the previous update in October 2021 [47]. AMSC gathered information from a variety of sources to generate the update, including direct input from subject matter experts and inputs from SDO staff [48]. The April 2022 progress report identifies updates to 61 % of the high priority gaps, 60 % of the medium priority gaps, and 33 % of the low priority gaps as well as 1 standard that was closed and 5 new standards [48]. The AM community anticipates release of Version 3.0 of the AMSC Standardization Roadmap in 2023. This substantial update will address the many new and revised AM standards released since the prior version [49].

7.3.3. Aerospace

7.3.3.1. Development, Implementation, and Promotion of AM (Aerospace)

The aerospace industry has been heavily involved in development of AM materials, processes, and applications since the mid-1990s [50], and many major aerospace companies are developing or using AM capabilities. Applications include brackets, latches, air ducts, parts for heat exchangers, parts for antenna systems, parts for aircraft and rocket engines, and application-specific solid propellant [50–52]. In some instances, aerospace industry users of AM technology are also AM material and process developers [50].

The aerospace industry uses polymers, metals, and composite materials [7] for rapid prototyping, tooling applications (for example, casting dies, manufacturing and assembly tools, and fixtures), component production, and part and tooling repair. The material and process selected for a part is based on user requirements, including performance, lifetime, and cost. Increased use of AM materials, equipment, and parts in the aerospace industry will require continued development of material, metrology, process, data, and testing standards.

7.3.3.2. AM Public-Private Partnerships and Consortia (Aerospace)

Numerous PPPs and consortia—in addition to those focused on AM in general—are advancing AM innovation and adoption by the U.S. aerospace industry (Table 5). In fact, many cross-sector AM PPPs started with a focus on aerospace applications because the aerospace sector was an early adopter of AM technology.

Table 5. Aerospace and Automotive Sector PPPs and Consortia.

America Makes
National Center for Additive Manufacturing Excellence (NCAME)
LIFT
ASTM Additive Manufacturing Center of Excellence (AM CoE)
Additive Manufacturing Consortium (AMC)
Alliance for the Development of Additive Processing Technologies (ADAPT)
SAE Aerospace Materials Specification—Additive Manufacturing Data Consortium (SAE AMS-AMDC)
National Institute for Aviation Research (NIAR)
Center for Aerospace Manufacturing Technologies (CAMT)

LIFT is part of the Manufacturing USA network supporting innovation in manufacturing for the U.S. mobility sector [53], specifically focused on wire arc and cold spray AM technologies [54]. SAE AMS-AMDC is an industry technology consortium formed to develop pedigreed AM material property data that meet requirements for inclusion in industry-accepted databases, which are needed for generating data minima values for SAE Aerospace Materials specifications and standards [55].

Industry and Federal agencies also support university centers where pre-competitive AM R&D is performed. The National Institute for Aviation Research (NIAR) at Wichita State University is funded by the Federal Aviation Administration (FAA) through the FAA joint Centers of Excellence for Advanced Materials (COE JAMS) and the Department of Defense (DoD) through America Makes to define and develop a database in support of qualification of the materials, processes, and parts made using laser powder bed fusion of Ti-6Al-4V metal alloy [56]. Also, NIAR has signed a memorandum of understanding for a collaborative effort to support DoD's accelerated adoption of metal AM technology [57]. The Center for Aerospace Manufacturing Technologies (CAMT) at Missouri University of Science and Technology was established in partnership with Boeing and the Air Force Research Laboratory (AFRL). It is a U.S. center of excellence "for the development and transition of innovative advanced technologies for the aerospace manufacturing supply chain," including AM [58]. An industrial consortium was established at CAMT that performs R&D for its members [59].

7.3.3.3. AM Standards Bodies and Current State of Industry-Based Standards (Aerospace)

A number of SDOs, engineering and technical societies, and government agencies are involved in developing AM standards in the aerospace sector (Table 6).

SAE is a major SDO for the aerospace industry, particularly the SAE AMS-AM technical committee in SAE's Aerospace Materials Systems Group, which develops aerospace material and process practices, specifications, standards, and other documents covering AM-specific materials, processing-related nondestructive testing, and quality assurance documentation. As of September 2021, there were 30 SAE AMS-AM materials and process specification standards either approved or in development [60].

Table 6. Aerospace Sector SDOs and Industry Groups.

Aerospace Industries Association (AIA)
American Society of Mechanical Engineers (ASME)
ASTM International (ASTM)
American Welding Society (AWS)
Institute for Electrical and Electronics Engineers (IEEE)
International Organization for Standardization (ISO)
Metal Powder Industries Federation (MPIF)
SAE International (SAE)

Source: [23]

In response to a request by the FAA to collaborate on a document that addressed unique aspects of certifying AM aerospace components, the Additive Manufacturing Working Group of the Aerospace Industries Association (AIA), which develops voluntary National Aerospace Standards [61], issued *Recommended Guidance for Certification of AM Components* [62]. The report summarizes best practices for consideration as a foundation for compliance to applicable regulations. Additionally, the FAA is engaged with the Metallic Materials Properties Development and Standardization (MMPDS) Emerging Technology Working Group and the Composite Materials Handbook-17 (CMH-17) Additive Manufacturing Coordination Group to develop data and a corresponding framework for allowables for metallic and non-metallic AM materials, respectively.

7.3.4. Automotive

7.3.4.1. Development, Implementation, and Promotion of AM (Automotive)

The automotive industry has used AM for rapid prototyping since the 1980s [63], but in more recent years, the technology's use has expanded to fabrication of customized tooling and low-volume production [50]. The use of AM for production parts is increasing among automakers for components such as aluminum shift paddles [50], nylon ducts, and aluminum and plastic brackets [64]. In addition, aftermarket upgrade and accessory parts are increasingly being made using AM [64].

The automotive industry is involved in R&D of AM to achieve benefits such as reduction in time needed for functional prototyping, effective and efficient fabrication of tooling, and weight reduction or light-weighting, which increases fuel efficiency and is an area of interest in the development of electric vehicles [65]. Automotive OEMs are investing in R&D centers focused on advancing AM for use in future production vehicles [66; 67] and are establishing partnerships with AM companies.

The United States Council on Automotive Research (USCAR) "is a collaborative automotive technology company" whose member companies support pre-competitive R&D projects in collaboration with suppliers, National Labs, universities, and other research institutions [68], including in the area of AM. In September 2021, it published a roadmap to provide an automotive industry perspective on advancements needed for AM to become a common technology used in the production of automotive parts and vehicles [65]. The roadmap focused on four areas—design, materials, manufacturing, and operations/workforce [65]—and is intended to facilitate interaction and collaboration among automotive OEMs, their suppliers, and other stakeholders in AM (Table 7).

Table 7. USCAR Goals for Advancement of Additive Manufacturing in the Automotive Sector.

Design Goals

Educate/train designers and engineers versed in AM and traditional design concepts and approaches.

Develop easily accessible, end-to-end (i.e., materials to part), design methods, and tools having common data/information formats and machine language.

Develop methods and tools to integrate design considerations and actual design with the value proposition and business case for AM.

Develop facility and plant floor layout methods and tools that effectively and efficiently integrate AM equipment and production.

Materials

Develop AM materials that are AM-equipment (for example, laser powder bed fusion equipment) agnostic and are automotive grade as defined by AM specifications and standards

Establish an industrial base to ensure the availability and usability of AM feedstock materials.

Develop new chemistries, materials, and processes to lower the cost of AM feedstock materials.

Develop tools and methods to increase the sustainability and recycling of materials used in AM.

Develop materials characterization and validation methods, tools, and databases.

Manufacturing

Develop cost-effective AM equipment that has throughput, repeatability, size, and robustness to meet production needs; is interoperable with other production (non-AM) equipment and systems; and is compatible with plant-floor automation.

Develop inspection and testing tools and methods that address challenges presented by AM processes, materials, and components.

Develop processes and equipment that reduce energy consumption and waste produced.

Operations and Workforce

Operations

Develop AM equipment that has the ability to connect to plant floor networks through standard interfaces and operational workflow models, and utilizes unified Manufacturing Execution Software (MES).

Integrate monitoring and control systems with AM equipment that enables in-situ digital monitoring and control.

Establish and implement safety standards for AM materials storage, handling, AM part production and transportation of AM materials and parts.

Develop AM equipment considering maintenance activities during design and development.

Workforce

Develop AM equipment where human factors and safety for operators and maintainers are essential design factors.

Develop training and certification programs to educate AM equipment operators and maintainers.

Explore targeted education programs and non-traditional pathways to realize a skilled and diverse AM workforce.

Source: [65]

7.3.4.2. AM Public-Private Partnerships (Automotive)

A number of PPPs and consortia focus on advancing AM innovation and maturity as well as supporting the adoption of AM by U.S. industries, including the automotive sector. Since many of the benefits of using AM are shared between the aerospace and automotive sectors, the advancements achieved by the PPPs and consortia listed for the aerospace sector (Table 5) will benefit the automotive sector as well.

7.3.4.3. AM Standards Bodies and Current State of Industry-Based Standards (Automotive)

The development of material, metrology, process, data, and testing standards is essential to support the increased use of AM materials, equipment, and parts in the automotive industry. SAE International is a main SDO for the automotive industry, although a search for AM-specific SAE automotive standards on the SAE website [69] yielded no results. ISO/TC 261 is developing a standard that applies directly to the automotive industry entitled *ISO/ASTM AWI 52945: Additive Manufacturing for Automotive—Qualification Principles—Generic Machine Evaluation and Specification of Key Performance Indicators for PBF-LB/M Processes* [70]. This joint ISO/ASTM work item was proposed under the ASTM F42.07 subcommittee in December 2020 [71]. As the automotive sector expands its use of AM, other standards may apply based on the materials and AM processes used for automotive applications.

7.3.5. Biomedicine

7.3.5.1. Development, Implementation, and Promotion of AM (Biomedicine)

AM's growth in the biomedical sector is primarily derived from its potential to produce devices and medicines that cannot be made using traditional processes or that are personalized to the needs of individual patients [72–75]. Biomedical uses of AM fall under three broad categories that differ in processes, materials, and applications: devices, pharmaceuticals, and biologics. A device is an object that does not achieve its primary intended purpose through chemical action within or on the body and which is not dependent upon being metabolized [76]. Pharmaceuticals are medications used to prevent, cure, or treat disease. Biologics are products composed of biomaterials, often including living cells. AM examples of biologics include 3D-printed skin tissue for treating severe burns and cuts [77] and a tissue-engineered ear transplant made from a patient's own cells [78]. At this time, AM biologics are primarily a focus of research and have not yet been approved for use in clinical settings.

Medical Devices

Medical devices produced using AM include anatomical models for teaching and planning medical procedures; tools, such as guides used to direct cutting and drilling during surgery; prosthetic limbs, orthopedic implants, cranial implants, and dental restorations; parts for medical machines like ventilators and pumps; and personal protective equipment [73; 75; 79]. AM medical devices have been in use for several decades: custom dental implants first appeared in the 1990s, the first AM prosthetic leg was produced in 2008, and the first AM jaw implant in 2012 [75]. The Food and Drug Administration (FDA) has reviewed and approved more than 100 medical devices including screws, valves, stents, implants (spinal, thoracic, and craniofacial), hip and knee joints, catheters, and dental appliances (crowns, bridges, and dentures). AM implants can be made of a wide variety of biocompatible materials including ceramics, polymers, and metals (including titanium alloys, chromium-cobalt alloys, tantalum, and stainless steel), each appropriate for different applications and made using different AM processes. AM implants can also be made of bio-absorbable material in order to serve as scaffolding for healing tissue—for example, biodegradable stents that do not require surgery to remove [79].

Pharmaceuticals

Like medical devices, AM pharmaceuticals have particularly great potential to advance personalized medicine by producing tablets that contain one or more drugs in specific doses, have customized drug-release profiles, include unique structural and compositional features, and have complex shapes [80; 81]. Appropriate materials for AM drugs include biocompatible polymers, resins, and powders, which can carry the active ingredient themselves or act as a binding agent for the active compounds.

Although pharmaceuticals are an area of active AM R&D, the only AM drug approved by the FDA (in 2015) is Spritam, which is used to treat epilepsy [81; 82]. Spritam takes advantage of AM fabrication to produce a very porous tablet that rapidly disintegrates and delivers the drug significantly faster (in 2 to 27 seconds when taken with water) than conventional fast-melt dosage forms. Although it is manufactured using 3DP, it is not a patient-matched or personalized AM pharmaceutical.

7.3.5.2. AM Public-Private Partnerships (Biomedicine)

Most AM technologies used to create medical devices and pharmaceuticals were developed for other applications in other industrial sectors and were not originally intended for use with biocompatible materials. Both America Makes and the ASTM AM Center of Excellence have projects relevant to medical applications. For example, the ASTM AM Center of Excellence supports a project on *Powder Cleanliness Assessment Classification and Measurement Methodologies* [83] and America Makes sponsors a project on *AM of Biomedical Devices from Bioresorbable Metallic Alloys for Medical Applications* [84].

7.3.5.3. AM Standards Bodies and Current State of Industry-Based Standards (Biomedicine)

The FDA database of voluntary consensus standards includes 87 standards concerning materials, processes, software, and products for biomedical uses that apply to AM, but most are not AM-specific. The organizations that issued these standards are listed in Table 8 [85].

Table 8. Biomedical Sector SDOs.

National Electrical Manufacturers Association (NEMA)
Clinical Laboratory Standards Institute (CLSI)
Association for the Advancement of Medical Instrumentation (AAMI)
International Electrotechnical Commission (IEC)
International Organization for Standardization (ISO)
Underwriters Laboratories, Inc. (UL)
ASTM International (ASTM; formerly the American Society for Testing and Materials)

Source: [85]

No industry-based standards related to AM pharmaceuticals or biologics were found in the course of preparing this chapter. In the area of medical devices, the Radiological Society of America (RSNA) 3D Printing Special Interest Group has issued *Guidelines for Medical 3D Printing and Appropriateness for Clinical Scenarios* [86], which provides recommendations for safe and consistent production of AM models derived from medical images and describes a set of clinical scenarios for appropriate use of AM in patient care.

7.3.6. Consumer Products

7.3.6.1. Development, Implementation, and Promotion of AM (Consumer Products)

Although the most advanced AM technology remains in the realm of research labs and industrial manufacturing facilities, the availability of inexpensive desktop 3D printers (some costing less than $500 [50]) coupled with open-source design software and widely shared 3D digital design files on the internet is allowing consumers to make products like toys, kitchen utensils, and many other items at home [87]. Over the past decade, desktop printers—

primarily using material extrusion of polymers and vat photopolymerization—have experienced explosive sales growth, from around 40,000 sold in the United States in 2012 to over 750,000 in 2020 [50]. Besides home use for hobbyists, 3D printers are also increasingly being used in educational settings from K-12 to universities [87; 88].

In addition to being accessible to individual consumers, AM technology has been adopted to make a variety of consumer products. Because it can minimize production and manufacturing costs, AM is seen as a tool to lower barriers to entry for new businesses and also to conserve resources and reduce waste. AM is particularly well suited to making highly customized products, which allows consumers to personalize items to reflect their individual styles [89] as well as their specific needs and preferences. Application and potential for AM is regarded as particularly high in two consumer product industries: jewelry and sporting goods manufacturing.

In addition to using AM to fabricate final products, AM can also be used in conjunction with other fabrication technologies. For example, injection molding is one manufacturing method used to produce many types of rigid plastic parts in common consumer products. AM can be used to create injection molds that allow faster and more uniform cooling of a product than conventionally made casts. Improved cooling that reduces production cycle times can lead to substantial cost and time-savings for high-volume manufacturing [90].

Jewelry

AM is employed to design and develop metal casting patterns made from expendable materials, which are then used to make a mold for production of the item. Manual labor costs are reduced, and designs can be easily modified or recreated as the patterns can be digitally edited and reprinted [91].

AM is also used to manufacture jewelry directly by printing an item created using computer-aided design (CAD). The process lends itself to the customization of products for individual consumers as the design can be edited or completely remade for each print. Furthermore, this technology may enable the production of zero-waste jewelry [92]. That is, many AM products require build platforms and supports to be incorporated into the design to ensure that the product remains sturdy during fabrication. Current research is exploring the possibility of designing AM jewelry without support structures that must subsequently be removed and discarded [92]. Using AM technology to create jewelry also allows consumers to participate in the design process.

Lastly, allowing jewelry retailers direct access to AM production technology can reduce storage and security expenses associated with maintaining large inventories of finished products [93].

Sporting Goods

AM is used in the sporting goods industry to produce customized products tailored to fit a consumer's specific measurements. Examples include bike helmets designed to fit specific head shapes [94], climbing shoes fitted to enable better grip [95], and mouthguards made to match an individual's jawline [96]. In each case, a scan is taken of the body part, either using a mobile phone or through company scanners, and then used to print customized sports gear. AM also allows the production of lightweight, high-strength sports equipment based on geometries and shapes that are not feasible using other manufacturing processes. Examples include bicycle frames and yokes as well as wheels for in-line skates [97; 98]. Some sporting goods companies [99] have begun to incorporate AM as part of their production process, whereas others have partnered with AM service companies.

7.3.6.2. AM Public-Private Partnerships (Consumer Products)

No PPPs focused on AM consumer products as a whole were identified as part of this study. Technologies developed and promoted by broad-based PPPs like America Makes are expected to be adopted in the consumer products sector where there is commercial incentive and opportunity.

7.3.6.3. AM Standards Bodies and Current State of Industry-Based Standards (Consumer Products)

Numerous organizations have issued standards or are in the process of preparing standards for desktop 3D printer equipment and materials for use in home, small business, educational, and other non-industrial settings (Table 9). In 2019, UL Chemical Safety and UL Standards issued ANSI/CAN/UL 2904, *Standard Method for Testing and Assessing Particle and Chemical Emissions from 3D Printers* [100; 101]. In addition, the Joint ISO/TC 261-ASTM F42 Group has convened a working group focused on *Environmental Health and Safety for 3D Printers* [102]. Lastly, ASTM Subcommittee F42.07.09 focuses on Consumer AM, although they have not issued any specific standards at this time [103].

Table 9. SDOs Addressing Desktop AM Equipment and Materials.

International Organization for Standardization (ISO)
Underwriters Laboratories, Inc. (UL)
ASTM International (ASTM; formerly the American Society for Testing and Materials)

Source: [104]

Standards regulating jewelry focus on the molding and casting process and are not specific to AM beyond general guidelines and practices relevant to the equipment and materials.

The National Operative Committee on Standards for Athletic Equipment (NOCSAE) is a standards organization that aims to enhance athlete safety through performance standards. NOCSAE does not currently have any standards that apply specifically to AM sporting equipment, although the National Football League and other sports leagues require equipment, including AM products, to meet NOCSAE standards. Alternatively, gear can be certified directly by the appropriate national sports league or oversight body. For example, the National Hockey League has certified an AM helmet for professional play [105], and some players in the National Football League have used similar technology [106].

7.3.7. Energy

7.3.7.1. Development, Implementation, and Promotion of AM (Energy)

AM technologies have been applied to a wide range of energy sectors, including wind, solar, hydroelectric, nuclear, and oil and gas [107], where they are used in both energy generation, conversion (for example, solar, fuel, and electrolysis cells; chemical reactors; thermal energy conversion), and storage (for example, zinc and lithium batteries) [108].

AM technologies have been considered for use in the fabrication of nuclear reactor core components to reduce costs and production timelines and to increase safety and performance by tailoring each part to its operating conditions [109; 110]. Currently, private companies, such as Westinghouse Nuclear are engaged in efforts to implement AM in nuclear energy [110].

In the oil and gas sector, AM can improve the design of new technologies by allowing (1) quick prototyping of new parts and (2) manufacture of parts as needed. The first benefit shortens the design-build-test cycle for new field equipment; the second surmounts lengthy procurement processes for spare parts.

7.3.7.2. AM Public-Private Partnerships (Energy)

With respect to PPPs, the Department of Energy (DOE) engages with industry sectors in a variety of ways surrounding AM for energy purposes. For example, Oak Ridge National Laboratory (ORNL) developed a project with the purpose of exploring AM for low-cost development of wind turbine molds. ORNL further collaborated with a wind energy manufacturer to design and build a mold that can be used for the manufacture of wind turbine components [111]. The project spanned from 2015 to 2017 and demonstrated how AM technologies could be used to reduce the manufacturing costs of wind turbine production while achieving performance comparable to conventionally fabricated turbines.

The Manufacturing Demonstration Facility (MDF) at ORNL has a cooperative R&D agreement with a private-sector partner (Cincinnati Incorporated) to further develop MDF’s Big Area Additive Manufacturing (BAAM) system. BAAM is used to serve MDF’s larger goal of improving American manufacturing energy efficiency. The new BAAM system will also work with DOE’s Bioenergy Technology Office and the Center for BioEnergy Innovation [112] to enable more rapid development of bio-derived materials such as bamboo, poplar, flax, and cellulosic fibers [113].

7.3.7.3. AM Standards Bodies and Current State of Industry-Based Standards (Energy)

Generally, although a number of SDOs interact with the energy industry (Table 10), there are few standards that apply specifically to AM in this sector. However, creation of the Energy and Oil/Gas subcommittees within the ASTM F42 International Committee on Additive Manufacturing Technologies suggests that standards in these fields may be developed in the future.

Table 10. Energy Sector SDOs.

ASTM International (ASTM)
International Organization for Standardization (ISO)
SAE International (SAE)
American Society of Mechanical Engineers (ASME)
American Welding Society (AWS)

In the nuclear energy sector, there are no existing standards specifically focused on components manufactured using AM. Certain committees such as the ASTM F42 technical committee have established interest in creating new standards in AM for energy technologies [28].

Current standards applied to AM in the oil and gas industry center on the manufacturing, production, and documentation of metallic equipment components. Only one standard, published in October 2021, provides requirements specifically for the oil and gas industry [114].

7.3.8. Printed Electronics

7.3.8.1. Development, Implementation, and Promotion of AM (Printed Electronics)

The application of AM to printed electronics allows for both the complex design of new products and a reduction in the time to market for such products [115]; it has the potential to be an important competitive factor in the global semiconductor market. Two applications of AM in the electronics industry lie in semiconductor manufacturing and telecommunications.

Semiconductors

AM has been noted as a particularly effective method for reducing errors and costs associated with semiconductor fabrication. This area of application falls under two categories of use: (1) AM of the parts used in semiconductor capital equipment and (2) AM of the semiconductors themselves.

In semiconductor capital equipment, AM increases reliability and improves performance by replacing multipart assemblies with monolithic parts, integrating circuitry into the body of an object, optimizing structure, and maximizing energy efficiency of the finished item [116]. The design freedom and quick transition from prototyping to low volume production of parts may enable semiconductor capital equipment manufacturers to optimize performance and reduce development and production costs.

Although AM is primarily used in the semiconductor industry to make parts for capital equipment, researchers are also exploring the application of AM for the production of semiconductors themselves. There are ongoing efforts to develop AM technologies for the manufacture of two-dimensional (2D) semiconductor materials that could potentially surpass the performance of silicon-based semiconductor devices [117; 118]. Although AM for 2D semiconductor manufacturing is still relatively nascent and not yet commercially feasible, the process holds the potential to lower the cost of developing new products and facilitate new device architectures that are impossible with current fabrication methods [118].

Telecommunications

Current applications of AM in the telecommunications industry center on improving existing technologies by allowing for rapid prototyping and the manufacture of complex parts at a relatively low cost [119]. One example lies in radio-frequency identification (RFID), which uses radio waves to identify physical tags attached to objects that transmit data to a user when triggered from a RFID reader device [120]. AM is currently being used to create ultra-high frequency RFID devices [121].

AM has also been used to manufacture radio-frequency filters to help telecommunication satellites filter out unwanted signals [122]. AM radio-frequency filters are particularly effective in reducing weight and allowing for continued design innovation after the satellite is deployed [123].

7.3.8.2. AM Public-Private Partnerships (Printed Electronics)

AM PPPs touching on printed electronics largely focus on specific R&D objectives rather than the sector as a whole. For example, DOE's Office of Energy Efficiency and Renewable Energy Vehicle Technologies Office has collaborated with ORNL to additively manufacture heat exchangers and other parts for a liquid cooled carbide traction drive inverter [124], a device that is crucial in converting power from the battery of an electric vehicle [125]. The inverter is manufactured from 50 % AM parts and enables more efficient performance than standard semiconductor materials used in electric vehicles.

7.3.8.3. AM Standards Bodies and Current State of Industry-Based Standards (Printed Electronics)

No standards currently exist specifically addressing AM in the telecommunications field. The IPC trade group, which specializes in the standardization of electronic equipment, has issued a number of standards on printed electronics (IPC/JPCA 2291-2013; IPC/JPCA -6901; IPC 4921A-2017; IPC 2292-2018; IPC 4591A-2018), although none of these specifically apply to telecommunications. An important SDO engaged in telecommunications standards is the Telecommunications Industry Association (TIA), but to date, it has not published any standards specifically concerning AM.

The standards regulating AM production of semiconductors are similar to those for telecommunications. In addition to the IPC standards, the Institute of Electrical and Electronics Engineers (IEEE) Standards Association published *IEEE 1620-2008: Standard for Test Methods for the Characterization of Organic Transistors and Materials*, which establishes reporting practices for electrical characterization of printed and organic transistors [126]. In addition, the electrotechnical commission has provided a standardization of terminology, processes, and equipment for printed electronics in *TC 119 Printed Electronics* [127].

7.3.9. Construction

7.3.9.1. Development, Implementation, and Promotion of AM (Construction)

AM applications in the construction sector have matured considerably in recent years in response to rising demand for more efficient, sustainable, safe, and affordable construction solutions [128]. Paired with building information modeling and employing common construction materials such as concrete, asphalt, polymers, metals, and ceramics, 3D printers can create prefabricated building components (for example, walls, roofing, doors) and replacement parts; they can also produce entire structures directly onsite. Working with technology developers and manufacturers, construction firms worldwide are beginning to test various printers and train their workers to operate them. Although 3D-printed building projects remain relatively few today and the technology is still in the early stages of development, the industry expects substantial growth in 3DP suppliers, material compatibility, and construction within the next 5 years [50].

AM is commonly used to create small-scale architectural models during the structural design process. In recent years, there have been attempts to scale up and develop AM technologies that incorporate conventional construction materials like concrete to "print" homes that are as easy to build and customize as architectural models. The first fully 3D-printed house was built in Amsterdam in 2014 as a proof-of-concept project. Since then, a number of companies have successfully built commercial and residential structures, the largest of which stands two stories tall and has a total area of 6,900 square feet. The majority of these structures are made from concrete or concrete-like materials; some developers use thermosets composed of a resin matrix embedded with glass or carbon fibers to increase tensile strength and others are experimenting with bioplastics, steel, and living materials like fungus [129; 130].

AM has the potential to greatly improve the cost, time, and sustainability of construction. Three-dimensional concrete printing (3DCP) technologies can result in less material waste than traditional construction [131] and provide opportunities to incorporate in-situ resources into material feedstock in resource-scarce environments. Proponents of AM technologies claim that inexpensive, rapidly built 3D-printed homes could alleviate the housing crisis facing many U.S. cities. One firm estimates that its AM construction technology can print a single-family home (excluding the time and cost of installing electrical wiring, plumbing, roofing, etc.) for $4,000 in less than a day and plans to begin constructing a residential community of 100 homes in 2022 [132].

In 2017, the National Science Foundation (NSF) hosted a workshop on *Additive Manufacturing (3D Printing) For Civil Infrastructure Design and Construction* that resulted in general recommendations to address knowledge gaps and knowledge transfer and promote research in AM for civil infrastructure [133].

7.3.9.2. AM Public-Private Partnerships (Construction)

The National Aeronautics and Space Administration (NASA) and DoD have expressed significant interest in the versatility and flexibility of 3DCP technologies in extreme and expeditionary environments. ICON is developing a 3DCP system that can be adapted for both terrestrial and space environments; the company participated in NASA's 3D-Printed

Habitat Challenge and has partnered with NASA's Moon-to-Mars Planetary Autonomous Construction Technologies (MMPACT) project to produce and demonstrate its lunar launchpad construction system [134]. ICON has also partnered with the Defense Innovation Unit within DoD to demonstrate the rapid fabrication of "vehicle hide structures" in expeditionary environments [135]. The U.S. Army Corps of Engineers Automated Construction of Expeditionary Structures program has worked with Caterpillar and other partners in the construction industry to develop robust 3D printers that can produce bridges, bunkers, and other expeditionary infrastructure while incorporating local materials into the mortar mix [136].

7.3.9.3. AM Standards Bodies and Current State of Industry-Based Standards (Construction)

Broader adoption of AM construction technologies faces significant technical and regulatory challenges. The design and construction of structures built using traditional materials and methods relies on construction standards based on empirical data and knowledge accumulated over many years. Establishing AM as a reliable, verifiable construction technology will require research and standardization by engineers and designers and substantial coordination with regulatory bodies. Work in this area is early and ongoing, and many standards-setting activities in AM for construction focus on concrete and concrete-like materials (Table 11).

Table 11. Construction Sector SDOs.

UL (Underwriters Laboratories)
International Code Council (ICC)
ASTM International (ASTM; formerly the American Society for Testing and Materials)
National Fire Protection Association (NFPA)
American Concrete Institute (ACI)
American Society of Civil Engineers (ASCE)

Individual construction projects often require the use of customized materials and processes, which hinders efforts to develop general standards and guidelines for 3DCP. Additional engineering analyses and documentation needed to ensure that a final structure will meet State and local building codes could result in a more involved and time-consuming process for both the developers using novel materials and the local authorities that determine compliance [137].

For example, companies developing 3DCP technologies often use proprietary formulas that are optimized for the local environment (for example, the feedstock mix used to construct buildings in Dubai is adapted to withstand high temperatures). Characteristics of printed concrete are highly dependent on the printing process, configuration, formulation, and local conditions. There is limited research on best practices and formulations for 3DCP—some studies have developed printed concrete with higher stiffness and fire resistance than conventional concrete, while others studies have concluded that printed structures are weaker than those built using conventional techniques [129].

In the United States, there is no federally mandated building code; building codes are established and enforced by State and local jurisdictions. However, voluntary, consensus-based codes published by the International Code Council (ICC) and National Fire Protection Association (NFPA) are "nationally recognized" and are typically adopted by State and local authorities [138]. These model codes provide a comprehensive guide for builders to ensure human health and safety and reference relevant standards developed and published by other standards-setting and professional organizations such as ANSI, ASTM, and the American Society of Civil Engineers (ASCE). ICC's *International Building Code* (IBC) is adopted by or is in use in all 50 States [139]. NFPA has also developed the *NFPA 5000: Building Construction and Safety Code*, which is intended to be NFPA's equivalent to the IBC. NFPA 5000 is currently only referenced in seven States and has not been adopted by any, although numerous NFPA standards are referenced throughout the IBC and other codes [140].

The American Concrete Institute's Committee 564-3-D Printing with Cementitious Materials is working to develop and report information on AM with inorganic cementitious materials. Its goals include the development of publications related to AM with cement-based materials, collaboration with ACI committees and other technical organizations (for example, ISO, ASCE, ASTM) on information sharing, and development of guidelines for evaluation of AM materials and technology. Subcommittee 564-0A is working to develop and publish a report on concrete 3DP emerging technologies. Two other subcommittees (564-0B and 564-0C) are developing guidance documents for structural design, material testing, and formulation of concrete 3DP applications [141].

In 2020, Underwriters Laboratories (UL) released UL 3401, *Outline of Investigation for 3D Printed Building Construction*, a code outlining a method for evaluating "the printer, fabrication process, and materials used to verify that they consistently produce building elements with the same properties" [129]. 3DCP companies can follow these guidelines to test and evaluate material samples and produce data and documentation that can be used to determine compliance with standards in the IBC and NFPA 5000. UL partnered with ASTM, the ICC, and other building authorities in developing UL 3401, and its standards are referenced in the 2021 edition of the *International Residential Code* (which provides guidelines for the construction of residential homes three stories or less) and may be added to future editions of other ICC codes [137]. Within ASTM, committees on concrete and concrete aggregates (C09) and AM technologies (F42) are working on developing new standards for 3DCP and harmonizing 3DCP technologies with existing requirements. ASTM is also a member of an ISO working group on 3DCP [131].

7.3.10. Heavy Equipment

7.3.10.1. Development, Implementation, and Promotion of AM (Heavy Equipment)

Although not as large a sector as aerospace or automotive, heavy equipment manufacturers are working to integrate AM components and technologies into production lines for OEM products and to supply replacement parts for aftermarket users. Similar to other industries, heavy equipment manufacturers are using AM components and tooling to reduce labor costs, shorten production lead times, and improve machine capability and performance [142]. In

2015, Caterpillar established its Additive Manufacturing Factory for prototype design and development and for production-scale manufacturing for new equipment [143]; in 2017, it partnered with German AM company FIT AG to produce aluminum and titanium parts for production [144]. As of 2018, Volvo CE has used AM to manufacture plastic spare parts for replacement in off-road equipment, and is working towards producing metal AM components as well [145].

7.3.10.2. AM Public-Private Partnerships (Heavy Equipment)

While the majority of R&D on AM components for heavy equipment has been conducted by private companies, in 2017 a number of industry groups (the Association of Equipment Manufacturers, National Fluid Power Association, and the Center for Compact and Efficient Fluid Power), and academic institutions (Georgia Tech, the University of Illinois–Urbana-Champaign, and the University of Minnesota) partnered with ORNL's MDF to develop the Additive Manufactured Excavator [146]. The operator cab, boom (hydraulic arm), and heat exchanger of an excavator were successfully 3D-printed at the MDF, and the working system was demonstrated at the CONEXPO-CON/AGG trade show [146].

7.3.10.3. AM Standards Bodies and Current State of Industry-Based Standards (Heavy Equipment)

No standards for heavy equipment that specifically pertain to the use of AM components were identified in the course of preparing this chapter. Standards-making bodies like ASTM are working towards standardizing AM applications for heavy equipment; ASTM's F42 committee on AM includes subcommittees focused on construction [147] and "Transportation/Heavy Machinery" [148]. Similar efforts to qualify and standardize material properties and characteristics of AM parts and processes for heavy equipment and heavy machinery will likely affect the construction and related industries as they are incorporated into standards or accepted as best practices.

7.4. Federal Agencies with Jurisdiction

AM products are generally governed by the same Federal regulations, guidelines, and standards that apply to analogous products made using non-AM processes. As a result, no single agency oversees all uses of AM and each agency's jurisdiction is generally constrained to the particular sectors covered by its mission and authority. The focus here is how Federal agencies are approaching the unique challenges posed by AM within various economic sectors rather than attempting to comprehensively document every authority that may apply to AM. In many sectors, particularly those where AM is primarily at the R&D stage of maturity and has not yet been widely adopted for commercial use, Federal agencies have not yet issued guidelines or regulations specifically addressing AM or they are currently in the process of gathering information in preparation to issue guidelines in the future. The challenges faced by Federal agencies in overseeing and regulating AM arise from the technology's rapid rate of development and adoption, decentralized nature, high degree of process sensitivity, and ability to create highly personalized products. Mass production at centralized facilities fosters consistency in process and uniformity of product, which makes inspection and enforcement of standards and regulations straightforward. AM, in contrast, allows small-scale producers with less experience fulfilling regulatory requirements to produce variations on existing products, potentially making application of rules more ambiguous and enforcement more difficult. In addition, the melding of material processing and product fabrication may have implications for Federal buy-American policies that will require adjusting rules regarding percent-based component requirements and manufacturing location.

7.4.1. Aerospace

The responsibility for certification of aerospace systems resides with FAA, NASA, and DoD (Fig. 2).

The FAA has authority to issue aviation safety rules [149] that include establishing "minimum standards required in the interest of safety for appliances and for the design, material, construction, quality of work, and performance of aircraft, aircraft propellers and engines [150]." To ensure the safety of new appliances, the FAA establishes certification procedures for new products that include a type certificate and a production certificate. The FAA issues a type certificate when an applicant has demonstrated via test and analysis that the type design data meet applicable regulatory requirements. A production certificate is issued when an applicant's manufacturing facilities demonstrate the capability to produce the specified product in accordance with the type certificate [151].

NASA utilizes technical standards (developed by industry, SDOs, and NASA) [152] in program and project requirements documents [153]. NASA's use of technical standards is important for ensuring compliance with legal and other requirements, holding contractors accountable for delivering specified products and services, capturing lessons that can inform future technical recommendations and requirements, establishing a common basis for interoperability, and minimizing conflicts and duplication of effort [153].

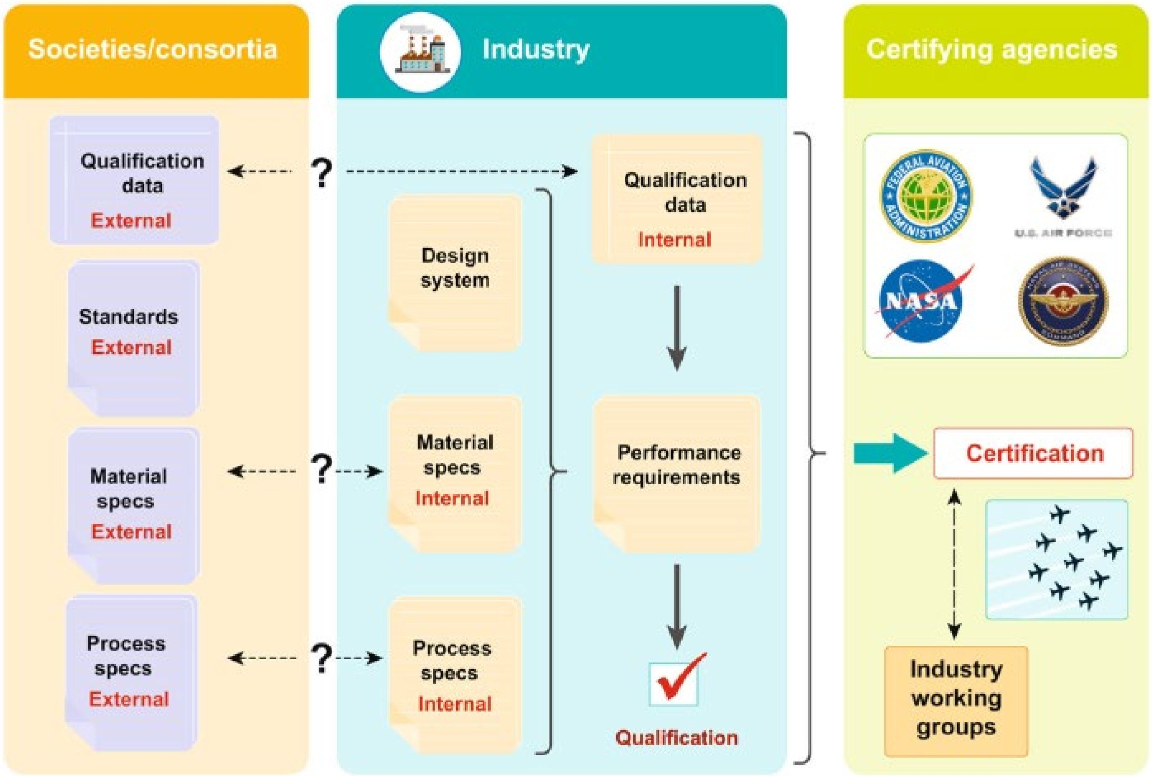


Figure 2. Illustration of the Qualification and Certification Landscape for Aerospace Systems.

Source: [154].

Each service branch within DoD is interested in using AM for making hard-to-find replacement parts for older systems, for fabrication of tools and parts by expeditionary forces, and in production of new systems [155]. The Air Force is the main service that is involved in establishing specifications and standards for aerospace systems, but each service or agency within DoD establishes requirements for a program or for organizational use of a technology utilizing established specifications and standards. Similar to other Federal agencies, DoD uses non-government standards to the maximum extent possible to meet the needs for a given program or organization [156].

7.4.2. Automotive

The National Highway Traffic Safety Administration (NHTSA) regulates the safety of motor vehicles and related equipment and issues *Federal Motor Vehicle Safety Standards* (FMVSS) [157], some of which incorporate standards from SDOs and other agencies [158]. NHTSA also regulates fuel economy in light-duty vehicles and medium- and heavy-duty trucks through the Corporate Average Fuel Economy (CAFE) program.

EPA establishes regulations that control the automotive sector’s impact on the environment, including regulations governing manufacturing, repair, and waste as well as air pollution [159; 160]. EPA regulations specify the test procedures employed to generate the data used to certify compliance with a specific regulation. The EPA can approve SDO standards (for example, test method standards), which can be used for compliance testing [161; 162].

7.4.3. Biomedicine

The FDA is the primary agency overseeing AM in the medical sector. Part of its mission is to ensure the safety, efficacy, and security of human and veterinary drugs, biological products, and medical devices, including those produced using AM [163]. For the most part, FDA has been able to review and regulate AM medical devices using existing regulations by proactively identifying similarities with non-AM technologies [164] and applying quality system regulations that provide a framework to ensure that a manufacturer's product consistently meets required specifications. At this time, almost all AM products that have received FDA approval are medical devices, regulated by the Center for Devices and Radiological Health (CDRH); the FDA has not issued any special guidance for AM drugs or biologics at this time (regulated by the Center for Drug Evaluation and Research and the Center for Biologic Evaluation and Research, respectively).

In 2017, the CDRH issued *Technical Considerations for AM Medical Devices: Guidance for Industry and Food and Drug Administration Staff*, which outlined considerations for AM manufacturers with respect to design and manufacturing as well as device testing with a focus on quality system requirements and documentation of AM parameters and processes for devices that include at least one AM component or step. However, the opportunities for decentralized and personalized fabrication made possible by AM, embodied in point-of-care (POC) manufacturing, present new challenges to the regulation of medical devices: (1) assuring POC devices are safe and effective, (2) assuring control of the AM process used to make a POC device, (3) clarifying responsibility for safety and efficacy of POC devices, and (4) establishing training and manufacturing capabilities at POCs.

To address the issues raised by POC manufacturing, in 2021 the CDRH released *FDA Discussion Paper: 3D Printing Medical Devices at the Point of Care*, whose purpose was to gather feedback from the public to inform future policy development [165]. FDA identifies three regulatory classes for all medical devices based on the level of risk and the regulatory controls necessary to provide reasonable assurance of safety and effectiveness:

> Class I—low risk: Class I devices are exempt from premarket review but must comply with manufacturing and quality control standards. Examples of Class I AM devices include bandages, gloves, and handheld surgical devices.
>
> Class II—moderate risk: Class II devices must be demonstrated to be substantially equivalent to an existing device, reducing the need for clinical research. This is done through the use of a 510(k) premarket submission made to FDA. Examples of Class II AM devices include infusion pumps and pregnancy kits.
>
> Class III—high risk: Class III devices are life-supporting or life-sustaining; they require a full application for premarket approval including data from clinical trials. Examples of Class III AM devices include implants and pacemakers.

To guide ongoing discussions about the regulation of AM devices produced at a POC, FDA posed a series of hypothetical scenarios in its discussion paper with different levels of responsibility for health care facilities and device manufacturers [165]:

A. Fabrication of devices at the POC through the use of turn-key medical device production systems (MDPS) provided by a manufacturer but operated by staff at a health care facility. In this scenario, the manufacturer would be responsible for meeting regulatory requirements and obtaining approval for the MDPS.

B. A manufacturer is co-located at or near the POC and is the party responsible for fulfilling regulatory requirements as part of the service it provides to a health care facility. In this case, the manufacturer could be certified once but operate local branches at multiple POC sites.

C. The POC health care facility assumes all the responsibilities of a device manufacturer, including meeting regulatory requirements.

The scenario-based discussion framework acknowledges the need for clear standards for materials, processes, equipment, training, certification, and manufacturing parameters to manage risk.

Like AM medical devices, a major benefit of AM pharmaceuticals is that they can be produced at a POC. For production of personalized drugs using AM technology, a quality-by-design approach that precisely defines the parameters and steps of the AM process may provide a more sound basis for patient-specific medications with consistent and stable dosage and other characteristics [80; 81]. Broader adoption of personalized medicine through the use of AM pharmaceuticals will require expanding current guidelines to cover AM-specific materials and manufacturing techniques.

7.4.4. Consumer Products

The Consumer Products Safety Commission (CPSC) is the Federal agency tasked with reducing unreasonable risk of injuries and deaths associated with consumer products and enforcing consumer product safety regulations [166]. In 2020, the CPSC issued a report on *Safety Concerns Associated with 3D Printing and 3D Printed Consumer Products* [87] that identified two broad hazard areas for AM: (1) hazards posed by AM processes and materials and (2) hazards posed by printed products. AM equipment hazards were similar to other kinds of machinery: thermal, fire and combustion, electrical (shock), mechanical, and chemical (emission of vapor and particulates), and can be mitigated by adherence to appropriate standards and manufacturer certifications. Material hazards concern the safe storage and use of AM feedstock, with particular note of the danger posed by toxic emissions (chemical and particulate) that may occur during the AM fabrication process. The agency noted that the rapid expansion of desktop 3D printers has made the technology available to a much larger population of users with less expertise, less familiarity with regulations, and working in less controlled environments than operators in industrial settings. The CPSC further noted that small manufacturers may also be less prepared to perform failure analysis and to select safe and appropriate raw materials when making specialized or customized products.

In addition, the low barriers to entry for manufacturing and development for some AM applications present new challenges for the protection of IP and competitive advantage that may require new regulations [167].

Section 5-A of EPA's Toxic Substances Control Act may also apply to the development of consumer products [168]. The section notes that EPA requires notice before a chemical substance or mixture is used in a new way that may create concern. One such example is acrylonitrile butadiene styrene, the material used to create LEGO bricks. While this material is approved for generating hard plastic bricks, it has not been approved for 3DP in the home and has the potential to release chemical emissions when heated in a desktop 3D printer (EPA interview, 1/18/2022).

7.4.5. Energy

The principal Federal agency engaged in advancing AM technology broadly in the energy sector is DOE. DOE's Advanced Manufacturing Office has partnered with ORNL to print items that achieve greater efficiency in energy generation [169] (other DOE labs are also active in AM R&D with a wide range of applications, including the energy sector). Although creating AM standards is not part of DOE's mission, the agency does engage with a number of standards organizations in an advisory role, including ASMC through America Makes (DOE interview, 1/24/2022).

The NRC contributes to standards and has oversight over components used in nuclear power plants. Regulations and requirements depend on the significance of a particular component. Some components may fall under the process described in 10 CFR §50.59, which allows nuclear power plants to make hardware changes without NRC approval [170]. Novel hardware changes to other components generally require NRC approval.

7.4.6. Printed Electronics

The Federal Communications Commission (FCC) has the authority to create legally binding public rights and obligations [171] and can also issue non-legislative rules and procedural rules, which are not binding but can demonstrate an exercise of discretionary power. As AM is applied to the communications sphere, FCC may release rules affecting the use of AM in telecommunications.

DoD is another agency that may have jurisdiction over AM electronics. As a starting point, DoD places significant restrictions on integrated circuits designed and manufactured for the Federal Government [172]. The agency's work in supply chain regulation, particularly surrounding semiconductor technology [8], may also affect AM as it transforms the nature of semiconductor design, manufacturing, and transport.

7.4.7. Construction

There is no Federal agency tasked with enforcing building code compliance in the United States. The regulation and standardization of 3DCP technologies for construction will largely be determined by updates to model building codes and actions by State and local authorities, although Federal agencies are involved in the development of building codes and compliance efforts for federally funded construction.

NIST proactively contributes to the development and updating of model building codes by developing measurement science tools and scientific knowledge for reinforced 3D-printed concrete structures, information that could contribute to future building codes [173]. NIST also has authority under the National Construction Safety Team Act, 15 U.S.C. § 7301 [174], to investigate the causes of certain building failures and to recommend, as necessary, specific improvements to building standards, codes, and practices based on the findings of the investigation.

The Federal Emergency Management Agency (FEMA) uses its funding authority to enforce minimum code standards for federally funded construction or reconstruction projects following a disaster. If a building's repair replacement is funded using FEMA public assistance, it must meet minimum standards (hazard-resistant codes published by the ICC) unless local codes are stronger [175; 176].

Under the Public Buildings Amendments of 1988 [177], construction by the General Services Administration (GSA) and other Federal agencies must comply with nationally recognized building codes (such as the ICC and NFPA) "to the maximum extent feasible."

7.4.8. Heavy Equipment

The Occupational Safety and Health Administration (OSHA) within the Department of Labor sets and enforces workplace safety and health regulations and standards, including standards related to the use and design of a wide range of machinery and equipment used in construction and other heavy industries, such as cranes, dump trucks, bulldozers, and excavators. For example, some of OSHA rules and guidance reference consensus standards established by ASME, ANSI, and ASTM, among others [178]. OSHA does not test, approve, certify, or endorse any specific equipment, product, or procedure, including machine design and risk assessment techniques.

The Federal Motor Carrier Safety Administration (FMCSA) within the Department of Transportation is the lead federal agency responsible for regulating and providing safety oversight of commercial motor vehicle operations. The FMCSA regulates the operation of vehicles used in construction that operate on roadways and meet the Federal definition of a commercial motor vehicle [179].

Lastly, EPA regulates emissions standards for heavy equipment [180].

7.5. Interaction of Federal Agencies with Industry Sectors

Federal agencies interact with industry sectors in a variety of ways including collaborating with manufacturers through PPPs, providing regulatory oversight, and fostering economic development as well as conducting and supporting basic and applied R&D (Table 12). In addition to the roles captured in Table 12, the U.S. Government is also a consumer of AM products; in these cases, agencies such as NASA and DoD work in close partnership with providers and enforce stringent standards for the specialized AM products they purchase (see below for agency-specific policies). The exact nature of an agency's presence on the AM landscape depends on its mission and authority. In addition to publicly available information, the following descriptions of agency activities in the AM sector were augmented with interviews with agency representatives. Agencies and points of contact were provided by NIST.

Table 12. Agencies' Roles in Additive Manufacturing.

Agency	Research and Development	Regulatory Enforcement	Establishing Standards	Public-Private Partnerships
BIS		X		
CDC	X			
CPSC		X	X	
DoD	X		X	X
DOE	X			X
EPA	X	X		
FAA	X	X	X	X
FDA		X		X
FMCSA		X		
NASA	X		X	X
NHTSA		X		
NIST	X		X	X
NRC		X	X	
NSF	X			X
VA	X			X

7.5.1. National Institute of Standards and Technology (NIST)

NIST's core mission focuses on working with industry to advance measurements and standards. NIST laboratories conduct measurement science research in AM to provide new measurement capabilities and provide the technical basis for new standards, including in the areas of material characterization, real-time control of AM processes, qualification methodologies, and system integration [181]. NIST also maintains the Additive Manufacturing Materials Database through its Configurable Data Curation system, which provides a forum for data sharing and open data access for the AM community. The NIST Metals-Based Additive Manufacturing Grants Program has provided dedicated funding for growth of metals-based AM since 2017. NIST holds workshops, industry meetings, and outreach events attended by industry representatives, researchers, and SDOs to identify needs and priorities for standards and to drive AM technology advancements (for example, the next-generation of AM simulation software through the AM-Bench series of technology challenges [182]). NIST researchers partner with Manufacturing USA institutes such as America Makes, LIFT, MxD, and the National Institute for Innovation in Manufacturing Biopharmaceuticals (NIIMBL), as well as with industry consortia such as the Additive Manufacturing Consortium. NIST representatives serve on SDO committees (including those convened by ASTM, ISO, SAE, ASME, and AWS) that also include industry and other representatives. NIST also participates in the AMSC. Although not limited to AM, NIST's Manufacturing Extension Partnership supports the advancement of AM through a national network of technical and business experts that can support company growth, business improvement, and risk mitigation efforts for small- and medium-sized enterprises.

7.5.2. Food and Drug Administration (FDA)

An important part of FDA's mission is to ensure the safety, efficacy, and security of drugs, biological products, and medical devices. In this role, FDA regulates only the labeling and distribution of medical products, not how they are used in the practice of medicine. As a consequence, FDA's oversight of AM primarily focuses on biomedical products technology rather than the AM equipment used to create those products. FDA communicates with equipment manufacturers to help implement quality process guidelines for AM production of medical devices. In addition, FDA personnel conduct inspections of manufacturer facilities and interact with industry representatives at conferences and through organizations like NIIMBL and MxD (Manufacturing times Digital) (both Manufacturing USA institutes), the Parenteral Drug Association, ASME, and Advent. FDA also participates as a partner in America Makes (FDA interview, 1/18/2022).

7.5.3. Department of Defense (DoD)

DoD carries out a large variety of activities in support of developing and applying AM technology in the defense sector. AM-related policy within DoD is coordinated by the Joint Additive Manufacturing Working Group (JAMWG) under the Joint Defense Manufacturing Council. The JAMWG coordinates research and engineering, acquisition, sustainment, and logistics related to AM and works to integrate AM into DoD and the defense industrial base as well as align AM activities across DoD and with external partners. In addition to being a partner in America Makes and sitting on SDO committees, DoD defines and publishes material and process specifications for AM parts through efforts like the Joint Metal Additive Database Definition (JMADD) Pathfinder, a publicly available, substantiated material property and process specification database for laser powder bed fusion of titanium alloy Ti6Al4V that is being built in collaboration with other Federal agencies, universities, and industry partners. In addition to carrying out and supporting basic and applied AM research at the Defense University Research Instrumentation Program, the Multidisciplinary University Research Initiative Program, Defense Advanced Research Projects Agency (DARPA), and each of the service branch research laboratories (Army, Navy, and Air Force), DoD also supports several Manufacturing USA Institutes and participates in America Makes (DoD interview, 1/24/2022).

7.5.4. Federal Aviation Administration (FAA)

FAA's primary focus on AM technology is to assure its safe introduction in aviation and supporting efficient product certification by U.S. industry. It works closely with industry through SDOs, working groups, and consortia—including the AIA AM Working Group, ASTM, the Composite Materials Handbook-17 (CMH-17) Additive Manufacturing Coordination Group, Metallic Materials Properties Development and Standardization (MMPDS) Emerging Technology Working Group, and SAE—to develop industry-based standards for the AM materials and processes used to make aircraft parts. In addition, FAA collaborates with other Federal agencies and industry partners in America Makes, MMPDS, and CMH-17 and supports AM R&D conducted by university partners through its Centers of Excellence (FAA interview, 2/7/2022). Lastly, FAA is also engaged in discussions with foreign civil aviation authorities to harmonize regulatory requirements for AM used in civil aviation applications to eliminate multiple (country-specific) regulatory requirements for the U.S. aviation industry.

7.5.5. National Highway Traffic Safety Administration (NHTSA)

The National Highway Traffic Safety Administration (NHTSA) within the Department of Transportation regulates the safety of motor vehicles and related equipment and issues *Federal Motor Vehicle Safety Standards* (FMVSS) [157]. NHTSA also regulates fuel economy in light-duty vehicles and medium- and heavy-duty trucks through the Corporate Average Fuel Economy (CAFE) program.

7.5.6. Federal Motor Carrier Safety Administration (FMCSA)

The Federal Motor Carrier Safety Administration (FMCSA) within the Department of Transportation is the lead federal agency responsible for regulating and providing safety oversight of commercial motor vehicles. The FMCSA regulates the operation of vehicles used in construction that operate on roadways and meet the Federal definition of a commercial motor vehicle [179].

7.5.7. Centers for Disease Control (CDC)

Within the CDC, the National Institute for Occupational Safety and Health (NIOSH) is actively engaged in research on health and safety aspects of AM to identify knowledge gaps, advance understanding in the field, and best apply these developments in order to protect American workers. NIOSH performs both laboratory and field studies to determine the hazards and potential for worker exposures when using emerging technologies such as AM and issues guidelines for safe use of the technology [183; 184].

As an example, NIOSH has studied emissions from the use of recycled material in AM [185–191]. Laboratory studies have indicated that fused filament fabrication desktop printers emit respiratory irritants and that filament material and coloration significantly affect volatile organic compound emission rates [192–194]. The NIOSH Nanotechnology and Advanced Materials Field Studies Team conducts fieldwork to assess exposure under real-world conditions at AM manufacturing sites. A third component of NIOSH activities is comprehensive toxicological assessments of respiratory and systemic toxicity resulting from inhalation of emissions released during polymer-based 3DP, which have indicated potential for transient respiratory effects both in vitro and in vivo.

7.5.8. National Aeronautics and Space Administration (NASA)

As the U.S. civilian space agency, NASA has a variety of interests concerning AM. First and foremost, NASA develops and issues the standard for the design and building certification qualifications of AM hardware for spaceflight (NASA-STD-6030 [195]). The standard concerns end-user specifications of parts critical for safety and effectiveness. NASA has adopted a risk-based scheme with three classes:

7. Class A—High Consequence of Failure: Failure of the part can lead to mission failure or loss of life.
8. Class B—Intermediate Consequence of Failure: Failure of the part is not catastrophic, but can have a major programmatic impact.
9. Class C—Negligible Consequence of Failure: Failure of the part does not lead to hazardous conditions, eliminate critical redundancy, or threaten the safety and welfare of crew members.

The NASA standard governs the ever-increasing number of AM parts used in vendor-provided spacecraft components like rocket engines, lander engines, and rover parts. In addition to defining its own standards, NASA interacts with industry through its membership in America Makes and through its participation in ASTM and SAE standards committees and working groups. NASA also conducts and supports AM R&D on in-space manufacturing and off-world construction, including in partnership with America Makes (NASA interview, 2/15/2022).

7.5.9. Department of Energy (DOE)

In the area of AM, DOE does not have a regulatory role, and although it does provide advice and technical information relevant to standards and guidelines, it does not directly participate in the development or issuance of standards. Its primary means of interaction with industry is through America Makes as well as support for AM R&D through cooperative research and development agreements with industry partners. Several of DOE's National Laboratories include AM in their research portfolios, including ORNL, Lawrence Livermore National Laboratory (LLNL), and Sandia National Laboratories. In particular, ORNL manages the Manufacturing Demonstration Facility [196], a user facility where industry and academic researchers have access to advanced, large-scale AM technology (DOE interview, 1/24/2022).

7.5.10. National Science Foundation (NSF)

NSF has no regulatory authority, but it does interact with industry through its participation in America Makes and the NEXT Manufacturing Center Consortium. NSF supports foundational, use-inspired, and translational research on AM technology in academic settings through its standard funding programs. In addition, NSF also has capacity through its SBIR/STTR programs, its I-CORPS Hubs, and the Regional Innovation Engines Program, to help new AM technologies transition into commercial application (NSF interview, 1/21/2022).

7.5.11. Nuclear Regulatory Commission (NRC)

NRC is responsible for licensing and regulating the Nation's civilian use of radioactive materials. The agency's focus in AM standards development is currently on assessing gaps from a technical and regulatory perspective, although the agency's role in standards development also covers additional activities. As with other regulatory agencies, it is primarily concerned with the safety and quality of components, regardless of manufacturing technology, rather than overseeing the manufacturing process.

NRC actively participates in SDO activities with ASME as well as other SDOs, such as ASTM and AWS, to identify potential safety concerns so that they can be addressed during standards development. The agency engages with ASTM on AM standards and is a formal participant in ASME code activities for advanced manufacturing technologies, which include AM: (1) the ASME BPTCS/BNCS Special Committee on Use of Additive Manufacturing, a working group developing guidelines for AM applications for pressure-retaining components; (2) the development of a code case for laser powder bed fusion of 316L steel; and (3) a task group developing code elements for AM in high-temperature applications. NRC's participation facilitates more efficient review and potential approval of the ASME Code and associated Code Cases for use in nuclear applications.

In addition, NRC visits and audits vendors to assure the quality and specifications of parts, including those produced using AM, and participates in public forums to address technical and regulatory issues and solicit feedback (NRC interview, 2/7/2022).

7.5.12. Environmental Protection Agency (EPA)

The mission of the EPA is to protect human health and the environment. In addition to its regulatory responsibilities, it also conducts research to understand potential pollution scenarios and health effects, largely driven by requests from regulators. To the degree that EPA's research and enforcement activities intersect with AM, they are concerned with the potential health and environmental effects of materials and processes (such as raw materials, emissions, waste, etc.). The agency's interaction with industry is largely limited to requests about the chemical composition of materials. As the use of AM expands in novel directions, it can result in situations requiring manufacturers to notify the EPA as required by Significant New Use Rules (EPA interview, 1/18/2022).

7.5.13. Consumer Products Safety Commission (CPSC)

The CPSC's mission is to reduce the unreasonable risk of injuries and deaths associated with consumer products [166]. It has the authority to issue and enforce mandatory standards and can ban consumer products when appropriate. It also conducts research on potential product hazards, works with SDOs and industry to develop voluntary standards, and informs and educates consumers directly concerning product safety [166]. In the area of AM, the CPSC has reached out to manufacturers and SDOs to develop appropriate standards for desktop 3D printing equipment and materials as well as presenting its work on AM at conferences [87]. In addition, it has worked with a number of other Federal agencies, including NIOSH, NIST, FDA, DoD, and EPA, to better understand the potential hazards associated with AM [87]. Its research focuses on understanding the material science, base materials, and manufacturing processes associated with AM and how they affect durability and potential chemical exposure over the life cycle of an AM product [87].

7.5.14. Bureau of Industry and Security (BIS)

BIS's mission is to advance U.S. national security, foreign policy, and economic objectives by ensuring an effective export control and treaty compliance system, and by promoting continued U.S. strategic technology leadership. BIS implements and enforces export controls on dual-use items (items that have commercial uses, but also may have military applications), including AM equipment, as well as some less lethal munitions items. BIS continually assesses critical and emerging technologies like AM for appropriate control. BIS's enforcement role covers illegal exports of AM equipment and precursors and of technical drawings and blueprints. BIS works closely with attorneys at the Department of Justice and other law enforcement partners. Violations of the Export Administration Regulations, 15 C.F.R. Parts 730-774 (EAR) [197] may be subject to both criminal and administrative penalties.

7.5.15. Department of Veterans Affairs (VA)

As part of its mission to provide benefits and services to U.S. veterans, the VA's Veterans Health Administration (VHA) is the largest integrated health care network in the United States. In this capacity, VA has over a decade of experience utilizing AM technologies to restore the health of veterans and has taken an active role in advancing AM capabilities in the health care space.

VHA established the Office of Advanced Manufacturing (OAM) to guide the utilization of advanced manufacturing technologies, like 3D printing, in health care applications. OAM is building digital and physical infrastructure to ensure veterans and all Americans have access to innovative products and services, including AM. In addition, VA has developed and implemented a quality management system compliant with 21 C.F.R. Part 820 [198] and has registered two VA hospitals with the FDA as medical device manufacturers.

Among the AM developments pioneered by VA, the agency obtained compassionate use authorization for a patient-matched ear stent, has listed and is manufacturing an FDA class I 510(k) exempt medical device that improves safety of home oxygen, and received FDA class II 510(k) clearance for a the VHA OroMaxilloFacial Advanced Surgical Planning system in August 2022. VHA received its second FDA class II 510(k) clearance for the radiation therapy bolus in November 2022. VHA is developing additional products including anatomical models supporting education and the planning of medical procedures, multiple dental devices and systems, a hearing stent, and AM production processes for prosthetics. VA also hosts the Biofabrication Community of Science, which brings together diverse stakeholders across government and industry to advance the development and clinical deployment of biofabricated solutions, like a vascularized bone graft product that is currently in development.

VA has engaged in collaborations with multiple industry partners to develop AM technologies for veterans and all Americans. These include partnerships with GE Healthcare, Stratasys, Formlabs, 3D Systems, Desktop Metal, and Advanced Solutions Life Sciences. During the COVID-19 pandemic, VA partnered with America Makes, the Barnes Group, and 3D Systems to support the development and manufacture of AM personal protective equipment. In addition, VA has established VA Ventures as a government-based incubator for the development, testing, and clinical deployment of AM health care products. VA Ventures invites government, academic, and private partners to co-locate and share resources to speed AM device innovations that will benefit American healthcare.

Lastly, VHA is working closely with the VA Office of Information Technology to establish pathways to create a safe and secured digital workflow for AM in healthcare. This includes the vetting of 3D printers and software for security risks and the creation of a secure cloud architecture to move patient data, images, 3D blueprints, and reports across the health enterprise.

7.6. Interagency Activities

7.6.1. Informal Interagency Activities

Informal interagency activities are those in which no formal agreement exists between two or more agencies, but agency representatives share information or cooperate on developing policy. Informal activities typically stem from relationships formed between individuals at conferences, through working groups, or other interpersonal interactions. Several agency collaborations center on discussing best practices, shared problems, and aspects of AM's potential to disrupt existing regulations. Other agency interactions center on discussing AM in applications that overlap between agencies, such as AM for aerospace applications between DoD and NASA (NASA interview, 2/15/2022). The informal nature of these activities results in little or no direct documentation, although they can plant the seeds for subsequent formal outcomes.

7.6.2. Formal Interagency Activities

Formal interagency activities generally consist of participating in working groups, co-hosting workshops, or sharing resources or funding. In addition, several AM research collaborations include multiple agencies.

7.6.2.1. Interagency Writing Team on Performance and Reliability of Advanced Manufactured Parts (IWT-PRAM)

The IWT-PRAM is an interagency group established in 2021 under the auspices of the National Science and Technology Council (NSTC) Subcommittee on Advanced Manufacturing and NSTC Subcommittee on the Materials Genome Initiative. Its goal is to ensure that critical parts and components used in sensitive and high reliability applications fabricated using AM work as intended. Application areas include aerospace, aviation, transportation, and medical devices. Agencies represented on the IWT-PRAM include NIST, DoD (Air Force Research Laboratory and Office of Naval Research), NASA, FDA, DOE, NSF, FAA, DOS, and EPA. The interagency group issued their final report in September 2022, titled *The Strategy for American Leadership in High-Consequence Additive Manufacturing* [10].

7.6.2.2. 4D Bio^3

4D Bio^3 is a biomedical research initiative that aims to adapt biotechnology for warfighter benefit. The program is housed at the Uniformed Services University of the Health Sciences and aims to assist DoD and other Federal agencies—including FDA, NIST, VA, and the National Institutes of Health (NIH) National Heart Lung and Blood Institute—in biomedical research [199; 200] (FDA interview, 1/18/2022).

7.6.2.3. Materials Genome Initiative

The Materials Genome Initiative (MGI) is a multi-agency effort (DoD, OSTP, DOS, NSF, ARPA-E, DOE, NIST, National Nanotechnology Initiative, USGS, NNSA, NASA, FDA, U.S. Army, U.S. Air Force, U.S. Navy, and NITRD) aimed at expediting the development and deployment of advanced materials using advanced computational materials methods, including AM [201].

7.6.2.4. Joint Metal Additive Database Definition (JMADD)

DoD, FAA, NASA, and DOE are working with Auburn University, Wichita State University, Boeing, and other participating organizations to develop a publicly available, statistically substantiated material property database and corresponding material and process specifications for laser powder bed fusion of titanium alloy. This collaboration operates under America Makes and also includes several other universities and private sector companies [202] (DoD interview, 1/24/2022).

7.6.2.5. Formal Collaborations at NRC

NRC periodically meets with DOE’s advanced manufacturing group and has an agreement with NIST through which NRC provides funding for technical consultation and training in the arena of AM. NRC also periodically meets with other groups, such as the Electric Power Research Institute, to discuss research activities associated with AM. In addition., NRC interacts with agencies and other groups by holding and participating in information-sharing and information-gathering workshops.

7.6.2.6. Joint Incentive Fund Between VA and DoD

VHA’s Office of Healthcare Innovation and Learning and DoD’s Walter Reed Medical Hospital received support from the Joint Incentive Fund aimed at building sustainable AM capabilities through (1) adoption of a single, inter-governmental AM quality system which meets or exceeds FDA and ISO criteria for 3D printed parts, thus decreasing potential patient safety issues; (2) increased 3DP capabilities and capacity at two medical manufacturing 3D printing facilities (one DoD and one VA) to expand the number of patients who receive 3D printed healthcare solutions; (3) providing cross-agency AM services coverage when needed to reduced risks of planned and unplanned AM manufacturing downtimes and to assist in transition of care for wounded warriors from DoD to VA; and (4) development of an inter-agency training and workforce development program for AM health care jobs that will improve access and quality of care for active duty service members and veterans and improve VA/DoD hiring potential for a technical specialty with a workforce scarcity. This training will increase access to digital technology and 3DP in multiple locations throughout the DoD and VA networks and also allow VA and DoD, in collaboration with FDA, to establish best practices for 3D printing in hospitals.

7.6.2.7. Memorandum of Understanding: Streamlining Emerging Technology Medical Device Development Through Regulatory Tools

In September 2022, FDA and VHA issued a memorandum of understanding [203] to mutually collaborate on advancements in regulatory science to support the translation of novel AM products and technologies into clinical care. This collaboration focuses on the creation and dissemination of regulatory science tools that will provide “off the shelf” testing and evaluation strategies that innovators using emerging technologies can use in their medical device regulatory strategies.

7.7. Regulations, Guidelines, Mandatory Standards, Voluntary Standards, and Other Policies Implemented by Federal Agencies

The diversity of materials and processes falling under AM means that no single Federal agency has oversight over the technology as a whole. Rather, agency regulations and standards govern the products, by-products, or conditions resulting from AM rather than the process itself. Regulations, guidelines, mandatory standards, voluntary standards, and other policies implemented by Federal agencies affecting AM are constrained by the missions and authorities of each individual agency and are addressed in *section 7.4 Federal Agencies with Jurisdiction* of this chapter.

7.8. Guidelines, Mandatory Standards, Voluntary Standards, and Other Policies Implemented by Industry-Based Bodies

Guidelines, mandatory standards, voluntary standards, and other policies implemented by industry-based bodies for AM as a whole are addressed in *Section 7.3.2.2 AM Standards Bodies and Current State of Industry-Based Standards (Cross-Sectoral)* of this chapter. Because different industries apply different AM processes for different uses, numerous standards, guidelines, and policies governing specific types of products apply to the use of AM technology; industry-specific standards and SDOs are covered in the appropriate sub-sections of *Sections 7.3.3* through *7.3.10* of this chapter.

7.9. Federal Government Resources for Small Businesses to Evaluate the Use of Additive Manufacturing

The Federal Government has various mechanisms that may help support small businesses to develop, qualify, and adopt AM technologies. The following discussion is a non-exhaustive list of Federal resources that could support small businesses in evaluating AM technologies.

7.9.1. Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR)

The Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) programs are mechanisms through which small businesses can receive Federal funding to start or grow an enterprise that both stimulates technological innovation and helps meet Federal needs. Eleven Federal departments and agencies participate in the SBIR program, and five also participate in STTR, which differs from SBIR in requiring small businesses to formally partner with a research institution [204]. A non-comprehensive search of FY2020 SBIR/STTR data using the search term "additive manufacturing" resulted in 195 awards totaling $74 million in funds. Awards with abstracts mentioning "additive manufacturing" were funded by DOC, DoD, DOE, HHS, DOT, NASA, and NSF. DoD funded 124 of the 195 awards, followed by NASA and DOE, which funded 31 and 28 awards, respectively [205].

7.9.2. Manufacturing USA Institutes

Manufacturing USA is a national network composed of 16 institutes that was "created to secure U.S. global leadership in advanced manufacturing through large-scale public-private collaboration on technology, supply chain and workforce development" [206]. Each institute focuses on specific technology areas [207]. America Makes is solely focused on AM technologies, although a number of other institutes conduct activities relevant to AM and provide AM-related resources available to small businesses through various mechanisms.

7.9.2.1. America Makes

As the largest U.S. PPP focused on AM, America Makes provides a wide range of resources to businesses of all sizes to support industrial AM applications. America Makes supports projects that advance AM design, process improvements, materials, and value chains—work that ultimately may help consumers and small businesses evaluate the use of AM technologies and applications [208].

7.9.2.2. BioFabUSA

BioFabUSA's mission is to "integrate innovative cell and tissue cultures with advances in biofabrication, automation, robotics, and analytical technologies to create disruptive R&D tools and FDA-compliant volume manufacturing processes." BioFabUSA conducts education and workforce training activities, technology development, and provides regulatory consulting services for members, which include tissue-engineering and regenerative medicine start-up companies developing tissue bioprinting technologies [209].

7.9.2.3. Institute for Advanced Composites Manufacturing Innovation (IACMI)

IACMI's mission is to "accelerate the development and adoption of innovative composites manufacturing technologies" [210]. The institute was initially supported by DOE through

Manufacturing USA and has collaborated with partners such as ORNL and industry groups on research efforts that use AM technologies for manufacture of composites [211].

7.9.2.4. LIFT

LIFT is operated by the American Lightweight Materials Manufacturing Innovation Institute (ALMMII) and focuses on advancing manufacturing within the mobility sector. As a PPP formed by DoD, industry partners, and academia, LIFT's membership includes small- and medium-sized companies. LIFT's goals are to accelerate technology transfer from industry to DoD while advancing U.S. manufacturing as a whole. The institute's activities include technology development, workforce training, and government contracting [212]. LIFT supports a wide range of technologies including wire arc AM and cold spray AM [213].

7.9.2.5. MxD (Manufacturing x Digital)

As a DoD-partnered PPP, MxD's mission is to "equip U.S. factories with the digital tools, cybersecurity, and workforce expertise" to advance U.S. manufacturing [214]. MxD's activities include workforce development, digital engineering, and supply chain optimization. Their facilities serve as a digital manufacturing testbed to help demonstrate digitization technologies for small- and medium-sized manufacturers and allow them to understand how they could integrate these capabilities into their own factories [214]. MxD has received funding from the FDA to research medical AM applications [215].

7.9.2.6. National Institute for Innovation in Manufacturing Biopharmaceuticals (NIIMBL)

NIIMBL is a PPP funded through a cooperative agreement with NIST. It focuses on advancing manufacturing capabilities for biopharmaceutical products, both existing and new, including AM. In addition, NIIMBL aims to develop a well-trained, robust biopharmaceutical manufacturing workforce and supports the development of standards for advanced manufacturing capabilities [216].

7.9.3. Manufacturing Extension Partnership (MEP)

The NIST Manufacturing Extension Partnership (MEP) is a PPP that provides a wide range of resources for small- and medium-sized U.S. manufacturers through a national network of technical and business experts that can support company growth, business improvement, and risk mitigation efforts [217]. MEP's "Advanced Manufacturing Technology Services/Industry 4.0" business improvement service helps companies establish adoption strategies, conduct project scoping, and identify and manage suppliers; it lists AM as a MEP area of expertise [218]. In addition, MEP plays a key role in identifying supply chain gaps where Federal agencies must rely on foreign sources for critical items. Connecting opportunities to deploy AM in domestic firms can potentially reduce cost differentials and enable more domestic manufacturing firms to supply government requirements.

7.9.4. Additive Manufacturing Materials Database (AMMD)

NIST maintains the Additive Manufacturing Materials Database (AMMD) through its Configurable Data Curation system (CDCS), which provides a forum for data sharing and open data access for the AM community [219]. Detailed data on AM feedstock materials, machines, part designs, and part testing are available for public use [220].

7.9.5. Government-Supported User Facilities

Three DOE National Labs—ORNL, LLNL, and Sandia National Laboratories—offer state-of-the-art AM capabilities to private partners through a range of partnership mechanisms, including technical support agreements, cooperative research and development agreements, and user agreements [221].

ORNL's MDF conducts early stage R&D activities with the goal of improving the efficiency and productivity of U.S. manufacturers. Their AM capabilities include large-scale metal AM systems, metrology and characterization tools, and modeling and simulation techniques for non-destructive part validation and verification [222].

LLNL's Advanced Manufacturing Laboratory (AML) similarly offers sophisticated technological resources to industry partners. Their capabilities include high-performance computing resources that can be used for topological optimization of AM parts or process modeling of AM systems and synthesis and characterization capabilities for development of novel materials [223].

Sandia National Laboratories conducts AM R&D activities focused on analysis-driven design, materials reliability, and multi-material AM [50]. Sandia has a history of partnering with industry and provides an inquiry form for prospective collaborators to contact them regarding potential AM-related partnerships [224].

7.10. Marketplace and Supply Chain

7.10.1. Risks Posed to the Marketplace and Supply Chain

The AM supply chain consists of two parts: AM equipment and AM materials (which consist of both raw material commodities and AM-ready feedstock). Since AM is a family of manufacturing processes employed very differently in many economic sectors, its impact on markets and supply chains of final products depends on the particular circumstances of its application.

7.10.2. AM Systems Supply Chain

Wohlers Associates [50] divides AM equipment into industrial AM systems and "desktop" printers. No outstanding vulnerabilities to the U.S. supply chain for AM systems were identified through reviews of literature or interviews with technical experts. One Federal agency interviewee mentioned that many state-of-the-art metal AM systems are supplied by manufacturers headquartered in Europe (FDA interview, 1/18/2022); however, they did not conclude that this general trend posed a major risk to domestic supply chains. AM industry tradeshows and other AM exhibitions and meetings are useful in tracking developments in AM systems and materials. Recent advancements highlighted at an international tradeshow for AM and industrial 3D printing include advancements in AM process development for existing and new processes (e.g., directed energy deposition, DED) and in materials for AM including ceramics, polymers and polymer-based composites; an increase in well-established manufacturing companies entering the AM system marketplace; and examples of the impact AM is having on other manufacturing technologies (e.g., advanced molds for casting) [225].

7.10.2.1. Industrial AM Systems

Industrial AM systems have experienced significant growth in the last decade [50]. In 2012, there were 33 manufacturers, whereas by 2020, the number had grown to 228. Of those 228 manufacturers, 37 sold 100 machines or more in 2020. The United States is home to more of these manufacturers (47) than any other country, followed by Germany (27) and China (25). Stratasys, 3D Systems, and Markforged lead the industrial AM market, capturing 13.5, 9.6, and 7.7 % of market share, respectively. In 2020, manufacturers headquartered in the United States captured 35 % of unit sales, followed by Europe (27.1 %) and the Asia/Pacific region (19.1 %). With an average price of $501,844 in 2020, metal AM systems are significantly more expensive than polymer AM systems, which had an average price of $54,350. In 2020, 8.5 times as many polymer systems were sold than metal systems.

7.10.2.2. Desktop AM Systems

The desktop AM market has also experienced substantial growth in recent years, with over 700,000 units sold in 2020 at a price typically less than $5,000. Wohlers Associates [50] notes that identifying manufacturers and tracking sales of desktop units is more difficult than industrial AM systems due to the large number of small companies selling these machines and the wide availability of desktop components and assemblies from online vendors. Wohlers Associates [50] reports evidence of a significant increase in Chinese manufacturers supplying desktop printers to the United States and Europe in 2020, possibly in response to COVID-19 supply chain disruptions.

7.10.3. AM Materials Supply Chain

Materials used in AM processes include polymers, metals, ceramics, and various composites that may come in the form of filaments, wires, pellets, sheets, liquids or powders. Fundamentally, supply chain risks for materials result from insufficient availability to support manufacturing, which can arise due to a shortage of either raw materials or AM-ready feedstock. The supply chain for each of the different materials used in AM is distinct and depends on the specific AM process and post-processing as well as the desired properties of the final product (for example, strength, rigidity, or biocompatibility).

Many AM equipment providers are also suppliers of feedstock, with some manufacturers blocking or discouraging the use of materials provided by other suppliers (for example, by voiding equipment warranties or by having operating software reject non-OEM materials). In contrast, some producers of AM systems have historically favored an open-architecture model compatible with materials from third-party suppliers [226]. Overall, as AM becomes more common and is increasingly used to produce final parts at production scale, equipment manufacturers are generally moving towards greater acceptance of third-party material suppliers [50].

On the whole, the raw materials of AM—particularly metals and polymers, which are the most widely used materials for commercial applications—are common commodities and review of publicly available literature, market studies, and Federal agency interviews did not raise immediate pressing concerns related to supply chains for raw materials needed to produce AM feedstock [227]. As such, AM is no more vulnerable to raw material supply chain risks than alternative manufacturing processes. This does not mean that AM is invulnerable to risks in the supply chains of raw materials, only that its vulnerabilities are comparable to those of the other manufacturing sectors.

Numerous Federal agencies maintain lists of critical commodities and their potential supply chain vulnerabilities, including materials used in AM. The Department of the Interior [228] maintains a list of critical minerals that includes a number of those used in AM, such as titanium and vanadium. In addition, the Defense Logistics Agency (DLA) [229] maintains a list of materials that are essential for defense goods [230] as part of its responsibility to maintain the National Defense Stockpile (NDS), including raw materials used in AM production of parts in the aerospace industry and other sectors related to national security. The NSTC has also identified a potential risk to domestic supply chains for titanium and titanium alloys used to produce metal powders required for high-criticality components in the defense and aerospace industries made using AM [231]. Lastly, DOE, DoD, and DOS recently signed a memorandum of agreement formalizing a partnership to acquire and recycle selected materials for clean energy technologies, including metals used to produce AM parts in the sector [232].

In contrast to the supply of raw AM material, the primary concern around AM feedstock is a lack of sufficient production capacity. This concern is expected to be exacerbated as AM is increasingly used to support manufacturing of high volume parts, for example, in the automotive sector [233].

7.10.3.1. Polymers

The global market for 3DP plastics was valued at $520.5 million in 2019, with a projected compound annual growth rate of 23.7 % from 2020 to 2027 [234]. For comparison, the global market for plastics as a whole was valued at $579.7 billion in 2020 [234]. Although the polymer AM market is likely to experience significant growth (and associated growth pains) in the foreseeable future, no ongoing or imminent risks unique to the U.S. polymer AM material supply chain were identified in the course of preparing this chapter, which reflects the robustness of the domestic plastics industry.

Polymer feedstock used in AM is significantly more expensive (4 to 100 times) than equivalent materials intended for conventional manufacturing methods like injection molding. Desktop printer feedstock is available for $20 per kilogram, while filament, powder, and liquid used in high-quality industrial AM machines can cost $40 to $250 per kilogram [50]. The higher cost, which can make up a significant proportion of the cost of a finished AM part, reflects the additional processing needed to produce AM-compatible feedstock and the relatively small size of the AM industry [235]. As AM markets grow, economies of scale are expected to lower feedstock costs.

Advances in polymer chemistry will continue to expand the range of polymers available for AM. For example, in response to supply chain disruptions created by the COVID-19 crisis, suppliers developed or repurposed biocompatible materials for AM as a stopgap measure to replenish dwindling supplies of test kit swabs, mechanical components for medical equipment, and personal protective equipment [5; 6]. In addition, developers are working to create AM materials with reduced opacity, increased corrosion resistance, or other desirable properties for specialized applications.

7.10.3.2. Metals

Feedstocks for metal AM processes come in various forms (for example, powder, wire, sheet) depending on the specific process and system. The most commonly used form is powder for laser powder bed fusion and directed energy deposition (DED), and the second most commonly used form is wire for DED. The characteristics of the feedstock—i.e., form, structure, and composition—impact the ability to additively manufacture an item and the quality of the item.

An increasing number of metals are compatible with AM processes, including tool steels, stainless steels, nickel, aluminum, titanium, and titanium alloys, although the current variety of alloys that has been successfully employed in AM is much lower than the full range used in conventional manufacturing [10]. Metal powder feedstock for AM is optimally composed of more uniformly-sized, spherical particles than conventional industrial powder metallurgy processes produce, and metal AM powder prices depend on the order volume, particle size distribution, and the precursor materials, among other factors. Wohlers Associates [50] estimates that AM powder prices range from $20 to $250 per kilogram. In contrast, wire feedstock is typically 30 % to 73 % the cost of powder of the same material [236; 237].

7.11. Marketplace

The changes in a product’s supply chain and market due to the use of AM will depend on the degree to which AM in integrated with, or replaces, other manufacturing processes used to make the product. Because AM is used very differently in different economic sectors, its impact on markets and supply chains is sector-specific. The discussion here focuses on general considerations of how AM can alter a market landscape rather than prognosticating its effect on specific markets.

Although AM has the potential to alter markets of products made using other manufacturing processes, it is not a universally disruptive technology: other manufacturing processes may be better choices to serve a given market for a particular product or under particular circumstances. AM’s production advantages include [238]:

10. not requiring retooling to change the item being produced in response to sharp changes in demand or desired customization;

11. being well suited to producing geometrically complex items with per-unit cost of production independent of the item's complexity (although additional complexity may require additional validation and quality control); and

12. producing single parts to replace assemblies composed of many parts, thereby reducing the number of processes, suppliers, and steps in production.

However, AM also has a number of disadvantages:

13. AM material costs are typically higher than other manufacturing technologies because materials require additional processing for AM use;

14. AM production rates per item are generally slower than alternative manufacturing processes, leading to higher overhead costs; and

15. Because the cost of producing an item using AM does not decrease with greater quantity, AM does not benefit from economies of scale.

In summary, with respect to production costs, AM has an advantage over other manufacturing technologies in the production of small quantities of complex objects, but conventional manufacturing technologies are likely to be more cost effective for large quantities (Fig. 3). The exact cross-over in advantage depends on the specific material, geometric complexity, and production volume of the item.

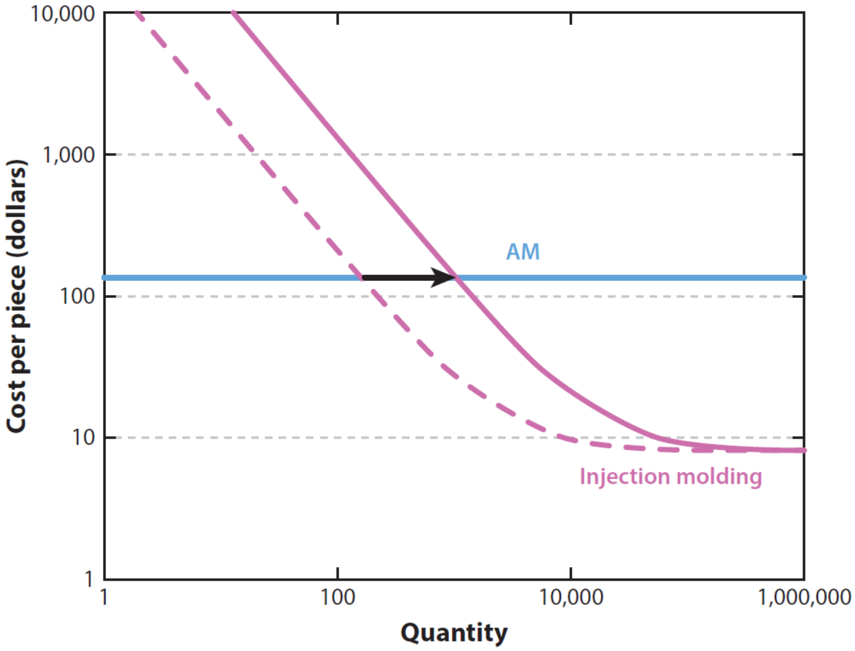


Figure 3. Cost to Produce an Item as a Function of Quantity of Items to be Produced.

In **Figure 3**, AM (solid blue line) has constant cost per item, regardless of quantity. Injection molding (dashed pink line), an alternative manufacturing process, has diminishing cost per item with increased quantity. Cost per item produced using injection molding increases with complexity (solid pink line). Where the blue line is below the pink line, production using AM is more cost effective than injection molding. In general, AM has the advantage in production cost for small quantities of items with complex geometries. [239].

Although AM generally has a slower production rate for a given item than an alternative manufacturing technology, AM's flexibility can shorten supply chains to a degree that makes up for its greater overhead production cost. In particular, in industries where the timing and volume of demand for a product is volatile and hard to predict, firms typically maintain an inventory to be ready to respond to customer orders quickly and prevent losing business to competitors. When demand exceeds what a firm can deliver, non-AM machinery must be retooled to supply the demand. In contrast, AM equipment can be redirected much more quickly and cheaply by uploading a new 3D digital model (and changing material, if needed). When the costs of maintaining inventory are lower than the excess production costs incurred by AM, conventional manufacturing has the advantage, but when quantities are small and demand is volatile, AM can be more cost effective than maintaining inventory [238].

Similar to inventory, AM can also displace the costs of transportation and logistics in circumstances where production of items closer to their point of use is cheaper than the cost of distant production plus the cost of delivery. AM generally requires a smaller amount of labor (although more highly skilled) than conventional mass production [226]. This reduces the pressure to locate production facilities where labor is cheap (i.e., offshoring), thereby allowing the placement of fabrication facilities closer to the point of final delivery. Both UPS and Amazon have already begun to explore the possibilities of integrating AM to reduce transport and logistics costs: UPS has partnered with CloudDDM to co-locate AM fabrication facilities with UPS shipping hubs and Amazon has applied for a patent to put 3D printers in delivery trucks [226]. As was the case for reducing inventory costs, the production cost per item made using AM may be higher than the same item produced using an alternative manufacturing process, but by producing it closer to the point of use, the savings incurred from reduced transport may outweigh the additional production expense.

A dramatic example of AM's potential impact on markets and supply chains was observed in its use to respond to the sharp increase in demand for personal protective and other medical equipment (for example, nasal swabs) during the early months of the COVID-19 pandemic [6]. As need for these critical items skyrocketed in the spring of 2020 and conventional manufacturers were unable to meet demand, numerous firms with AM capacity rapidly redirected their equipment. A PPP between America Makes, FDA, NIH, and VHA that was established in March 2020 posted digital design files on a public NIH database. FDA worked to expedite approvals for posted designs and VHA tested posted items. This recent history highlights how the flexibility of AM allowed producers new to an item or sector to meet a sudden surge in demand rapidly and effectively. In the wake of the COVID-19 pandemic, the PPP including VA, FDA, NIH, and America Makes, in cooperation with OSTP, is looking into digital stockpiling—i.e., a framework in which digital AM workflows would be proactively designed and ready for rapid implementation to make critical health care products at distributed manufacturing facilities in times of need or crisis.

7.11.1. Intellectual Property Issues and Considerations for AM

Characteristics of AM that are highly advantageous to designers, manufacturers, and end users—flexibility, customization, and ease of access—present challenges when trying to secure and enforce IP rights for AM software, physical products, and processes. Nevertheless, IP protections not only help safeguard but can also facilitate creation of legitimate marketplaces for AM technologies and products.

The accessibility and affordability of 3D printers and the relative ease with which some products can be copied and shared as digital files can lead to cases of IP infringement and other violations that are difficult to detect or deter. In addition, counterfeiters can use AM to print unauthorized copies of trademarked goods or patent-protected items. Companies may need to strengthen their cybersecurity infrastructure and practices to protect digital design files to avoid theft, illegal copying, and sabotage.

7.11.1.1. Options for Protecting AM IP

Patents

A patent issued by the United States Patent and Trademark Office (USPTO) grants the patent holder the right to exclude others from making, using, offering for sale, or selling the invention in the United States or importing the invention into the United States for a limited period of time.

Two types of patent are relevant to AM: utility patents, which cover a "new and useful process, machine, manufacture, or composition of matter, or a new and useful improvement thereof," and design patents, which cover "any new, original and ornamental design for an article of manufacture" [240]. The number of patent applications for inventions involving AM has grown significantly in recent years: The USPTO issued 1,861 AM-related patent applications in 2020, compared to 294 in 2012 [50].

Holders of AM-related patents include AM system manufacturers seeking to protect technological innovations and improvements and companies seeking to protect products and processes enabled by AM. In 2020, the greatest number of AM-related patents were issued for AM system hardware (24 %), followed by medical/dental applications (15 %), consumer products/electronics (13 %), industrial/business machines (12 %), AM software (10 %), and aerospace (9 %) [50].

Although patent law affords a patent holder the right to exclude others from using a patented invention, the concept of "permissible repair" means that users may acquire or make replacement parts for unpatented components of multi-component patented objects for the purposes of repairing the object without violating the object's patent (as long as the component part being replaced is not itself patented and barring additional contractual restrictions imposed by the patent holder that limit the end user's rights) [241; 242]. Although there remains a gray area between "repair" (permitted) and "reconstruction" (not permitted) [243], AM technology may give consumers the ability to fix items that would ordinarily require regular replacement or servicing by the manufacturer. The increased accessibility of at-home consumer repair enabled by AM technologies could extend the life of these products beyond the manufacturer's initial projections, posing a risk to their business models.

There is limited precedent in the area of AM IP, including patent law, and numerous questions are not yet settled by case law. Legal scholars have drawn analogies to digital media case law to provide frameworks for how these questions could be addressed and to recommend best practices for designers, manufacturers, and suppliers seeking to protect their IP and better understand their legal responsibilities related to the acquisition, transfer, and use of AM IP.

Trade secret law

Trade secrets are protected by both State and Federal law. State laws are primarily based on the Uniform Trade Secrets Act (USTA), adopted in 1979 and amended in 1985 [244]. At the Federal level, a civil cause of action was added in 2016 by the Defend Trade Secrets Act [245], codified within *the Economic Espionage Act (EEA) [244]. Specific trade secret definitions vary among statutes, but generally, a trade secret is information that has either actual or potential independent economic value because it is not generally known, has value to others who cannot legitimately obtain the information, and is subject to reasonable efforts to maintain its secrecy [246]. Thus, trade secret law could protect AM process improvements, novel materials, or build files that are considered to be a company's proprietary information and that provide a competitive market advantage. As long as the definitional criteria are met, the trade secret will not expire. However, if any of the criteria fail, then the information is no longer a trade secret. Unlike patent protection, companies are not required to pre-emptively file or disclose information to qualify for trade secret protections.*

Copyright Law

Similar to trade secret protection, copyright protects works automatically if the relevant criteria are met (although registration is necessary to commence litigation for infringement of a U.S. work). Since AM makes it possible for anyone to copy a physical object, or transform two dimensional drawings into three dimensional objects, it could be used to facilitate copyright infringement. Copyright law can provide protection for original designs used in AM. It can also protect computer programs that are part of the AM process as well as creative elements of AM products.

The inherently digital nature of AM design files means that manufacturers of tangible AM objects can face the challenges experienced by the movie, music, and publishing industries from massive copying and sharing of digital files. Copyright law provides certain protections under the Digital Millennium Copyright Act (DMCA) relevant to AM, which could be used to remove or deter infringing online sharing of AM files [241].

Trademark law

Federal trademark law grants the holder of a trademark registration the exclusive right to use the registered mark in commerce in connection with the goods and services specified in the registration. Trademarks identify the source of goods and services and help prevent consumer confusion. "Trade dress" (the commercial look and feel of a product) is a type of trademark that protects non-functional features or characteristics of products when they are distinctive or identifiable as originating from a specific source or brand [247]. Trade dress protections offered by trademark or unfair competition laws could be used to help limit the sale of counterfeit 3D-printed items by manufacturers that willfully deceive customers by presenting their product as an authentically-sourced object [226].

7.12. Risks to the National Security, Including Economic Security, of the United States

7.12.1. Economic Threats

Three categories of economic threat have been identified for AM: (1) theft of technical data (legally protectable IP as well as information necessary to produce a part, such as process parameters), (2) sabotage of AM (manipulating specifications [shape or material composition] or the manufacturing process), and (3) manufacturing of illegal products (manufacturing an item without authorization or manufacturing a prohibited item) [248]. Each of these areas holds the potential to impose risks on the marketplace and supply chain for AM technologies, at present and in the future.

With respect to the theft of technical data, from an economic perspective, there is an increased potential for IP theft and for discovery of protected information (i.e., process parameters or other critical manufacturing information) through the reverse engineering of products. That is, products with easy to intuit designs can be manufactured using CAD systems and desktop 3D printers. Such a scenario may warrant terms of service restricting the reverse engineering of these products in a similar fashion to that which is already in place for software (DoD interview, 1/24/2022).

Vulnerability to sabotage of AM technologies was demonstrated by researchers in 2016, who hacked and altered electronic files of a drone design to modify its propellers in a way that was imperceptible to the human eye, but still caused the drone to crash [249]. The sensitivity of AM digital information—design files, build files, machine inspection files, etc.—is shared by all technologies connected to the Internet of Things [250].

Two areas in which AM can be prone to malicious actors concerns the material used to manufacture the products and the digital files used to make an item. To deflect these threats, at least one large company has developed a ledger using blockchain technology that can be used to verify the author of a digital file or the origin of the material used [251; 252]. It should be noted, however, that as with any blockchain technology, the information itself can still be exposed to cyber-attacks.

To help reduce the cybersecurity vulnerabilities of AM, the IWT-PRAM recommended (1) identifying and developing mitigation strategies for all steps unique to AM data streams and (2) encouraging efforts to enable data registration and communication across modes of data (e.g., CAD, simulation, and inspection) [10]. In particular, data provenance should be documented fully and assured. In addition, the AM community should collaborate with the cybersecurity community to identify solutions to challenges with data security.

Some Federal agencies are already implementing procedures to ensure that AM data are secure. For example, VHA is working closely with the VA Office of Information Technology to establish pathways to create a safe and secured digital workflow for AM in healthcare. This includes the vetting of 3D printers and software for security risks and the creation of a secure cloud architecture to move patient data, images, 3D blueprints, and reports across the enterprise.

7.12.2. Defense and Homeland Security Impacts and Risks

The use of AM will impact national defense and homeland security capabilities and will introduce some potential threats and risks. The use of AM in national defense has been demonstrated, and is being further developed to support deployed and expeditionary units, where AM is used for tooling, on-demand part repair, fabrication of parts to keep a system in operation, fabrication of parts to modify a system to make it more effective (for example, low-criticality fixtures like visor clips), and to fabricate entire systems that can provide needed capability on site (for example, unmanned aerial vehicles that can carry a camera) [253]. In addition, AM can be used to fabricate hard-to-get, obsolete parts utilizing organic manufacturing capabilities within DoD. DoD maintains these capabilities at depots, arsenals, and ammunition plants to replace or supplement commercial supplier capability and ensure part availability.

For deployed forces, AM provides unique capability to fabricate parts from a variety of materials in a deployable volume with available power sources—for example, an AM fabricator in a standard shipping container. These same features are advantageous for DoD's organic manufacturing components compared to the larger footprint and power generally needed to fabricate similar parts using conventional technologies.

Risks related to AM in the security and defense arenas are similar to those in the private sector: lack of availability of raw materials, lack of availability of AM-ready feedstock materials, lack of qualified processes and designs, and insufficiently secure cyber infrastructure to prevent corruption of digital files.

An additional risk arises when AM is combined with 3D scanning technologies to create a 3D digital design file that allows a scanned part to be made using AM. The ability to make a replacement for a broken part by U.S. forces is an important strength of AM technology, but it also gives enemy forces the ability to replicate U.S. parts using accessible technology [254]. For example, adversaries that capture or otherwise obtain complex warfighting technologies can use 3D scanning and AM to repair and replace parts as they break without access to OEM parts or large-scale manufacturing infrastructure (DoD interview, 1/24/2022). In such scenarios, products can no longer be effectively controlled or restricted at the point of sale [255]. Such capability is a risk for homeland security as well. For example, an untraceable unmanned aerial system capable of carrying surveillance equipment capable of compromising the security of a facility could be made using AM [254].

The opportunities and threats of AM for homeland security have been considered in the Homeland Security Advisory Council's *Final Report of the Emerging Technologies Subcommittee: 3-D Printing* [254]. Threats identified include the sabotage of AM parts, concealment of illicit objects within an AM part, manufacture of untraceable parts/products, supply chain exposure, and counterfeit part manufacture as well as the production of AM parts that enable spoofing of biometric protection measures (for example, using an AM fabricated structure to spoof fingerprint readers). The report contains three recommendations to mitigate potential deleterious impacts of AM on homeland security: (1) adopt technologies that establish traceability for AM parts and for all associated digital files; (2) develop and use tools to detect and identify harmful objects concealed by an AM structure, flaws introduced into AM parts, and AM components that contain explosive materials; and (3) reinforce cybersecurity measures to protect digital design data, 3D models, and manufacturing (build process) files that can be easily shared across networks with multiple users and systems.

7.12.3. Export Controls

Export controls are one of the tools the United States uses to mitigate risks inherent in the transfer of technology, equipment, or products to foreign end-users. Export controls include restrictions on the export of technology or know-how from the United States in addition to the export of physical goods. The primary non-nuclear U.S. export control regulations are the Export Administration Regulations (EAR) and the International Traffic in Arms Regulations (ITAR). The Commerce Control List (CCL), which is maintained as part of the EAR, consists of technology or know-how subject to the EAR [256]. CCL items are organized by export classification numbers (ECCNs). The United States Munitions List (USML) is maintained as part of and is subject to the ITAR [257]; it consists of items, services, and related technical data designated as defense articles or services [258].

Currently, the EAR regulates specific AM equipment that could be used to produce single turbine blades (ECCN 9B001) and CNC machine tools that also have one or more AM components (ECCN 2B001) [259]. Currently, AM equipment is not enumerated on the USML, while many AM design files directly related to defense articles are described in the associated technical data entries for those defense articles. The U.S. interagency, including the Department of State, DOE, DOC, and DoD, continue to monitor the technology frontier to identify and evaluate new and nascent capabilities and assess whether and how current national and multilateral export controls should be updated, based on U.S. national security and foreign policy interests and priorities.

7.13. Emerging Risks to and Long-Term Trends in the Marketplace and Supply Chain of Additive Manufacturing

The future of AM is based on its ability to fabricate a wide variety of objects with little or no retooling. Although this characteristic is not unique to AM as a manufacturing technology, AM can respond particularly rapidly to sudden increases in demand and meet needs for specialized objects that would otherwise not be economic to produce. Although these aspects of AM have long been understood by those familiar with the technology, the use of AM to meet the urgent need for personal protective equipment, nasal swabs, and other items in short supply in the face of the COVID-19 pandemic brought its potential to the attention of a much larger audience [5].

Wohlers Associates [50] identifies three sectors that have strong potential for future development of commercial AM products: 3D-printed electronics, which will allow incorporation of control circuits and sensors directly into products without requiring a separate circuit board; 3D-printed pharmaceuticals and biologicals, which will advance the ongoing expansion of personalized medicine; and 3D-printed consumer products, which range from jewelry to food. As noted previously, adoption of AM technology in these sectors may require new regulatory guidance.

In industry sectors where AM is already being adopted, it is expected to be increasingly incorporated into production as a complement to traditional manufacturing processes [260].

AM is particularly valuable as a means of simplifying a production system by consolidating assemblies composed of multiple parts into a single fabrication step [50]. In addition, AM is well suited as a means of making tools, fixtures, and jigs that allow rapid retooling of conventional production machinery, essentially extending AM's flexibility into the wider manufacturing arena [227]. Currently, the manufacturing sector is undergoing a digital transformation through the increased use of technologies such as the Internet of Things, artificial intelligence and machine learning, cybersecurity, and cloud computing [261]. AM is a manufacturing technology that is well suited for incorporation into the evolving digital manufacturing environment.

In addition to streamlining and extending the capabilities of traditional production lines, AM is also expected to encourage the expansion of distributed, localized manufacturing. Before the development of AM technologies, the start-up costs and resources necessary to manufacture items represented a significant hurdle to developing new products. By allowing for small scale manufacturing of complex parts, AM lowers these barriers in a number or ways. The flexibility of AM allows rapid production of small numbers of specialized objects at or near the point of use, which allows firms to both reduce the need to maintain a large inventory of many different objects as well as the time and expense of transporting and delivering products over long distances. In essence, AM converts physical inventory to digital files, which are easier to store and transmit than the material objects they represent [262]. In anticipation of the growth of localized fabrication capabilities, UPS has installed 3D-printing equipment associated with some of its distribution centers [226], which allow it to shift resources from long-distance hauling to "last mile" delivery for appropriate items. Decreasing equipment costs and increasing capability is also expected to result in the expansion of AM service providers, meeting needs ranging from specialized products and parts for industry to 3D-printing services at local copy and print shops for individuals [262].

In addition to expanded use of AM for production, the technology is also expected to become increasingly incorporated in the product design process. As a design tool, AM has historically been used for prototyping, but it is also being used for generative design, which uses artificial intelligence to create a suite of alternative solutions to a design problem that can be compared for optimal function and fabrication [262]. This application takes advantage of the inherently digital nature of AM, in which design files can be easily modified and fabricated for comparison of alternative solutions.

Expansion of AM will require a shift in the traditional business model of AM equipment providers. Historically, AM has been used primarily for prototyping and small-batch production of specialized objects. To meet these relatively modest needs, AM companies largely produced proprietary systems integrating equipment, software, and 3DP material. The closed nature of these systems has been a hindrance in integrating them into production streams. As the use of AM has expanded, however, third-party material suppliers are increasingly entering the market to serve customers without going through equipment manufacturers as intermediaries [263]. In addition, defining standard file formats will also be important to fully integrate AM into production systems [73].

The materials used for AM—polymers, metal powders, and ceramics—are largely not dependent on single sources (at least, no more so than the same materials used in traditional manufacturing) [227]. They are, however, typically more expensive than the same materials used in conventional manufacturing due to additional processing needed to prepare AM feedstock: polymers, which are conventionally sold as granules, must be converted to powders or filaments, and metals must be powdered and sifted [263]. Current research is focused on developing better processes to produce materials in a form appropriate for AM as well as designing AM equipment that can use conventionally prepared raw materials [263]. Lastly, advances in materials, like carbon fiber-polymer composites and specialized metal alloys, are expected to expand the usefulness of AM to new applications [260].

Expanding the use of AM technology and products will require R&D focused on [10]:

1. Further innovation and maturation of validated AM material performance models and analysis capabilities;
2. Expanding the number of materials that can be used in AM by establishing well-characterized and trusted process-structure-property relationships;
3. Developing and innovating in situ monitoring and control methods of AM processes that allow adaptive feedback control and defect detection; and
4. Developing post-processing and non-destructive evaluation tailored for AM parts in high-consequence applications.

The global market of AM technology and materials is expected to grow from $10.7 billion in 2020 to $34.6 billion in 2026 [50]. In addition, AM's integration into manufacturing is ultimately expected to be 50 times its current footprint [50]. The anticipated growth of AM in both production and design will require a sufficient number of designers, engineers, and equipment operators with understanding of the technology to meet future demand [263].

7.14. Recommendations

Over the past 30 years, AM technology has advanced significantly and is increasingly becoming integral to numerous sectors of the U.S. economy. Maintaining U.S. leadership on an increasingly competitive global manufacturing playing field will require supporting the entirety of the AM ecosystem: R&D, technology transfer, economic development, and education and training. The U.S. Government is uniquely positioned to advance AM technology by convening the full diversity of AM stakeholders, including universities and vocational schools (for education and training), researchers and technology providers (for technology advancements), standards development organizations (for technology transfer), investors and regulators as well as manufacturers and other end-users. The following recommendations are actions the United States can take to:

- grow the U.S. economy through the secure and safe development of AM;
- strengthen U.S. global competitiveness through faster and broader adoption of AM;
- mitigate current and emerging risks to the AM marketplace, supply chain, and workforce; and
- advance AM's adoption where there is advantage and opportunity to be gained.

7.14.1. Ensure that AM is Fully Integrated into the Modern Digital Manufacturing Environment

The global production and supply network of the 21st century increasingly relies on smart technologies, artificial intelligence, modeling and simulation, machine-to-machine communication, the Internet of Things, and distributed advanced manufacturing, including AM. Maintaining the U.S. position of global leadership in industrial innovation will require more rapid qualification and insertion of new AM technologies into the modern digital manufacturing ecosystem to accelerate their broader adoption and develop innovative new products. Seamless integration of AM into digital manufacturing networks requires clear technical standards, common file formats and data representations (e.g., digital twins), and digital design and analysis capabilities for AM parts, materials, processes, system controls, post-process inspection, and qualification/certification methods.

> **Recommendation 1a.** Expand Federal resources to accelerate development and adoption of technical standards, common file formats, and guidance to promote and facilitate more rapid qualification and insertion of new AM technologies into the digital manufacturing environment.
>
> **Recommendation 1b.** The U.S. Government should continue to support the efforts of the Manufacturing USA institutes to develop multi-institute collaborative projects to advance the integration of AM technologies into the manufacturing environment.

7.14.2. Identify and Mitigate Vulnerabilities in the Supply Chain of AM Feedstock

The supply of AM-ready feedstock is limited by the relatively small number of providers, many outside the United States, and despite an increasing number of third-party suppliers entering the market, the susceptibility of AM materials to foreign and domestic supply disruptions is uncertain. For example, titanium-based alloys play an important role in the aerospace and biomedical sectors. Ensuring a domestic capacity to produce, reclaim, and recycle AM-ready feedstock for titanium and other high-performance metal alloys could mitigate supply disruptions to these sectors. Expanding the supplier base of feedstock materials and investing in the development of new printable materials—including new metal alloys, ceramics, carbon fiber, and high-temperature composites—are needed to diversify the range of alternative AM materials and products and mitigate potential future supply chain vulnerabilities.

> **Recommendation 2a.** The U.S. Government should carry out a full assessment of both the capability and capacity of domestic AM material supply chains to meet national security, including economic security, needs and to be prepared to respond to future crises.
>
> **Recommendation 2b.** The assessment of AM capability and capacity should be used to formulate a Federal strategy to diversify the materials that can be responsibly used for AM to mitigate potential material supply chain disruptions.
>
> **Recommendation 2c.** The U.S. Government should assess the need for R&D, standards development, and other efforts to facilitate reclaiming and safe use of

recycled materials for AM as a potential source of feedstock materials and support such activities accordingly.

7.14.3. Coordinate and Support Investment in AM Research and Development Across the Federal Government

The U.S. Government plays numerous roles in the AM R&D ecosystem: it both conducts AM R&D and supports it through multiple Federal agencies, it provides unique R&D infrastructure in the form of user facilities (e.g., MDF at ORNL), and it participates in highly successful PPPs (e.g., America Makes). However, the focus of many government-supported or government-run AM R&D activities is determined by the sponsoring agency's mission and strategy at the expense of cross-sectoral technology development. Sustaining U.S. innovation in AM technology will require a Federal-level strategic investment policy for research and training that coordinates agency efforts.

Recommendation 3a. Assess the need for a Federal AM R&D interagency body with the mission of coordinating agency and cross-agency efforts to accelerate the advancement of AM technology by:

- identifying gaps in the U.S. AM R&D portfolio,
- identifying and minimizing redundancy in AM R&D among different agencies,
- encouraging and facilitating cross-fertilization of AM R&D across agencies and industrial sectors, and
- developing guidelines and sharing best practices for the strategic development, purchase, and responsible use of AM technology that enable the Federal Government to be a smart buyer of leading-edge AM systems.

Recommendation 3b. Ensure adequate Federal investments are dedicated to address high priority R&D gaps by conducting precompetitive research and transferring results to the AM community.

7.14.4. Support the Expansion of AM by Manufacturers Across Industrial Sectors and the Adoption of AM by Small Businesses and Manufacturers

AM technologies are well suited for small, localized manufacturing businesses. AM start-up costs are relatively low and the flexibility of the technology reduces entrepreneurs' risks by allowing rapid response to sudden changes in demand. However, development and application of AM in the United States is dominated by large companies, with smaller businesses lagging behind. The AM Forward initiative recently announced by the White House is a voluntary compact between large manufacturers and smaller U.S.-based suppliers that aims to strengthen supply chains by investing in small- and medium-sized companies, overcoming coordination challenges that limit adoption of AM technology, and investing in regional manufacturing ecosystems in the United States.

Recommendation 4a. The U.S. Government should increase support through the SBIR/STTR programs for small businesses and entrepreneurs developing and applying AM technology.

> **Recommendation 4b.** The U.S. Government should commit the resources needed to advance the objectives of AM Forward: encouraging increased participation of small businesses in the AM supply chain, providing capital and delivering technical assistance to small- and medium-sized manufacturers seeking to adopt AM, setting industry standards, and investing in the AM workforce.

7.14.5. Expand Technical Training and Workforce Development in AM

Despite its role in an increasingly automated manufacturing ecosystem, AM still requires human engineers, designers, technicians, and operators skilled in digital design, equipment operation, process controls, and post-process operations, particularly for the creation of objects that have narrow technical tolerances (e.g., airplane and spacecraft engine parts) or are highly personalized (e.g., surgical implants). As emphasized by the AM Forward initiative, the expansion of AM technology throughout the U.S. manufacturing landscape will require growth of an AM-qualified workforce as well as the pool of engineers and designers to develop new applications for AM technology.

> **Recommendation 5a.** The U.S. Government should continue to encourage cooperation among AM stakeholders (universities, community colleges, industry, standards development organizations, and professional societies) to develop and adopt certifications and credentials for AM operations.

> **Recommendation 5b.** The U.S. Government should identify and address high-priority gaps in vocational and university education programs aimed at expanding the AM workforce.

References

[1] Text - H.R.133 - 116th Congress (2019-2020): Consolidated Appropriations Act, 2021. Public Law 116-260. June 8, 2022. Accessed June 08, 2022. https://www.congress.gov/bill/116th-congress/house-bill/133/text.

[2] ISO (2022) *ISO/ASTM 52900:2021*. Available at https://www.iso.org/standard/74514.html.

[3] Calignano F, Manfredi D, Ambrosio EP, Biamino S, Lombardi M, Atzeni E, Salmi A, Minetola P, Iuliano L, Fino P (2017). Overview on Additive Manufacturing Technologies. *Proceedings of the IEEE* 105(4):593–612. https://doi.org/10.1109/JPROC.2016.2625098.

[4] Lohr, Steve (2022) 3-D Printing Grows Beyond Its Novelty Roots. *The New York Times*, July 3, 2022. https://www.nytimes.com/2022/07/03/business/3d-printing-vulcanforms.html.

[5] Gonzalez CM (2022) *On-Demand Additive Manufacturing Is the Future - ASME*. Available at https://www.asme.org/topics-resources/content/is-3d-printing-the-future-of-manufacturing.

[6] McCarthy MC, Di Prima MA, Cruz P, Ribic B, Wilczynski J, Ripley BA, Coburn JC (2021). Trust in the Time of Covid-19: 3D Printing and Additive Manufacturing (3DP/AM) As a Solution to Supply Chain Gaps. *NEJM Catalyst*. https://catalyst.nejm.org/doi/full/10.1056/CAT.21.0321.

[7] MarketsandMarkets (2021). 3D Printing Market with COVID-19 Impact Analysis: Global Forecast to 2026, by Offering (Printer (Industrial, Desktop), Material, Software, Service), Technology, Process, Application (Prototype, Tooling, Functional Part), Vertical, and Geography. https://www.marketsandmarkets.com/Market-Reports/3d-printing-market-1276.html

[8] The White House (2021) Fact Sheet: Biden-Harris Administration Announces Supply Chain Disruptions Task Force to Address Short-Term Supply Chain Discontinuities. *The White House*, June 8, 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/08/fact-sheet-biden-harris-administration-announces-supply-chain-disruptions-task-force-to-address-short-term-supply-chain-discontinuities/.

[9] The White House (2022) *Using Additive Manufacturing to Improve Supply Chain Resilience and Bolster Small and Mid-Size Firms*. Available at https://www.whitehouse.gov/cea/written-materials/2022/05/09/using-additive-manufacturing-to-improve-supply-chain-resilience-and-bolster-small-and-mid-size-firms/.

[10] Benedict, M., Moylan, S., Al-Abed, S., Ashford, C., Chou, K., Di Prima, M., Elwany, A., Gorelik, M., Lewis, A, Luxton, T., Marshall, B., Mullins, W., Sapochak, L., Russell, R., Warren, J., and Wells, D. (2022) The Strategy for American Leadership in High-Consequence Additive Manufacturing. NIST Advanced Manufacturing Series NIST AMS 600-10. https://nvlpubs.nist.gov/nistpubs/ams/NIST.AMS.600-10.pdf.

[11] U.S. Government Accountability Office (2015) GAO-15-505SP, 3D Printing: Opportunities, Challenges, and Policy Implications of Additive Manufacturing.

GAO-15-505SP. https://www.gao.gov/assets/files.gao.gov/assets/gao-15-505sp.pdf.

[12] Administrative Conference of the United States (ACUS), Public-Private Partnerships Working Group (2018) Guide to Legal Issues Involved in Public-Private Partnerships at the Federal Level. https://www.acus.gov.

[13] Additive Manufacturing Users Group (2022) *AMUG Conference – Additive Manufacturing Users Group*. Available at https://www.amug.com/amug-conference/.

[14] SME Communications (2022) *RAPID + TCT 2022: North America's Largest and Most Influential Additive Manufacturing Event*. Available at https://www.sme.org/aboutsme/newsroom/press-releases/2022/rapid--tct-2022-north-americas-largest-and-most-influential-additive-manufacturing-event/.

[15] University of Texas at Austin (2022) *Solid Freeform Fabrication Symposium*. Available at https://www.sffsymposium.org/.

[16] Fact Sheet: Biden Administration Celebrates Launch of AM Forward and Calls on Congress to Pass Bipartisan Innovation Act (2022). News release. May 6, 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/06/fact-sheet-biden-administration-celebrates-launch-of-am-forward-and-calls-on-congress-to-pass-bipartisan-innovation-act/.

[17] America Makes *America Makes: The Nation's Additive Manufacturing Institute*. Available at https://www.americamakes.us/.

[18] EWI *Additive Manufacturing Consortium: Services*. Available at https://ewi.org/services/research-services/additive-manufacturing-consortium/.

[19] AM CoE (2021) ASTM International Additive Manufacturing Center of Excellence. https://amcoe.org/wp-content/uploads/2022/05/AM-CoE-Trifold.pdf.

[20] NCAME (n.d.) *National Center for Additive Manufacturing Excellence (NCAME) - About*. Available at https://www.eng.auburn.edu/research/centers/additive/about/.

[21] ADAPT – Alliance for the Development of Additive Processing Technologies (n.d.) *Alliance for the Development of Additive Processing Technologies - Optimize for Additive (2022)*. Available at https://adapt.mines.edu/.

[22] Office of Management and Budget (2016) *OMB Circular a-119: Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities*. Available at https://www.whitehouse.gov/wp-content/uploads/2020/07/revised_circular_a-119_as_of_1_22.pdf.

[23] America Makes & ANSI Additive Manufacturing Standardization Collaborative (2018) Standardization Roadmap for Additive Manufacturing, Version 2.0, June 2018. https://share.ansi.org/Shared%20Documents/Standards%20Activities/AMSC/AMSC_Roadmap_June_2018.pdf.

[24] ACI (n.d.) *Committee Home: 564 - 3-D Printing with Cementitious Materials*. Available at https://www.concrete.org/committees/directoryofcommittees/acommitteehome.aspx?committee_code=C0056400.

[25] ASME (n.d.) *About ASME*. Available at https://www.asme.org/about-asme.

[26] ASME (n.d.) *ASME Code Committees*. Available at https://www.asme.org/codes-standards/asme-code-committee.

[27] ASTM International (2022) *Additive Manufacturing — General Principles — Fundamentals and Vocabulary*. Available at https://www.astm.org/f3177-21.html.

[28] ASTM International (2022) *Committee F42 Subcommittees*. Available at https://www.astm.org/get-involved/technical-committees/committee-f42/subcommittee-f42.

[29] ASTM International (2022) *Committee B09 on Metal Powders and Metal Powder Products*. Available at https://www.astm.org/get-involved/technical-committees/committee-b09.

[30] ASTM International (2022) *Committee E04 on Metallography*. Available at https://www.astm.org/committee-e04.

[31] ASTM International (2022) *E07.10 Jurisdiction Page*. Available at https://www.astm.org/get-involved/technical-committees/committee-e07/subcommittee-e07/jurisdiction-e0710.

[32] ASTM International (2022) *Committee E08 on Fatigue and Fracture*. Available at https://www.astm.org/committee-e08.

[33] ASTM International (2022) *Committee E28 on Mechanical Testing*. Available at https://www.astm.org/committee-e28.

[34] ASTM International (2022) *Committee E29 on Particle and Spray Characterization*. Available at https://www.astm.org/get-involved/technical-committees/committee-e29.

[35] ASTM International (2022) *F04.12 Jurisdiction Page*. Available at https://www.astm.org/get-involved/technical-committees/committee-f04/subcommittee-f04/jurisdiction-f0412.

[36] AWS (n.d.) *About AWS : About*. Available at https://www.aws.org/about/page/home.

[37] IEEE (2022) *IEEE CONSTITUTION & BYLAWS*. Available at https://www.ieee.org/content/dam/ieee-org/ieee/web/org/about/corporate/ieee-constitution-and-bylaws.pdf.

[38] IPC (n.d.) *Homepage*. Available at https://www.ipc.org/.

[39] ISO (n.d.) *ISO - International Organization for Standardization*. Available at https://www.iso.org/home.html.

[40] MPIF (n.d.) *Metal Powder Industries Federation: Advancing Powder Metallurgy & Particulate Materials Worldwide*. Available at https://www.mpif.org/.

[41] MTConnect (n.d.) *MTConnect About*. Available at https://www.mtconnect.org/about.

[42] NEMA (n.d.) *About*. Available at https://www.nema.org/about.

[43] NEMA (n.d.) *Standards That Power and Connect the Electroindustry*. Available at https://www.nema.org/standards.

[44] DICOM (n.d.) *DICOM Standards Committee*. Available at https://www.dicomstandard.org/dsc/.

[45] SAE International (n.d.) *About SAE International*. Available at https://www.sae.org/about.

[46] McCabe J (2018) *America Makes & ANSI Additive Manufacturing Standardization Collaborative (AMSC) Standards Landscape (Version 2.0)*. Available at https://share.ansi.org/Shared%20Documents/Standards%20Activities/AMSC/AMSC_Standards_Landscape_June_2018.pdf.

[47] Ruffo J (2022) *Gaps Progress Report Available: America Makes & ANSI Standardization Roadmap for Additive Manufacturing*. Available at https://www.americamakes.us/gaps-progress-report-available-america-makes-ansi-standardization-roadmap-for-additive-manufacturing/.

[48] McCabe, James (2022) *April 2022 Progress Report on AMSC Roadmap V2 Gaps*. Available at https://share.ansi.org/Shared%20Documents/Standards%20Activities/AMSC/April_2022_Progress_Report_AMSC_Roadmap_v2_Gaps.pdf.

[49] American National Standards Institute (2022) *Calling All Stakeholders: America Makes and ANSI to Develop Version 3 of Standardization Roadmap for Additive Manufacturing*. Available at https://www.ansi.org/news/standards-news/all-news/2022/09/9-12-22-calling-all-stakeholders-america-makes-and-ansi-to-develop-roadmap-am.

[50] Wohlers Associates (2021) Wohlers Report 2021: 3D Printing and Additive Manufacturing Global State of the Industry.

[51] Hanaphy, Paul (2022) X-Bow Tests Bolt Rocket Powered by Additive Manufactured Solid Propellant for the First Time. *3D Printing Industry*, August 3, 2022. https://3dprintingindustry.com/news/x-bow-tests-bolt-rocket-powered-by-additive-manufactured-solid-propellant-for-the-first-time-213266/.

[52] Chandru RA, Balasubramanian N, Oommen C, Raghunandan BN (2018). Additive Manufacturing of Solid Rocket Propellant Grains. *Journal of Propulsion and Power* 34(4):1090–93. https://doi.org/10.2514/1.B36734.

[53] LIFT (2021) *Driving American Manufacturing into the Future*. Available at https://lift.technology/about-us/.

[54] Manufacturing USA, NIST (2021) Manufacturing USA Highlights Report-a Summary of 2020 Accomplishments and Impacts G2022-0068 and NIST AMS 600-9. https://nvlpubs.nist.gov/nistpubs/ams/NIST.AMS.600-9.pdf.

[55] SAE International (2021) *About the SAE Aerospace Materials Specifications—Additive Manufacturing Data Consortium (SAE AMS-AMDC)*. Available at https://www.sae-itc.com/programs/amdc.

[56] Andrulonis, Rachael, Royal Livingfoss, Brian Smith, and Joel White (2021) Additive Manufacturing Research Program at WSU-NIAR. JAMS Technical Review, WSU-NIAR, August 26. https://www.wichita.edu/industry_and_defense/NIAR/Documents/jams-presentations-2021/Additive-Manufacturing-Research-Program-Adrulonis-White.pdf.

[57] GE Additive (2021) *GE Additive and Wichita State's NIAR Team up to Accelerate Metal Additive Technology for Rapid DoD Implementation*. Available at https://www.wichita.edu/industry_and_defense/NIAR/MediaCenter/2021-11-16.php.

[58] CAMT (2022) *Center for Aerospace Manufacturing Technologies*. Available at https://camt.mst.edu/.

[59] Missouri One Start (2022) *Aerospace: Top State for Workforce Development and Customized Training*. Available at https://missourionestart.com/industries-served/aerospace/.

[60] Simpson, Timothy W. (2021) Another Giant Leap for AM — New Standards. *Additive Manufacturing*, September 2, 2021. https://www.additivemanufacturing.media/articles/another-giant-leap-for-am-new-standards.

[61] Aerospace Industries Association (2022) *National Aerospace Standards*. Available at https://www.aia-aerospace.org/standards/.

[62] AIA Additive Manufacturing Working Group (2020) Recommended Guidance for Certification of AM Components. https://www.aia-aerospace.org/wp-content/uploads/2020/02/AIA-Additive-Manufacturing-Best-Practices-Report-Final-Feb2020.pdf.

[63] Brooke L (2022) *Directing GM's 3D-Printed Future*. Available at https://www.sae.org/news/2020/08/directing-gm%E2%80%99s-3d-printed-future.

[64] Hendrixson, Stephanie (2021) Real Examples of 3D Printing in the Automotive Industry. *Modern Machine Shop*, May 17, 2021. https://www.mmsonline.com/articles/real-examples-of-3d-printing-in-the-automotive-industry.

[65] United States Council for Automotive Research (2020) Roadmap for Automotive Additive Manufacturing. https://uscar.org/download/357/additive-manufacturing/13457/uscar-roadmap-for-automotive-am-final.pdf.

[66] Lizotte, Cedric (2014) A View Inside Ford's 3D Printing Lab. *3DPrint.com*, June 6, 2014. https://3dprint.com/5318/ford-3d-printing/.

[67] General Motors (2020) *General Motors Increases Agility and Speed by Opening All-New Additive Industrialization Center Dedicated to 3D Printing*. Available at https://news.gm.com/newsroom.detail.html/Pages/news/us/en/2020/dec/1214-additive.html.

[68] United States Council for Automotive Research (2022) *Technologies – USCAR*. Available at https://uscar.org/technologies-teams/.

[69] SAE International (2022) *Standards Collections*. Available at https://www.sae.org/standards.

[70] ISO/ASTM (2022) *Additive Manufacturing for Automotive—Qualification Principles—Generic Machine Evaluation and Specification of Key Performance Indicators for PBF-LB/M Processes (ISO/ASTM AWI 52945)*. Available at https://www.iso.org/standard/81178.html.

[71] Sher, Davide (2020) Subcommittee F42 Publishes New ISO/ASTM 52941 Standard for AM. *3D Printing Media Network*, December 17, 2020. https://www.3dprintingmedia.network/subcommittee-f42-publishes-new-iso-astm-52941-standard-for-am/.

[72] Liaw C-Y, Guvendiren M (2017). Current and Emerging Applications of 3D Printing in Medicine. *Biofabrication* 9(2):24102. https://doi.org/10.1088/1758-5090/aa7279.

[73] Singh S, Ramakrishna S (2017). Biomedical Applications of Additive Manufacturing: Present and Future. *Current Opinion in Biomedical Engineering* 2:105–15. https://doi.org/10.1016/j.cobme.2017.05.006.

[74] Ahangar P, Cooke ME, Weber MH, Rosenzweig DH (2019). Current Biomedical Applications of 3D Printing and Additive Manufacturing. *Applied Sciences* 9(8):1713. https://doi.org/10.3390/app9081713.

[75] Kumar R, Kumar M, Chohan JS (2021). The Role of Additive Manufacturing for Biomedical Applications: A Critical Review. *Journal of Manufacturing Processes* 64:828–50. https://doi.org/10.1016/j.jmapro.2021.02.022.

[76] U.S. Food and Drug Administration (2019) *How to Determine If Your Product Is a Medical Device*. Available at https://www.fda.gov/medical-devices/classify-your-medical-device/how-determine-if-your-product-medical-device.

[77] Hay, Zachary (2019) 3D Printing Skin: The Most Promising Projects. *All3DP*, November 7, 2019. https://all3dp.com/2/3d-printing-skin-the-most-promising-projects/.

[78] Rabin, Roni Caryn (2022) Doctors Transplant Ear of Human Cells, Made by 3-D Printer. *The New York Times*, June 2, 2022. https://www.nytimes.com/2022/06/02/health/ear-transplant-3d-printer.html?smid=url-share.

[79] Bhattacharya S, Bustillos J, Moridi A, Quevedo Gozalez F, Spector JA (2020). Biomedical Applications of Metal Additive Manufacturing: Current State-of-the-Art and Future Perspective. *AJBSR* 7(1): 6- https://biomedgrid.com/pdf/AJBSR.MS.ID.001103.pdf. https://biomedgrid.com/fulltext/volume7/biomedical-applications-of-metal-additive-manufacturing-current-state.001103.php.

[80] Trivedi M, Jee J, Silva S, Blomgren C, Pontinha VM, Dixon DL, van Tassel B, Bortner MJ, Williams C, Gilmer E, Haring AP, Halper J, Johnson BN, Kong Z, Halquist MS, Rocheleau PF, Long TE, Roper T, Wijesinghe DS (2018). Additive Manufacturing of Pharmaceuticals for Precision Medicine Applications: A Review of the Promises and Perils in Implementation. *Additive Manufacturing* 23:319–28. https://doi.org/10.1016/j.addma.2018.07.004.

[81] Zhang J, Vo AQ, Feng X, Bandari S, Repka MA (2018). Pharmaceutical Additive Manufacturing: A Novel Tool for Complex and Personalized Drug Delivery Systems. *AAPS PharmSciTech* 19(8):3388–3402. https://doi.org/10.1208/s12249-018-1097-x.

[82] SPRITAM® (2021) *What Is SPRITAM?* Available at https://spritam.com/what-is-spritam/.

[83] ASTM Center of Excellence (2022) *2104: Powder Cleanliness Assessment Classification and Measurement Methodologies (MTC)*. Available at https://amcoe.org/project/powder-cleanliness-assessment-methodologies-2104.

[84] America Makes (2021) *4031 AM of Biomedical Devices from Bioresorbable Metallic Alloys for Medical Applications - America Makes*. Available at https://www.americamakes.us/projects/4031-biomedical-devices-bioresorbable-metallic-alloys-medical-applications/.

[85] U.S. Food and Drug Administration (2022) *Recognized Consensus Standards*. Available at https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfStandards/search.cfm.

[86] Chepelev L, Wake N, Ryan J, Althobaity W, Gupta A, Arribas E, Santiago L, Ballard DH, Wang KC, Weadock W, Ionita CN, Mitsouras D, Morris J, Matsumoto J, Christensen A, Liacouras P, Rybicki FJ, Sheikh A (2018). Radiological Society of North America (RSNA) 3D Printing Special Interest

Group (SIG): Guidelines for Medical 3D Printing and Appropriateness for Clinical Scenarios. *3D Print Med* 4(1):11. https://doi.org/10.1186/s41205-018-0030-y.

[87] Risk Management Group, Office of Hazard Identification and Reduction, CPSC (2020) Safety Concerns Associated with 3D Printing and 3D Printed Consumer Products. https://www.cpsc.gov/s3fs-public/Safety-Concerns-Associiated-with-3D-Printing-and-3D-Printed-Consumer-Products.pdf.

[88] University of Texas at Arlington Online (2022) *How Can 3D Printers Be Used for Educational Purposes?* Available at https://academicpartnerships.uta.edu/articles/education/how-can-3d-printers-be-used-for-educational-purposes.aspx.

[89] Formlabs (2018) *Gillette Uses 3D Printing to Unlock Consumer Personalization*.

[90] Godber M (2015) *Additive Manufacturing Takes Conformal Cooling to New Heights*. Available at https://www.plasticstoday.com/injection-molding/additive-manufacturing-takes-conformal-cooling-new-heights.

[91] Formlabs (2019) *How 3D Printing Is Disrupting the Jewelry Industry*.

[92] Pasricha A, Greeninger R (2018). Exploration of 3D Printing to Create Zero-Waste Sustainable Fashion Notions and Jewelry. *Fash Text* 5(1):1–18. https://doi.org/10.1186/s40691-018-0152-2.

[93] Quinlan H, Hart AJ (2020). Implications for Technological Change, Workforce Development, and the Product Lifecycle. *MIT Work of the Future Research Brief* 14: 1–58. https://workofthefuture.mit.edu/wp-content/uploads/2020/11/2020-Research-Brief-Quinlan-Hart4.pdf.

[94] Hexr (2022) *The World's First Custom Fit Helmet*. Available at https://hexr.com/.

[95] P., Madeleine (2021) Athos, 3D Printed Climbing Shoes That Adapt to an Athlete's Feet. *3Dnatives*, September 1, 2021. https://www.3dnatives.com/en/athos-the-3d-printed-climbing-shoes-020920214/.

[96] GuardLab (2022) *GuardLab Custom Mouthguards | 3D Scan Digital Accuracy*. Available at https://guardlab.com/.

[97] Chua, Julian (2021) How Additive Manufacturing Is Making a Difference in Sports. *Sports Technology Blog*, July 30, 2021. https://sportstechnologyblog.com/2021/07/30/additive-manufacturing-making-a-difference-in-sports/.

[98] Novak JI, Novak AR (2021). Is Additive Manufacturing Improving Performance in Sports? A Systematic Review. *Journal of Sports Engineering and Technology* 235(3): 163–75. https://journals.sagepub.com/doi/10.1177/1754337120971521.

[99] Adidas (2022) *Adidas 4D Fusio Shoes*. Available at https://www.adidas.com/us/4d-fusio-shoes/FZ3894.html.

[100] UL Standards Technical Panel (2019) *UL Standard | UL 2904*. Available at https://www.shopulstandards.com/ProductDetail.aspx?UniqueKey=35397.

[101] Chemical Insights (2019) *UL Publishes ANSI/CAN/UL 2904 Standard for 3D Printers*. Available at https://chemicalinsights.org/resource/ul-publishes-ansi-can-ul-2904-standard-for-3d-printers/.

[102] ISO (2022) *ISO/TC 261 - Additive Manufacturing*. Available at https://www.iso.org/committee/629086.html.

[103] ASTM International (2022) *Subcommittee F42.07.09 on Consumer*. Available at https://www.astm.org/get-involved/technical-committees/committee-f42/subcommittee-f42/jurisdiction-f420709.

[104] Consumer Product Safety Commission (2022) *Consumer Product Safety Commission: A Notice by the Consumer Product Safety Commission on 01/28/2022*. Available at https://www.federalregister.gov/documents/2022/01/28/2022-01721/cpsc-artificial-intelligence-and-machine-learning-test-and-evaluation-forum.

[105] Ashby D (2022) *CCM Hockey and Carbon Create the First-Ever NHL Certified 3D Printed Hockey Helmet Liner*. Available at https://www.carbon3d.com/news/press-releases/ccm-hockey-and-carbon-create-the-first-ever-nhl-certified-3d-printed-hockey-helmet-liner.

[106] Griffin E, Orsatti B, and Saric IH (2022) *Riddell and Carbon® Produce First-Ever 3D Printed Football Helmet Liner*. Available at https://www.carbon3d.com/news/press-releases/riddell-carbon-produce-football-helmet.

[107] Sun C, Wang Y, McMurtrey MD, Jerred ND, Liou F, Li J (2021). Additive Manufacturing for Energy: A Review. *Applied Energy* 282:116041. https://doi.org/10.1016/j.apenergy.2020.116041.

[108] Zhakeyev A, Wang P, Zhang L, Shu W, Wang H, Xuan J (2017). Additive Manufacturing: Unlocking the Evolution of Energy Materials. *Advanced science (Weinheim, Baden-Wurttemberg, Germany)* 4(10):1700187. https://doi.org/10.1002/advs.201700187.

[109] Connectivity Standards Alliance (2022) *Matter Arrives Bringing a More Interoperable, Simple and Secure Internet of Things to Life*. Available at https://csa-iot.org/newsroom/matter-arrives/.

[110] Westinghouse Electric (2019) *Advancing Our Manufacturing Capabilities to Meet Your Component Needs*. Available at https://info.westinghousenuclear.com/news/advancing-our-manufacturing-capabilities-to-meet-your-component-needs.

[111] Post B, Richardson B, Lloyd P, Love L, Nolet S, Hannan J (2017) Additive Manufacturing of Wind Turbine Molds. https://www.ornl.gov/sites/default/files/2019-06/web_TPI_MDF-TC-2016-084_Final%20Report.pdf.

[112] BioEnergy Science Center (2017) *BioEnergy Research Center 2007-2017*. Available at https://www.bioenergycenter.org/besc/.

[113] Seay SG (2017) *At the MDF: New Large-Area, Multi-Material Printer to Advance Research | ORNL*. Available at https://www.ornl.gov/blog/mdf-new-large-area-multi-material-printer-advance-research.

[114] American Petroleum Institute (2021) *API Standard 20S, 1st Edition*. Available at https://www.api.org/products-and-services/standards/important-standards-announcements/20s.

[115] Goh GL, Agarwala S, Goh GD, Tan HKJ, Zhao L, Chuah TK, Yeong WY (2018). Additively Manufactured Multi-Material Free-Form Structure with Printed Electronics. *Int J Adv Manuf Technol* 94(1-4):1309–16. https://doi.org/10.1007/s00170-017-0972-z.

[116] 3D Systems (2021) *Additive Manufacturing for Semiconductor Capital Equipment | 3D Systems*. Available at https://www.3dsystems.com/semiconductor.

[117] Gagnon JC, Presley M, Le NQ, Montalbano TJ, Storck S (2019). A Pathway to Compound Semiconductor Additive Manufacturing. *MRS Communications* 9(3):1001–7. https://doi.org/10.1557/mrc.2019.114.

[118] Guo Y, Shen P-C, Su C, Lu A-Y, Hempel M, Han Y, Ji Q, Lin Y, Shi E, McVay E, Dou L, Muller DA, Palacios T, Li J, Ling X, Kong J (2019). Additive Manufacturing of Patterned 2D Semiconductor Through Recyclable Masked Growth | Proceedings of the National Academy of Sciences. *PNAS* 116(9): 3437–42. https://www.pnas.org/doi/full/10.1073/pnas.1816197116.

[119] Amexci (2022) *Embarking on an Additive Manufacturing Journey with Ericsson – AMEXCI*. Available at https://amexci.com/embarking-additive-manufacturing-journey-ericsson/.

[120] Want R (2006). An Introduction to RFID Technology. *IEEE Pervasive Computing* 5(1): 25–33. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1593568.

[121] Colella R, Chietera FP, Montagna F, Greco A, Catarinucci L *On the Use of Additive Manufacturing 3D-Printing Technology in RFID Antenna Design* . Available at https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8892205.

[122] ESA (2017) *Metal 3D-Printed Waveguides Proven for Telecom Satellites*. Available at https://www.esa.int/Enabling_Support/Space_Engineering_Technology/Metal_3D-printed_waveguides_proven_for_telecom_satellites.

[123] 3D Systems (2017) *First Air-Worthy Metal 3D Printed RF Filter Ready for Take-Off*. Available at https://www.3dsystems.com/customer-stories/first-air-worthy-metal-printed-rf-filter-ready-take.

[124] DOE Office of Energy Efficiency & Renewable Energy (2015) *EERE Success Story—Novel 3-D Printed Inverters for Electric Vehicles Can Improve EV Power and Efficiency*. Available at https://www.energy.gov/eere/success-stories/articles/eere-success-story-novel-3-d-printed-inverters-electric-vehicles-can.

[125] Chowdhury S, E. Gurpinar E, Su G-J, Raminosoa T, Burress TA, Ozpineci B *Enabling Technologies for Compact Integrated Electric Drives for Automotive Traction Applications* . Available at https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8790594.

[126] IEEE Computer Society (2022) IEEE Standard for Test Methods for the Characterization of Organic Transistors and Materials. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5982063.

[127] International Electrotechnical Commission (2022) *TC 119 Printed Electronics*. Available at https://www.iec.ch/dyn/www/f?p=103:7:0::FSP_ORG_ID:8679.

[128] Abbot, Ginger (2021) 5 Top Trends in the Construction Industry for 2022. *National Center for Construction Education and Research*, November 18, 2021. https://www.nccer.org/news-research/newsroom/blogpost/breaking-ground-the-nccer-blog/2021/11/18/5-top-trends-in-the-construction-industry-for-2022.

[129] Verzoni, A. (2020). 3D Printed Buildings and UL 3401 - Printing Buildings. *NFPA Journal* 114(2). https://code-authorities.ul.com/3d-printed-buildings/.

[130] National Fire Protection Association (2020) *Beyond Concrete*. Available at https://www.nfpa.org/News-and-Research/Publications-and-media/NFPA-Journal/2020/March-April-2020/Features/3D-Printing/Beyond-Concrete.

[131] Maxwell, Jack (2021) The Shape of Concrete to Come. *Standardization New Online*, March 4, 2021. https://sn.astm.org/?q=features/shape-concrete-come-ma21.html.

[132] Vora, Shivani (2021) The World's Largest 3D-Printed Community Is Coming to Texas. *Architectural Digest*, November 10, 2021. https://www.architecturaldigest.com/story/austin-3d-printing-community.

[133] Bukkapatnam, S., J. Mander, S. Paal, Z. Pei, and L. Zeng (2017) NSF Workshop on Additive Manufacturing (3D Printing) For Civil Infrastructure Design and Construction. https://events.tti.tamu.edu/wp-content/uploads/2017/04/nsf-3dp-workshop-report.pdf.

[134] Everett, Hayley (2021) ICON and NASA Bring Lunar Infrastructure Closer with World's First 3D Printed Rocket Pad. *3D Printing Industry*, March 22, 2021. https://3dprintingindustry.com/news/icon-and-nasa-bring-lunar-infrastructure-closer-with-worlds-first-3d-printed-rocket-pad-187323/.

[135] Hanaphy, Paul (2020) U.S. Marines Use ICON 3D Printing to Create Concrete Structures at Camp Pendleton. *3D Printing Industry*, August 4, 2020. https://3dprintingindustry.com/news/u-s-marines-use-icon-3d-printing-to-create-concrete-structures-at-camp-pendleton-174200/.

[136] Hambling, David (2021) U.S. Army's New Expeditionary 3D Concrete Printer Can Go Anywhere, Build Anything. *Forbes*, October 14, 2021. https://www.forbes.com/sites/davidhambling/2021/10/14/us-army-expeditionary-3d-concrete-printer-to-go-anywhere-build-anything/?sh=3251d1b92d89.

[137] Hopper HD (2020) *Build Trust in 3D Manufactured Buildings with UL 3401*. Available at https://www.ul.com/news/build-trust-3d-manufactured-buildings-ul-3401.

[138] U.S. General Services Administration (2021) P100 - Facilities Standards for the Public Buildings Service (With 2022 Addendum). https://www.gsa.gov/cdnstatic/P100%202022%20Addendum%20Final_.pdf.

[139] International Code Council (2018). Code Adoption Maps. https://www.iccsafe.org/wp-content/uploads/Code_Adoption_Maps.pdf.

[140] Quick Response Fire Supply (2020) #313 – ICC and NFPA Codes and Standards: A Basic Guide. *Quick Response Fire Supply (QRFS.com)*, January 7, 2020. https://blog.qrfs.com/313-icc-and-nfpa-codes-and-standards-a-basic-guide/.

[141] American Concrete Institute (2022) *564 - 3-D Printing with Cementitious Materials - Committee Home*. Available at https://www.concrete.org/committees/directoryofcommittees/acommitteehome.aspx?committee_code=C0056400.

[142] Molitch-hou, Michael (2020) The State of 3D Printing in Heavy Equipment. *3DPrint.com*, January 25, 2020. https://3dprint.com/262432/the-state-of-3d-printing-in-heavy-equipment/.

[143] Johnson, S (n.d.) *Additive Manufacturing*. Available at https://www.caterpillar.com/en/company/innovation/customer-solutions/additive-manufacturing.html/.

[144] Davies, Sam (2017) FIT AG and Caterpillar Inc Join Forces to 3D Print Aluminium and Titanium Parts. *TCT Magazine*, March 14, 2017. https://www.tctmagazine.com/additive-manufacturing-3d-printing-news/fit-ag-caterpillar-join-forces-3d-print-aluminium-titanium/.

[145] Scott, Clare (2018) Volvo CE Adopts 3D Printing for Spare Parts and Prototyping. *3DPrint.com*, March 28, 2018. https://3dprint.com/208226/volvo-ce-3d-printing/.

[146] Association of Equipment Manufacturers (2017) *Project AME: World's First 3D Printed Excavator Unveiled*. Available at https://www.aem.org/news/project-ame-worlds-first-3d-printed-excavator-unveiled.

[147] ASTM International (2022) *Subcommittee F42.07.07 on Construction Matching Standards Under the Jurisdiction of F42.07.07 by Status*. Available at https://www.astm.org/get-involved/technical-committees/committee-f42/subcommittee-f42/jurisdiction-f420707.

[148] ASTM International (2022) *Subcommittee F42.07.04 on Transportation/Heavy Machinery Matching Standards Under the Jurisdiction of F42.07.04 by Status*. Available at https://www.astm.org/get-involved/technical-committees/committee-f42/subcommittee-f42/jurisdiction-f420704.

[149] 49 U.S. Code § 106 - Federal Aviation Administration. 49 U.S. Code § 106 - Federal Aviation Administration. June 8, 2022. Accessed June 22, 2022. https://www.law.cornell.edu/uscode/text/49/106.

[150] 49 U.S. Code § 44701 - General Requirements. 49 U.S. Code § 44701 - General requirements. https://www.law.cornell.edu/uscode/text/49/44701.

[151] Federal Aviation Administration (FAA) 14 CFR Part 21 (n.d.) Certification Procedures for Products and Articles. https://www.law.cornell.edu/cfr/text/14/part-21.

[152] National Aeronautics and Space Administration (2021) *NASA Technical Standards: Program Overview*. Available at https://standards.nasa.gov/program-overview.

[153] National Aeronautics and Space Administration (2017) *NASA Procedural Requirements NPR 7120.10A*. Available at https://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPR&c=7120&s=10A.

[154] Seifi M, Gorelik M, Waller J, Hrabe N, Shamsaei N, Daniewicz S, Lewandowski JJ (2017). Progress Towards Metal Additive Manufacturing Standardization to Support Qualification and Certification. *Journal of The Minerals, Metals and Materials Society (JOM)* 69(3):439–55. https://doi.org/10.1007/s11837-017-2265-2.

[155] Visconti, Kelly (2020) Joint Additive Manufacturing Working Group & Data Management Update. NIST FAIR Data Management Workshop, October 27. https://www.asminternational.org/documents/42461398/0/1.4+Kelly+Visconti+Brief+%28final%29.pdf%20/529be888-359f-2160-861c-6169060f9548.

[156] Defense Acquisition University (2022) *Specifications and Standards*. Available at https://www.dau.edu/acquipedia/pages/articledetails.aspx#!247.

[157] National Highway Traffic Safety Administration (2022) *Laws & Regulations*. Available at https://www.nhtsa.gov/laws-regulations.

[158] 49 CFR Part 571 - Federal Motor Vehicle Safety Standards. 49 CFR Part 571 - Federal Motor Vehicle Safety Standards. June 27, 2022. Accessed June 27, 2022. https://www.ecfr.gov/current/title-49/subtitle-B/chapter-V/part-571.

[159] 40 CFR Chapter I Subchapter U -- Air Pollution Controls (2022) *40 CFR Chapter I Subchapter U -- Air Pollution Controls*. Available at https://www.ecfr.gov/current/title-40/chapter-I/subchapter-U.

[160] Environmental Protection Agency (2013) *Automotive Sectors (NAICS 336, 4231, 8111)*. Available at https://www.epa.gov/regulatory-information-sector/automotive-sectors-naics-336-4231-8111.

[161] Petrolab (2013) *US EPA Confirms ASTM D6377 as an Alternative Test Method for Measuring Vapor Pressure of Crude Oils*. Available at https://www.petrolab.com/pressreleases/news/2013/october/us-epa-confirms-astm-d6377-as-an-alternative-test-method-for-measuring-vapor-pressure-of-crude-oils.

[162] Murphy B (2010) *U.S. EPA Approves ASTM Test Methods for Contaminated Water Testing*. Available at https://newsroom.astm.org/us-epa-approves-astm-test-methods-contaminated-water-testing.

[163] U.S. Food and Drug Administration (2018) *What We Do*. Available at https://www.fda.gov/about-fda/what-we-do.

[164] Di Prima M, Coburn J, Hwang D, Kelly J, Khairuzzaman A, Ricles L (2016). Additively Manufactured Medical Products - the FDA Perspective. *3D Print Med* 2(1):1–6. https://doi.org/10.1186/s41205-016-0005-9.

[165] U.S. Food and Drug Administration (2021) 3D Printing Medical Devices at the Point of Care: Discussion Paper. https://www.fda.gov/medical-devices/3d-printing-medical-devices/3d-printing-medical-devices-point-care-discussion-paper.

[166] U.S. Consumer Product Safety Commission (2022) *About Us*. Available at https://www.cpsc.gov/About-CPSC.

[167] U.S. Department of Commerce (2022) U.S. Department of Commerce Strategic Plan 2022-2026. https://www.commerce.gov/sites/default/files/2022-03/DOC-Strategic-Plan-2022%E2%80%932026.pdf.

[168] Environmental Protection Agency (2013) *Summary of the Toxic Substances Control Act*. Available at https://www.epa.gov/laws-regulations/summary-toxic-substances-control-act.

[169] U.S. Department of Energy (2017) *What Is Additive Manufacturing?* Available at https://www.energy.gov/eere/articles/what-additive-manufacturing.

[170] U.S. Nuclear Regulatory Commission (2022) *§ 50.59 Changes, Tests and Experiments*. Available at https://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-0059.html.

[171] Federal Communications Commission (2015) *Rulemaking Process*. Available at https://www.fcc.gov/about-fcc/rulemaking-process.

[172] Defense Microelectronic Activity (2022) *DMEA - Trusted IC Program*. Available at https://www.dmea.osd.mil/TrustedIC.aspx.

[173] NIST (2020) *Additive Manufacturing with Cement-Based Materials*. Available at https://www.nist.gov/programs-projects/additive-manufacturing-cement-based-materials.

[174] 15 USC 7301: National Construction Safety Teams. 15 USC 7301: National Construction Safety Teams. September 7, 2022. Accessed September 07, 2022.

https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title15-section7301&num=0&edition=prelim.

[175] Federal Emergency Management Agency (2016) Public Assistance Required Minimum Standards - FEMA Recovery Policy FP-104-009-4. https://www.fema.gov/sites/default/files/2020-05/FEMA_Public_Assistance_Minimum_Standards_Policy_signed_9-30-16.pdf.

[176] Ellard WH (2017) *FEMA Requires Compliance with National Standard Building Codes for Restoration of Facilities Funded Through Public Assistance Grant Program*. Available at https://www.bakerdonelson.com/fema-requires-compliance-with-national-standard-building-codes-for-restoration-of-facilities-funded-through-public-assistance-grant-program.

[177] 40 U.S. Code § 3312 - Compliance with Nationally Recognized Codes. 40 U.S. Code § 3312 - Compliance with nationally recognized codes. https://www.law.cornell.edu/uscode/text/40/3312.

[178] Occupational Safety and Health Administration (2022) *1926.6 - Incorporation by Reference*. Available at https://www.osha.gov/laws-regs/regulations/standardnumber/1926/1926.6.

[179] J.J. Keller and Associates, Inc. (2022) *Heavy Equipment*. Available at https://www.jjkeller.com/learn/heavy-equipment-overview.

[180] U.S. Environmental Protection Agency (2017) *Regulations for Emissions from Heavy Equipment*. Available at https://www.epa.gov/regulations-emissions-vehicles-and-engines/regulations-emissions-heavy-equipment.

[181] Jurrens, Kevin (2020) NIST Perspectives on Additive Manufacturing Standards Landscape, November 4.

[182] National Institute of Standards and Technology Additive Manufacturing Benchmark Test Series (AM-Bench) | NIST. https://www.nist.gov/ambench.

[183] National Institute for Occupational Safety and Health (2020) 3D Printing with Filaments: Health and Safety Questions to Ask. https://www.cdc.gov/niosh/docs/2020-115/pdfs/2020-115.pdf.

[184] National Institute for Occupational Safety and Health (2020) 3D Printing with Metal Powders: Health and Safety Questions to Ask. https://www.cdc.gov/niosh/docs/2020-114/pdfs/2020-114.pdf?id=10.26616/NIOSHPUB2020114.

[185] Bowers LN, Ranpara AC, Roach KA, Knepp AK, Arnold ED, Stefaniak AB, Virji MA (2022). Comparison of Product Safety Data Sheet Ingredient Lists with Skin Irritants and Sensitizers Present in a Convenience Sample of Light-Curing Resins Used in Additive Manufacturing. *Regulatory toxicology and pharmacology : RTP* 133:105198. https://doi.org/10.1016/j.yrtph.2022.105198.

[186] Bowers LN, Stefaniak AB, Knepp AK, LeBouf RF, Martin SB, Ranpara AC, Burns DA, Virji MA (2022). Potential for Exposure to Particles and Gases Throughout Vat Photopolymerization Additive Manufacturing Processes. *Buildings* 12(8):1222. https://doi.org/10.3390/buildings12081222.

[187] Stefaniak AB, Bowers LN, Knepp AK, Luxton TP, Peloquin DM, Baumann EJ, Ham JE, Wells JR, Johnson AR, LeBouf RF, Su F-C, Martin SB, Virji MA (2019). Particle and Vapor Emissions from Vat Polymerization Desktop-Scale 3-

Dimensional Printers. *Journal of occupational and environmental hygiene* 16(8):519–31. https://doi.org/10.1080/15459624.2019.1612068.

[188] Stefaniak AB, Bowers LN, Knepp AK, Virji MA, Birch EM, Ham JE, Wells JR, Qi C, Schwegler-Berry D, Friend S, Johnson AR, Martin SB, Qian Y, LeBouf RF, Birch Q, Hammond D (2018). Three-Dimensional Printing with Nano-Enabled Filaments Releases Polymer Particles Containing Carbon Nanotubes into Air. *Indoor Air* 28(6):840–51. https://doi.org/10.1111/ina.12499.

[189] Stefaniak AB, Bowers LN, Martin SB, Hammond DR, Ham JE, Wells JR, Fortner AR, Knepp AK, Du Preez S, Pretty JR, Roberts JL, Du Plessis JL, Schmidt A, Duling MG, Bader A, Virji MA (2021). Large-Format Additive Manufacturing and Machining Using High-Melt-Temperature Polymers. Part II: Characterization of Particles and Gases. *Journal of chemical health & safety* 28(4):268–78. https://doi.org/10.1021/acs.chas.0c00129.

[190] Stefaniak AB, Bowers LN, Martin SB, Hammond DR, Ham JE, Wells JR, Fortner AR, Knepp AK, Du Preez S, Pretty JR, Roberts JL, Du Plessis JL, Schmidt A, Duling MG, Bader A, Virji MA (2021). Large-Format Additive Manufacturing and Machining Using High-Melt-Temperature Polymers. Part I: Real-Time Particulate and Gas-Phase Emissions. *Journal of chemical health & safety* 28(3):190–200. https://doi.org/10.1021/acs.chas.0c00128.

[191] Stefaniak AB, Johnson AR, Du Preez S, Hammond DR, Wells JR, Ham JE, LeBouf RF, Menchaca KW, Martin SB, Duling MG, Bowers LN, Knepp AK, Su FC, Beer DJ de, Du Plessis JL (2019). Evaluation of Emissions and Exposures at Workplaces Using Desktop 3-Dimensional Printer. *Journal of chemical health & safety* 26(2):19–30. https://doi.org/10.1016/j.jchas.2018.11.001.

[192] Stephens B, Azimi P, El Orch Z, Ramos T (2013). Ultrafine Particle Emissions from Desktop 3D Printers. *Atmospheric Environment* 79:334–39. https://doi.org/10.1016/j.atmosenv.2013.06.050.

[193] Yi J, Duling MG, Bowers LN, Knepp AK, LeBouf RF, Nurkiewicz TR, Ranpara A, Luxton T, Martin SB, Burns DA, Peloquin DM, Baumann EJ, Virji MA, Stefaniak AB (2019). Particle and Organic Vapor Emissions from Children's 3-D Pen and 3-D Printer Toys. *Inhalation Toxicology* 31(13-14):432–45. https://doi.org/10.1080/08958378.2019.1705441.

[194] Dunn KL, Dunn KH, Hammond D, Lo S (2020). Three-Dimensional Printer Emissions and Employee Exposures to Ultrafine Particles During the Printing of Thermoplastic Filaments Containing Carbon Nanotubes or Carbon Nanofibers. *J Nanopart Res* 22(2):1–13. https://doi.org/10.1007/s11051-020-4750-8.

[195] National Aeronautics and Space Administration (NASA), Office of the Chief Engineer (2020) Additive Manufacturing Requirements for Spaceflight Systems, NASA-STD-6030. https://standards.nasa.gov/sites/default/files/standards/NASA/Baseline/0/2021-04-21_nasa-std-6030-approveddocx.pdf.

[196] Oak Ridge National Laboratory (2022) *Manufacturing Demonstration Facility*. Available at https://www.ornl.gov/facility/mdf.

[197] U.S. Department of Commerce (DOC) (n.d.) 15 CFR Part 730. https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-730?toc=1

[198] CFR - Code of Federal Regulations Title 21. Food and Drug Administration. December 6, 2022. Accessed December 06, 2022. https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=820.

[199] Uniformed Services University (2022) *4D Bio3 - What We Do*. Available at https://www.usuhs.edu/4D-Bio3.

[200] Uniformed Services University (2022) *4D Bio3, Leadership*. Available at https://www.usuhs.edu/4D-Bio3/leadership.

[201] Materials Genome Initiative (2022) *About the Materials Genome Initiative*. Available at https://www.mgi.gov/about.

[202] America Makes (2021) *5511.001 Joint Metal Additive Database Definition (JMADD)*. Available at https://www.americamakes.us/projects/5511-001-joint-metal-additive-database-definition-jmadd/.

[203] MOU 225-22-025: Memorandum of Understanding: Streamlining Emerging Technology Medical Device Development Through Regulatory Tools Between Food and Drug Administration, U.S. Department of Health and Human Services and Veterans Health Administration's VA Ventures Within the U.S. Department of Veterans Affairs. U.S. Food and Drug Administration; Veterans Health Administration. September 27, 2022. Accessed December 06, 2022. https://www.fda.gov/about-fda/domestic-mous/mou-225-22-025.

[204] Small Business Administration (2022) *About - the SBIR and STTR Programs*. Available at https://www.sbir.gov/about.

[205] Small Business Administration (2022) *SBIR-STTR: Award Data - Analytic Dashboard*. Available at https://www.sbir.gov/analytics-dashboard.

[206] Manufacturing USA (2022) *Manufacturing USA*. Available at https://www.manufacturingusa.com/.

[207] Manufacturing USA (2022) *Institutes*. Available at https://www.manufacturingusa.com/institutes.

[208] America Makes (2021) *Technology Roadmap*. Available at https://www.americamakes.us/technology-roadmap/.

[209] Advanced Regenerative Manufacturing Institute (2022) *BioFabUSA: WHere Manufacturing Meets Science*. Available at https://www.armiusa.org/biofabusa/.

[210] IACMI (2021) *About Us - IACMI*. Available at https://iacmi.org/our-story/about-us/.

[211] Radford D (2021) Development of Additively Manufactured Complex Tools for Autoclave Cure Composites. https://iacmi.org/wp-content/uploads/2022/01/IACMI-4.9-Final-Report-12-20-21-approved.pdf.

[212] Lightweight Innovations for Tomorrow (2021) *Our Work: We Solve the Manufacturing Equation*. Available at https://lift.technology/our-work/.

[213] Lightweight Innovations for Tomorrow (2022) *Technology: Leading Innovations for Tomorrow*. Available at https://lift.technology/technology/.

[214] MxD (2022) *Future Factory*. Available at https://www.mxdusa.org/focus-areas/future-factory/.

[215] Everett, Hayley (2021) MxD Announces $1.5 Million Funding for Digital Manufacturing and Cybersecurity R&D Projects. *3D Printing Industry*, October 3,

2021. https://3dprintingindustry.com/news/mxd-announces-1-5-million-funding-for-digital-manufacturing-and-cybersecurity-rd-projects-197067/.

[216] National Institute for Innovation in Manufacturing Biopharmaceuticals (2021) *About NIIMBL*. Available at https://niimbl.force.com/s/about-niimbl.

[217] National Institute of Standards and Technology (2022) *Manufacturing Extension Partnership (MEP)*. Available at https://www.nist.gov/mep.

[218] National Institute of Standards and Technology (2020) *Advanced Manufacturing Technology Services/Industry 4.0*. Available at https://www.nist.gov/mep/advanced-manufacturing-technology-servicesindustry-40.

[219] National Institute of Standards and Technology (2022) *NIST Additive Manufacturing Material Database (AMMD)*. Available at https://ammd.nist.gov/.

[220] Lu, Yan, Paul Witherell, Alkan Donmez, and Jason Fox (2016) An Open Material Database for Additive Manufacturing, 2016. https://ammd.nist.gov/static/files/MST2016Poster.pdf.

[221] Department of Energy, Office of Technology Transitions (2019) Spotlight: Additive Manufacturing Building the Future Spotlght. https://www.energy.gov/sites/default/files/2019/07/f64/2019-OTT-Additive-Manufacturing-Spotlight_0.pdf.

[222] Oak Ridge National Laboratory (2022) *User Facilities: Manufacturing Demonstration Facility*. Available at https://www.ornl.gov/facility/mdf.

[223] Lawrence-Livermore National Laboratory (2020) Advanced Manufacturing Laboratory at Lawrence Livermore National Laboratory's Livermore Valley Open Campus. https://engineering.llnl.gov/sites/engineering/files/2020-06/AMLbrochure.pdf.

[224] Sandia National Laboratory (2022) *Pushing the Boundaries of Additive Manufacturing for National Security*. Available at https://www.sandia.gov/am/.

[225] Zelinski, Peter (2022) 10 Important Developments in Additive Manufacturing Seen at Formnext 2022 (Includes Video). *Additive Manufacturing*, November 30, 2022. https://www.additivemanufacturing.media/articles/10-important-developments-in-additive-manufacturing-seen-at-formnext-2022-includes-video.

[226] Yang L, Hsu K, Baughman B, Godfrey D, Medina F, Menon M, Wiener S (2017) *The Additive Manufacturing Supply Chain* (Springer, Cham). Available at https://link.springer.com/chapter/10.1007/978-3-319-55128-9_6.

[227] Jabil (2022) *The Future of 3D Printing: Five Predictions*. Available at https://www.jabil.com/blog/future-of-3d-printing-additive-manufacturing-looks-bright.html.

[228] Burton J (2022) *U.S. Geological Survey Releases 2022 List of Critical Minerals*. Available at https://www.usgs.gov/news/national-news-release/us-geological-survey-releases-2022-list-critical-minerals.

[229] Defense Logistics Agency (2022) *DLA Products*. Available at https://www.dla.mil/What-DLA-Offers/Products/.

[230] Ryder D (2018) *DLA Strategic Materials Partners with Research and Development*. Available at https://www.dla.mil/AboutDLA/News/NewsArticleView/Article/1674904/dla-strategic-materials-partners-with-research-and-development/.

[231] NSTC Fast Track Action Subcommittee on Critical and Emerging Technologies (2022) Critical and Emerging Technologies List Update. https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf.

[232] Department of Energy, Office of International Affairs (2022) *U.S. Departments of Energy, State and Defense to Launch Effort to Enhance National Defense Stockpile with Critical Minerals for Clean Energy Technologies*. Available at https://www.energy.gov/ia/articles/us-departments-energy-state-and-defense-launch-effort-enhance-national-defense.

[233] United States Council for Automotive Research (2021) *USCAR Announces Publication of "Roadmap for Automotive Additive Manufacturing"*. Available at https://uscar.org/news/uscar-announces-publication-of-a%EF%BF%BD%EF%BF%BDroadmap-for-automotive-additive-manufacturing/.

[234] Grand View Research (2021) 3D Printing Plastics Market Size, Share and Trends Analysis Report by Type (Photopolymers, ABS and ASA, Polyamide/Nylon, PLA), by FOrm, by End Use, by Region, and Segment Forecasts, 2022-2030 Report ID: GVR-2-68038-576-2. https://www.grandviewresearch.com/industry-analysis/3d-printing-plastics-market#.

[235] Kunovjanek M, Knofius N, Reiner G (2020). Additive Manufacturing and Supply Chains – a Systematic Review. *Production Planning & Control*. https://www.tandfonline.com/doi/full/10.1080/09537287.2020.1857874.

[236] Cunningham CR, Flynn JM, Shokrani A, Dhokia V, Newman ST (2018). Invited Review Article: Strategies and Processes for High Quality Wire Arc Additive Manufacturing. *Additive Manufacturing* 22:672–86. https://doi.org/10.1016/j.addma.2018.06.020.

[237] Huckstepp, Alex (2019) Powder Vs Wire – a Guide to Metal Additive Manufacturing by Digital Alloys - Manufactur3D. *Manufactur3D*, September 28, 2019. https://manufactur3dmag.com/powder-vs-wire-a-guide-to-metal-additive-manufacturing-by-digital-alloys/.

[238] Alogla AA, Baumers M, Tuck C, Elmadih W (2021). The Impact of Additive Manufacturing on the Flexibility of a Manufacturing Supply Chain. *Applied Sciences* 11(8):3707. https://doi.org/10.3390/app11083707.

[239] Bourell DL (2016). Perspectives on Additive Manufacturing. *Annu. Rev. Mater. Res.* 46(1):1–18. https://doi.org/10.1146/annurev-matsci-070115-031606.

[240] Legal Information Institute (2022) *Patent*. Available at https://www.law.cornell.edu/wex/patent.

[241] Vogel B (2016). Intellectual Property and Additive Manufacturing / 3D Printing: Strategies and Challenges of Applying Traditional IP Laws to a Transformative Technology. *Minnesota Journal of Law, Science & Technology* 17(2): 881. https://scholarship.law.umn.edu/mjlst/vol17/iss2/8.

[242] Federal Trade Commission (n.d.) Nixing the Fix: An FTC Report to Congress on Repair Restrictions. https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

[243] Mallinckrodt, Inc. V. Medipart, Inc., 976 F.2d 700 (Fed. Cir. 1992). US Court of Appeals for the Federal Circuit - 976 F.2d 700, August 29. Accessed August 29, 2022. https://law.justia.com/cases/federal/appellate-courts/F2/976/700/47378/.

[244] Legal Information Institute *Trade Secret*. Available at https://www.law.cornell.edu/wex/trade_secret.

[245] U.S. Congress (2016). Defend Trade Secrets Act of 2016. https://www.congress.gov/114/plaws/publ153/PLAW-114publ153.htm.

[246] U.S. Congress (n.d.) 18 U.S. Code § 1831 - Economic Espionage. https://www.law.cornell.edu/uscode/text/18/1831.

[247] Justia (2018) *Trade Dress*. Available at https://www.justia.com/intellectual-property/trademarks/trade-dress/.

[248] Graves LMG, Lubell J, King W, Yampolskiy M (2019). Characteristic Aspects of Additive Manufacturing Security from Security Awareness Perspectives. *IEEE Access* 7:103833–53. https://doi.org/10.1109/access.2019.2931738.

[249] Sofia Belikovetsky, Mark Yampolskiy, Jinghui Toh, Jacob Gatlin, Yuval Elovici *Dr0wned – Cyber-Physical Attack with Additive Manufacturing*. Available at https://www.usenix.org/conference/woot17/workshop-program/presentation/belikovetsky.

[250] National Defense Industrial Association's Manufacturing Division and Cyber Division (2014) Cybersecurity for Advanced Manufacturing. https://www.ndia.org/-/media/sites/ndia/policy/documents/cyber/cyber_for_manufacturing_white_paper_5may14.ashx?la=en.

[251] Freer, John Joseph, Richard Paul Messmer, Arvind Rangarajan, and David Robert Safford (2017). Methods and Systems for Implementing Distributed Ledger Manufacturing History.

[252] Voulpiotis, Filippos (2018) GE Patents Blockchain Technology for Additive Manufacturing. *3Dnatives*, July 6, 2018. https://www.3dnatives.com/en/ge-additive-blockchain060720184/.

[253] Inspector General, U.S. Department of Defense (2019) Audit of the DoD's Use of Additive Manufacturing for Sustainment Parts. https://media.defense.gov/2019/Oct/21/2002197659/-1/-1/1/DODIG-2020-003.PDF.

[254] Homeland Security Advisory Council (n.d.) Emerging Technologies Subcommittee Final Report of the Emerging Technologies Subcommittee 3D-Printing. https://www.dhs.gov/sites/default/files/publications/final_report_hsac_emerging_technology_subcommittee_3dprinting_508_compliant.pdf.

[255] Johnston T, Smith TD, Irwin JL (2018) Additive Manufacturing in 2040: Powerful Enabler, Disruptive Threat. Security 2040. https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE283/RAND_PE283.pdf.

[256] PART 738—COMMERCE CONTROL LIST OVERVIEW and the COUNTRY CHART. Code of Federal Regulations. https://www.govinfo.gov/content/pkg/CFR-2018-title15-vol2/xml/CFR-2018-title15-vol2-part738.xml.

[257] SUBCHAPTER M—INTERNATIONAL TRAFFIC in ARMS REGULATIONS. Code of Federal Regulations. https://www.govinfo.gov/content/pkg/CFR-2016-title22-vol1/xml/CFR-2016-title22-vol1-chapI-subchapM.xml.

[258] Code of Federal Regulations (2022) *22 CFR Part 121 -- the United States Munitions List*. Available at https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-121.

[259] Bureau of Industry and Security (2022) *Export Administration Regulations (EAR)*. Available at https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear.

[260] Fried S (2019) *The Future of Additive Manufacturing in Engineering*. Available at https://www.nano-di.com/resources/blog/2019-the-future-of-additive-manufacturing-in-engineering.

[261] Abdallah YO, Shehab E, Al-Ashaab A (2021) *Towards Managing Digital Transformation in Manufacturing Industry: Theoretical Framework* (IOS Press, Derby, UK). https://dspace.lib.cranfield.ac.uk/handle/1826/17126.

[262] AMFG (2021) 5 Trends Shaping the Future of Additive Manufacturing (2021). *AMFG*, February 18, 2021. https://amfg.ai/2021/02/18/trends-shaping-the-future-of-additive-manufacturing/.

[263] Küpper, Daniel, Wilderich Heising, Thomas Krüger, Andreas Gocke, and Amit Ganeriwalla (2019) Surviving Disruption in Additive Manufacturing. *BCG Global*, January 7, 2019. https://www.bcg.com/publications/2019/surviving-disruption-additive-manufacturing.

Appendix P. Abbreviations

2D	two-dimensional
3DCP	3D concrete printing
3DP	three-dimensional printing
AAMI	Association for the Advancement of Medical Instrumentation
ACES	Automated Construction of Expeditionary Structures
ACI	American Concrete Institute
ADAPT	Alliance for the Development of Additive Processing Technologies
AFRL	Air Force Research Laboratory
AIA	Aerospace Industries Association
AM CoE	ASTM Additive Manufacturing Center of Excellence
AM	additive manufacturing
AMC	Additive Manufacturing Consortium
AMDC	Additive Manufacturing Data Consortium
AMMD	Additive Manufacturing Materials Database
AMSC	Additive Manufacturing Standardization Collaborative
ANSI	American National Standards Institute
ARPA-E	Advanced Research Projects Agency–Energy
ASCE	American Society of Civil Engineers
ASME	American Society of Mechanical Engineers
ASTM	ASTM International
AWS	American Welding Society
BAAM	Big Area Additive Manufacturing
CAD	computer-aided design
CAMT	Center for Aerospace Manufacturing Technologies
CDRH	Center for Devices and Radiological Health
CPSC	Consumer Products Safety Commission
DOC	U.S. Department of Commerce
DoD	Department of Defense
DOE	U.S. Department of Energy
EPA	Environmental Protection Agency
FAA	Federal Aviation Administration
FCC	Federal Communications Commission
FDA	U.S. Food and Drug Administration
FEMA	Federal Emergency Management Agency
FMCSA	Federal Motor Carrier Safety Administration
FMVSS	Federal Motor Vehicle Safety Standards
GRC	GE Global Research Center
GSA	General Services Administration
HHS	U.S. Department of Health and Human Services
IBC	International Building Code
ICC	International Code Council
IEEE	Institute for Electrical and Electronics Engineers

IP	intellectual property
IPC	Association Connecting Electronics Industries
ISO	International Organization for Standardization
IWT-PRAM	Interagency Writing Team on Performance and Reliability of Advanced Manufactured Parts
JMADD	Joint Metal Additive Database Definition
LLNL	Lawrence Livermore National Laboratory
MDCS	Material Data Curation system
MDF	Manufacturing Demonstration Facility
MDPS	medical device production systems
MEP	Manufacturing Extension Partnership
MGI	Materials Genome Initiative
MMPACT	Moon-to-Mars Planetary Autonomous Construction Technologies
MMPDS	Metallic Materials Properties Development and Standardization
MPIF	Metal Powder Industries Federation
NASA	National Aeronautics and Space Administration
NCAME	National Center for Additive Manufacturing Excellence
NCDMM	National Center for Defense Manufacturing and Machining
NSTC	National Science and Technology Council
NEMA	National Electrical Manufacturers Association
NFPA	National Fire Protection Association
NHTSA	National Highway Traffic Safety Administration
NIAR	National Institute for Aviation Research
NIH	National Institutes of Health
NIST	National Institute of Standards and Technology
NITRD	Networking and Information Technology Research and Development
NNSA	National Nuclear Security Administration
NOCSAE	National Operative Committee on Standards for Athletic Equipment
NRC	Nuclear Regulatory Commission
NSF	National Science Foundation
OEM	original equipment manufacturer
OMB	U.S. Office of Management and Budget
ORNL	Oak Ridge National Laboratory
OSHA	Occupational Safety and Health Administration
POC	point-of-care
PPP	public-private partnership
R&D	research and development
RFID	radio-frequency identification
RSNA	Radiological Society of America
SAE	SAE International
SBIR	Small Business Innovation Research
SDO	standards development organization

DOS	U.S. Department of State
STPI	Science and Technology Policy Institute
STTR	Small Business Technology Transfer
TIA	Telecommunications Industry Association
TSCA	Toxic Substances Control Act
USCAR	United States Council on Automotive Research
USGS	United States Geological Survey
USPTO	United States Patent and Trademark Office
USTA	*Uniform Trade Secrets Act*
VA	Department of Veterans Affairs
VHA	Veterans Health Administration