NIST Cybersecurity & Privacy Program

FY 2024 Annual Report

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

NIST SPECIAL PUBLICATION 800-236

NIST Special Publication 800
NIST SP 800-236

Fiscal Year 2024 Annual Report for NIST Cybersecurity and Privacy Program

Patrick O'Reilly, Editor
Computer Security Division
Information Technology Laboratory

Kristina Rigopoulos, Editor
Applied Cybersecurity Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-236

April 2025

U.S. DEPARTMENT OF COMMERCE
Howard Lutnick, Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Craig Burkhardt, Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director

TABLE OF CONTENTS

FOREWORD

Back to the future. As we look back on our past fiscal year's work in cybersecurity and privacy, we can see the fruition of many long-standing efforts that will position us well in the changing times ahead.

NIST has set foundations to ensure our security and privacy now and into the future with new quantum-resistant encryption algorithms, updates to the NIST Cybersecurity Framework, and the establishment of Artificial Intelligence programs, testbeds, and research agendas. Our research has also demonstrated practical applications of our work that spans several key priority areas that are outlined in this report with hyperlinked pointers to help you dig deeper and learn more.

NIST's work aligns with and supports many national initiatives to protect our Nation, including the National Cybersecurity Strategy and its related Implementation Plan, new policies for federal agencies from the Office of Management and Budget, initiatives from the Office of the National Cyber Director, and response actions directed by the National Security Council. NIST leads many standards-setting organizations around the world and ensures that U.S. priorities, requirements, and technologies are at the forefront of standards activities. This enables the development of products and services that meet our needs and are unquestionably secure. We are proud of and excited about the relevance and impact of our work as we continue to protect our information, economy, and way of life.

We hope that you will take the time to review some of the key highlights of our cybersecurity and privacy accomplishments from FY 2024 and to explore some of our priorities, programs, and projects. You can learn about the many conferences and workshops we had in the last fiscal year by viewing the recordings or reading the event proceedings, and we invite you to participate directly with us in our upcoming events.

Most importantly, we look forward to learning more from you as we work together to address the challenges of today and journey into the future. As ever, we appreciate your support and hope that you are making the best possible use of NIST's work.

Matthew Scholl
Chief, Computer Security Division, NIST

Rodney Petersen
Interim Chief, Applied Cybersecurity Division, NIST

Cryptography

Credit: NIST

CRYPTOGRAPHY

**Cryptography is foundational to our security and data protection needs.
The standards, guidelines, recommendations, and tools provided by NIST's Cryptography priority area enable the trustworthy assurance of integrity and confidentiality in all types of information and technology — now and in the future.**

Major Accomplishments in FY 2024:

- NIST published the first three Federal Information Processing Standards (FIPS) for post-quantum cryptography. These standards specify key-establishment and digital signature schemes that are designed to resist future attacks by quantum computers, which threaten the security of current standards. The three algorithms specified in these standards are each derived from different submissions to the NIST Post-Quantum Cryptography (PQC) Standardization Project.
- The PQC team hosted the Fifth PQC Standardization Conference in April 2024. This conference discussed the finalization of the initial PQC FIPS and the ongoing evaluation of the Round 4 Public-Key Encryption and Key-Establishment Algorithms and the Additional Digital Signature Schemes that are being considered for future standardization.
- The Multi-Party Threshold Cryptography (MPTC) and Privacy-Enhancing Cryptography (PEC) projects jointly released the initial public draft of NIST Internal Report (IR) 8214C, *NIST First Call for Multi-Party Threshold Schemes* (MPTS). The document's scope includes advanced techniques, such as fully homomorphic encryption, zero-knowledge proofs, and the building blocks of secure multi-party computation. As part of an effort to obtain public comments, NIST hosted the MPTS 2023 workshop and three events of the Special Topics on Privacy and Public Auditability (STPPA).
- NIST's Crypto Publication Review Board completed seven publication reviews, and five reviews are in progress to update and modernize the portfolio of cryptographic standards.

Learn more about this priority area

Education & Workforce

Credit: Florida International University

EDUCATION & WORKFORCE

The Education and Workforce priority area energizes, promotes, and coordinates a robust community that works together to advance an integrated ecosystem of cybersecurity education, training, and workforce development.

Major Accomplishments in FY 2024:

- A major update to the NICE Framework was released as the Version 1.0.0 Components, which incorporated changes to almost every level of the NICE Framework's structure and includes a list of 11 learner-focused Competency Areas. The new Components were released in multiple data formats, including as part of NIST's Cybersecurity and Privacy Reference Tool.
- NIST released two new resources in support of the NICE Strategic Plan Goal 4.6: "Expand international outreach to promote the NICE Framework and document approaches being used in other countries." The new NICE Framework components have been translated into five languages, and a list of international Cybersecurity Skills and Workforce Frameworks is now available. The list includes a representative sample of cybersecurity, cyber-related, digital literacy skills, and workforce frameworks from countries around the world.
- The NICE Community Coordinating Council's Promote Career Discovery Working Group launched the Cybersecurity Career Ambassador Program. The Transform Learning Process Working Group published the Landscape of Performance-Based Assessments in Cybersecurity.
- The Cybersecurity Education and Workforce Group published an update to NIST Special Publication (SP) 800-50r1 (Revision 1), *Building a Cybersecurity and Privacy Learning Program*.
- The Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) Cybersecurity Education and Workforce Development Program awarded cooperative agreements totaling nearly $6.6 million aimed at building the workforce needed to safeguard enterprises from cybersecurity risks. The grants of roughly $200,000 apiece were distributed to 33 education and community organizations in 22 states that are working to address the nation's shortage of skilled cybersecurity employees. Learn more about the RAMPS Communities.
- Several events were held throughout FY 2024, including the NICE Conference, K12 Conference, RICET, webinars, and FISSEA.

Learn more about this priority area

Emerging Technology

Credit: Shutterstock

EMERGING TECHNOLOGY

The rapid evolution of technology brings extraordinary opportunities and unavoidable challenges. NIST's cybersecurity researchers study these emerging technologies to understand their security and privacy capabilities, vulnerabilities, configurations, and overall structures to develop standards, guidelines, and references for improving their approaches before they are deployed.

Major Accomplishments in FY 2024:

- NIST released the final version of AI 100-2 E2023, *Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations*.
- SP 800-218A, *Secure Software Development Practices for Generative AI and Dual-Use Foundation Models: An SSDF Profile*, augments the secure software development practices identified in SP 800-218, *Secure Software Development Framework (SSDF)* with recommendations, considerations, notes, and informative references that are specific to generative AI and dual-use foundation model development.
- NIST launched a project to investigate immersive technologies and their potential cybersecurity and privacy considerations. The findings will inform a possible roadmap for NIST competencies around these technologies, focusing on cybersecurity and privacy risk management.
- NIST IR 8425A, *Recommended Cybersecurity Requirements for Consumer-Grade Router Products*, comprehensively maps router cybersecurity standards provisions to the NIST baseline.
- NIST held an open discussion forum and released the initial public draft of Cybersecurity White Paper (CSWP) 33, *Product Development Cybersecurity Handbook for IoT Product Manufacturers*, which describes considerations for developing and deploying secure IoT products across sectors and use cases and extends NIST's work to consider the cybersecurity of IoT product component configurations.
- NIST led the IoT Interagency Federal Working Group and collaborated with the IoT Advisory Board as it developed findings and recommendations on how the U.S. can reduce barriers to adopting IoT technologies. The findings were documented in a September 2024 report.

Learn more about this priority area

Human-Centered Cybersecurity

Credit: Shutterstock

HUMAN-CENTERED CYBERSECURITY

The mission of the Human-Centered Cybersecurity priority area is to "champion the human in cybersecurity." Through research and other human-centered projects, the program team seeks to better understand and improve people's cybersecurity interactions, perceptions, and behaviors to empower them to be active, informed participants in cybersecurity.

Major Accomplishments in FY 2024:

- The phishing project team published the NIST Phish Scale User Guide handbook on applying the Phish Scale — a novel method for measuring socially engineered email attacks. The guide has been downloaded over 20,000 times since its release. The Phish Scale is used in public- and private-sector organizations around the world to aid those who manage phishing awareness training programs in enhancing training effectiveness and strengthening organizations' security postures.
- The youth security and privacy project team continued participation in the White House Kids Online Health and Safety (KOHS) Task Force. NIST provided technical expertise and worked with multi-agency colleagues in three task force working groups to deliver a first-of-its-kind report, Best Practices for Families and Guiddlines for Industry. This report includes: (1) best practices for parents and caregivers to promote youth online health, safety, and privacy; (2) recommended industry practices; (3) a research agenda that identifies domains of further inquiry; and (4) recommended next steps for policymakers.
- NIST published results from practitioner and researcher survey studies that explored how human-centered cybersecurity concepts can be better integrated into practice and how practitioners can better inform human-centered cybersecurity research. To address some of the challenges identified in the studies, NIST launched the Human-Centered Cybersecurity Community of Interest, an online forum that brings practitioners and researchers together to share perspectives and facilitate collaboration. NIST also co-sponsored and served on the organizing committee for ConnectCon, an interactive workshop that brings together cybersecurity experts from academia, industry, and government to identify and discuss the most pressing human-centered cybersecurity challenges that organizations face today.

Learn more about this priority area

Identity & Access Management

Credit: NIST

IDENTITY & ACCESS MANAGEMENT

Identity and Access Management (IAM) is the cornerstone of data protection, privacy, and security. NIST's IAM priority area provides research, guidelines, and technology transition activities to help ensure that the right humans, devices, data, and processes have the right access to the right resources at the right time.

Major Accomplishments in FY 2024:

- After adjudicating nearly 4,000 comments, NIST published a second public draft of all four volumes of SP 800-63-4, *Digital Identity Guidelines*, which provide a foundation for the inclusion of new techniques and technologies into federal IAM programs.
- NIST's IAM team published updates to the suite of SP 800-73-5 documents, which specify the *Interfaces of Personal Identity Verification (PIV) Credentials* (Part 1), (Part 2), and (Part 3), and completed updates to SP 800-78-5, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*.
- NIST continuously updates the Face Recognition/Analysis Technology Evaluation (FRTE/FATE) to provide critical benchmarking for emerging applications of facial recognition and analysis. NIST IR 8525: *Face Analysis Technology Evaluation: Age Estimation and Verification*, was also released to evaluate the ability of face analysis to estimate age based on a subject's face image, which is something essential to emerging age verification schemes.
- NIST established an NCCoE project and Cooperative Research and Development Agreement (CRADA) consortium comprised of over 20 commercial and government partners to focus on creating implementation guidelines for the use of Cryptographically Verifiable Digital Credentials for online services.
- NIST's IAM team contributed to the final version of the Mobile Driving License Application standard (ISO/IEC 18013-7) and updated their reference implementation for the standard to facilitate testing and the certification of products.

Learn more about this priority area

Privacy

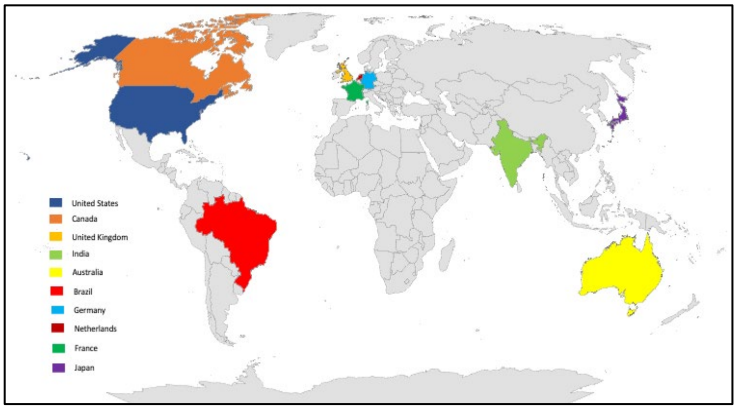
Credit: Shutterstock

PRIVACY

Privacy is integral to the trust that supports the growth of the digital economy and improves our quality of life. NIST has prioritized Privacy Engineering to support measurement science and system engineering principles through frameworks, risk models, and guidelines that protect privacy and civil liberties.

Major Accomplishments in FY 2024:

- NIST released the initial public draft of [SP 800-226, *Guidelines for Evaluating Differential Privacy Guarantees*]. This publication focuses on differential privacy — a privacy-enhancing technology that quantifies privacy risks to individuals when their information appears in a dataset.
- NIST held the Ready, Set, Update! Privacy Framework 1.1 + Data Governance and Management (DGM) Profile Workshop to inform an update of the NIST Privacy Framework to Version 1.1 and the development of the DGM Profile. NIST also released concept papers for the Privacy Framework, Version 1.1 and the DGM Profile in advance of the workshop.
- NIST published Diverse Community Data for Benchmarking Data Privacy Algorithms to disseminate major findings from the Collaborative Research Cycle (CRC) — a community challenge to evaluate de-identification algorithms.
- NIST released the Collaborative Research Cycle (CRC) Data and Metrics Archive, which is the largest global synthetic data evaluation ever performed—and an ongoing program that leads advancements in synthetic data technology. The program has over a dozen citations and has been featured in multiple conferences and workshops.



Credit: NIST

62,214 NIST Privacy Framework downloads in FY24 (Approx 29% increase from FY23)

Top 10 Countries – Privacy Framework Total Downloads

Learn more about this priority area

Risk Management

Credit: Shutterstock

RISK MANAGEMENT

Enabling effective risk management is the foundation and goal of the entire NIST cybersecurity and privacy portfolio — from cryptographic algorithm standards to enterprise risk management guidelines. Using NIST risk management resources, organizations can better understand risks, select and implement appropriate countermeasures, measure effectiveness, and implement continuous monitoring and improvement.

Major Accomplishments in FY 2024:

- NIST published the Cybersecurity Framework (CSF) Version 2.0 in February 2024 after a process of extensive stakeholder collaboration. New implementation resources were published to accompany the Framework, including profiles, quick start guides, and informative references. NIST also worked with stakeholders around the world to translate and verify international translations of the CSF and associated resources.
- NIST used the SP 800-53 Public Comment Site to propose new controls, hold a public comment period, and issue revised controls and assessment procedures within 30 days in response to a gap in the control catalog.
- Additional resources for implementers were released, including a series of free, self-paced online introductory courses on security and privacy controls, assessment procedures, control baselines, and the NIST Risk Management Framework for Small Enterprises Quick Start Guide (QSG).
- NIST continued to lead and support community engagement on cybersecurity supply chain risk management (C-SCRM) through the Software and Supply Chain Assurance (SSCA) Forum and Engineering Biology Research Consortium Workshops, support the Federal Acquisition Security Council, and issued two QSGs on establishing a C-SCRM capability using the CSF 2.0 and conducting due diligence on potential suppliers before procurement.
- NIST released beta prototypes of the Cyber Incident Data Analysis Repository and Cyber Supply Chain Survey Tool for stakeholder feedback and improvement. The prototypes are designed to anonymously collect and share cybersecurity incident and supply chain data for measurement and metrics analytics and to provide users with educational and informative resources to improve their C-SCRM.

Learn more about this priority area

Trusted Networks & Platforms

Credit: Shutterstock

TRUSTED NETWORKS & PLATFORMS

We all rely on the hardware, software, and networks that form the fabric of our digital ecosystems. NIST's Trusted Networks and Platforms priority area supports foundational and applied research and practical implementation guidelines and standards to ensure secure, reliable, and resilient technology across industry sectors.

Major Accomplishments in FY 2024:

- NIST launched the hardware security program to identify existing and emerging cybersecurity threats and develop mitigation techniques for semiconductors, including cybersecurity and supply chain standards, guidelines, and recommended practices in collaboration with the semiconductor community. NIST also hosted a Supply Chain workshop and published NIST IR 8540, *Report on Secure Hardware Assurance Reference Dataset Program*.
- To support data safeguarding, NIST released NIST IR 8432, *Cybersecurity of Genomic Data*; SP 1800-28, *Data Confidentiality: Identifying and Protecting Assets Against Data Breaches*; SP 1800-29, *Data Confidentiality: Detect, Respond to, and Recover from Data Breaches*; and NIST IR 8496, *Data Classification Concepts and Considerations for Improving Data Protection*.
- NIST published SP 1800-38B, *Migration to Post-Quantum Cryptography (PQC) Quantum Readiness: Cryptographic Discovery*, and SP 1800-38C, *Migration to PQC Quantum Readiness: Testing Draft Standards*.
- NIST published SP 800-231, *Bugs Framework (BF): Formalizing Cybersecurity Weaknesses and Vulnerabilities*; SP 800-204D, *Strategies for the Integration of Software Supply Chain Security in DevSecOps CI/CD Pipelines*; SP 800-218A, *Secure Software Development Practices for Generative AI and Dual-Use Foundation Models: An SSDF Community Profile*; and enhanced the Software Assurance Reference Dataset (SARD) with four test suites from the Static Analysis Tool Exposition (SATE) VI. NIST also improved the AI Bug Finder, and the National Software Reference Database added data from 10,000+ new or updated applications (totaling over 42 million files) to assist with computer security and digital forensics analysis.
- NIST published CSWP 36, *Applying 5G Cybersecurity and Privacy Capabilities: Introduction to the White Paper Series*; CSWP 36A, *Protecting Subscriber Identifiers with Subscription Concealed Identifier (SUCI): Applying 5G Cybersecurity and Privacy Capabilities*; CSWP 36B, *Using Hardware-Enabled Security to Ensure 5G System Platform Integrity: Applying 5G Cybersecurity and Privacy Capabilities*; and CSWP 36C, *Reallocation of Temporary Identities: Applying 5G Cybersecurity and Privacy Capabilities*.

Learn more about trusted networks and platforms

National Cybersecurity Center of Excellence Activities

Credit: NIST

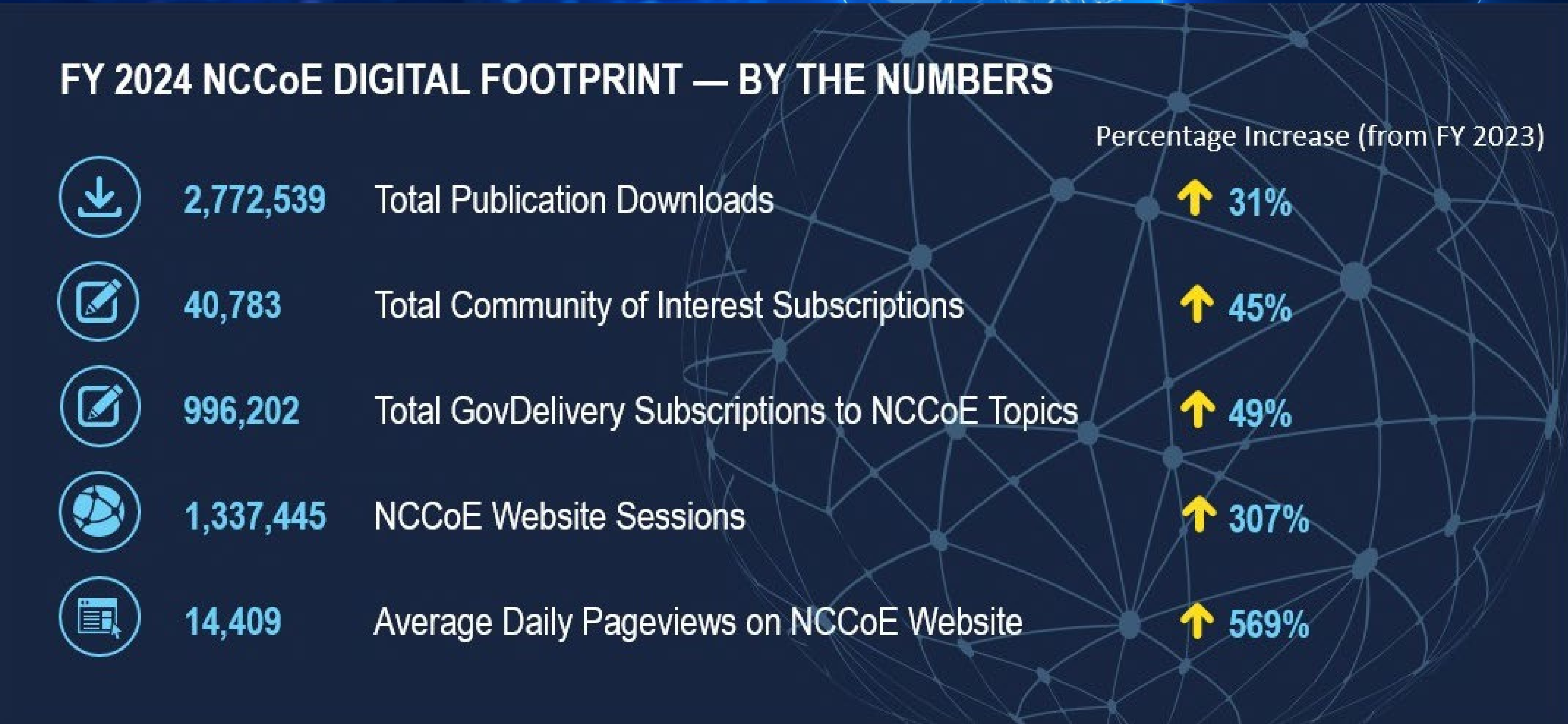
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE ACTIVITIES

The mission of the National Cybersecurity Center of Excellence (NCCoE) is to accelerate the adoption of secure technologies. The NCCoE works collaboratively with industry and other government agencies to address cybersecurity challenges facing the nation by demonstrating the use of commercial technologies and standards.

Major Accomplishments in FY 2024:

- NIST received approval to continue sponsorship of the National Cybersecurity Federally Funded Research and Development Center (FFRDC), which is now in its tenth year.
- The NCCoE held 167 active Cooperative Research and Development Agreements (CRADAs) in 2024 with industry, government, and academic organizations to provide in-kind contributions of technology and expertise toward NCCoE projects. New consortia were established for water cybersecurity and mobile driver's license projects, and the migration to post-quantum cryptography consortium grew to over 40 organizations. The NCCoE announced new collaborations with SEMI on semiconductor manufacturing cybersecurity and Hudson Alpha and the University of Alabama in Huntsville on the cybersecurity and privacy of genomic data. NCCoE had a cumulative total of 758 collaborators working on NCCoE projects, with 26,714 companies and organizations producing cybersecurity guides and other products.
- The NCCoE partnered with 39 National Cybersecurity Excellence Partners (NCEPs) and led U.S. organizations to provide insights into emerging cybersecurity and privacy technology issues. Joint meetings of the NCEPs were hosted by the NCCoE, Dell, and Cloudflare. The NCCoE also held Interagency Agreements with the Department of State, the U.S. Navy, and the U.S. Space Force.
- The NCCoE released 25 publications — including NIST 1800-Series Special Publications, Interagency Reports, Cybersecurity White Papers, and new GitHub publications — to provide guidelines for data security, genomic data cybersecurity and privacy, zero trust architectures, 5G cybersecurity, post-quantum cryptography migration, data classification practices, supply chain traceability, smart inverters, water cybersecurity, and more.
- The NCCoE introduced a new series of 5G Cybersecurity White Papers to offer short-form content that is easy to digest for a broader audience. Other outputs included the NIST Dioptra AI open-source test platform and GitHub Pages for several projects.

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE ACTIVITIES



FY 2024 NCCoE DIGITAL FOOTPRINT — BY THE NUMBERS

		Percentage Increase (from FY 2023)
2,772,539	Total Publication Downloads	↑ 31%
40,783	Total Community of Interest Subscriptions	↑ 45%
996,202	Total GovDelivery Subscriptions to NCCoE Topics	↑ 49%
1,337,445	NCCoE Website Sessions	↑ 307%
14,409	Average Daily Pageviews on NCCoE Website	↑ 569%

- The NCCoE increased its efforts on CSF 2.0 Community Profiles to help organizations implement the new CSF.

- The NCCoE held 17 events and webinars in FY 2024, including CSF 2.0 Community Profile webinars, and continued to host quarterly Cybersecurity Connections networking events for the small business community in partnership with the State of Maryland (MD) and Montgomery County, MD. The NCCoE also launched a new LinkedIn page and the NCCoE Speakers Corner to increase awareness of the Center.

- The NCCoE continued its summer internship program for undergraduate and graduate students for the 14th year. The NCCoE also participated in NIST's Summer Institute to provide cybersecurity resources to middle school teachers.

- The NCCoE continued to expand its cybersecurity and privacy topics, including post-quantum cryptography, natural language processing, trusted IoT, resilience for critical infrastructure and supply chains, and NIST Framework resources and tools.

Learn more about this priority area

Events & Stakeholder Engagement

Credit: NIST

EVENTS & STAKEHOLDER ENGAGEMENT

NIST cybersecurity and privacy events are rooted in collaboration, information sharing, and transparency. By hosting events, NIST can directly interact with broad audiences and share information about a wide range of topics on a continuous basis.

- The NIST Cybersecurity and Privacy Program hosted over 80 events in FY 2024, including conferences, workshops, collaborative meetings, webinars, panel discussions, forums, and working groups.
- NIST worked closely with event attendees to share information, collaborate with the public, and hold active discussions with cybersecurity and privacy experts across sectors and industries. These open discussions and collaborative interactions helped inform NIST's work, and the events streamlined NIST's information-sharing abilities with key audiences.
- NIST's cybersecurity and privacy event details are located on websites across our NCCoE events page, CSRC events page, and our NIST events overview page.

FY 2024 event topics included:

Cryptography	**Education and Workforce**	**Identity and Access Management**	**Internet of Things**	**NIST Frameworks**
Privacy	**Risk Management**	**Securing Emerging Technologies**	**Small Businesses**	**Software**

Learn more about this priority area

OPPORTUNITIES TO ENGAGE WITH NIST ON CYBERSECURITY & PRIVACY

NIST depends on developers, researchers, and everyday users of technologies and information to guide cybersecurity and privacy focus areas.

- Details on engaging with NIST are available here.
- Many NIST projects are supported by guest researchers, both foreign and domestic.
- The Pathways Program supports Federal Government internships for students and recent graduates.
- NIST funds industrial and academic research in several ways:
  - The Small Business Innovation Research Program (SBIR) funds research and development proposals.
  - NIST offers grants to encourage work in the fields of precision measurement, fire research, and materials science. For general information on NIST's grant programs, please contact Christopher Hunton at grants@nist.gov.
  - The Information Technology Laboratory (ITL) Speakers Bureau enables engagement with universities and colleges to raise student and faculty awareness about the exciting work going on at NIST and motivate them to consider pursuing opportunities to work with ITL.
- More information about NIST's research, projects, publications, and events can be found on the NIST Computer Security Resource Center (CSRC) website and the NIST Cybersecurity website.

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

How to Cite this NIST Technical Series Publication

O’Reilly PD, II, Rigopoulos KG (2025) Fiscal Year 2024 Annual Report for NIST Cybersecurity and Privacy Program. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-236. https://doi.org/10.6028/NIST.SP.800-236

Disclaimer

Any mention of commercial products or organizations is for informational purposes only; it is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the products identified are necessarily the best available for the purpose.

Contact Information

cyber@nist.gov

Abstract

Throughout Fiscal Year 2024 (FY 2024) — from October 1, 2023, through September 30, 2024 — the NIST Information Technology Laboratory (ITL) Cybersecurity and Privacy Program successfully responded to numerous challenges and opportunities in security and privacy. This Annual Report highlights the ITL Cybersecurity and Privacy Program's FY 2024 research activities, including the ongoing participation and development of international standards, research, and practical applications in several key priority areas (e.g., post-quantum cryptography, NIST Cybersecurity Framework [CSF 2.0], and new CSF profiles), improved software and supply chain cybersecurity, work on IoT cybersecurity guidelines, National Cybersecurity Center of Excellence (NCCoE) projects, a new comment site for NIST's Risk Management Framework, the release of a Phish scale, progress in the Identity and Access Management program, and Strategic and Emerging Research Initiatives (SERI) for autonomous vehicles.

Keywords

annual report; 2024 annual report; cybersecurity; cybersecurity program; cybersecurity and privacy program; Federal Information Security Modernization Act; FISMA; information security; Information Technology Laboratory; ITL; privacy; program accomplishments; program highlights; project accomplishments; project highlights.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.