NIST Internal Report
NIST IR 8183r2 ipd

Cybersecurity Framework 2.0 Manufacturing Profile

Initial Public Draft

Keith Stouffer
Michael Pease
CheeYee Tang
Timothy Zimmerman
Michael Thompson
Aslam Sherule
Zackary Louis Silva
Karen Quigg
Tom Cottle

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8183r2.ipd

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

NIST Internal Report
NIST IR 8183r2 ipd

Cybersecurity Framework 2.0 Manufacturing Profile

Initial Public Draft

Keith Stouffer
Michael Pease
CheeYee Tang
Timothy Zimmerman*
Smart Connected Systems Division
Communications Technology Laboratory

Michael Thompson
Aslam Sherule
Zackary Louis Silva
Karen Quigg
The MITRE Corporation

*Former NIST employee; all work for this publication was done while at NIST.

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8183r2.ipd

September 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

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

NIST Technical Series Policies
Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Publication History
Approved by the NIST Editorial Review Board on YYYY-MM-DD [Will be added to final publication.]
Supersedes NIST Series XXX (Month Year) DOI [Will be added to final publication, if applicable.]

How to Cite this NIST Technical Series Publication
Stouffer K, Pease M, Tang CY, Zimmerman T, Thompson M, Sherule A, Silva ZL, Quigg K (2025) Cybersecurity Framework Version 2.0 Manufacturing Profile. (National Institute of Standards and Technology, Gaithersburg, MD), NIST IR (Internal Report)) NIST IR 8183r2 ipd. https://doi.org/10.6028/NIST.IR.8183r2.ipd

Author ORCID iDs
Keith Stouffer: 0000-0003-1220-5487
Michael Pease: 0000-0002-6489-2621
CheeYee Tang: 0009-0000-2847-1443
Timothy Zimmerman: 0000-0001-8451-0515
Michael Thompson: 0000-0002-0836-244X
Aslam Sherule: 0000-0002-2003-3817
Zackary Louis Silva: 0000-0002-0721-1420
Karen Quigg: 0009-0004-4713-1128

Public Comment Period
September 29, 2025 – November 17, 2025

Submit Comments
CSF_Manufacturing_Profile@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Additional Information

Additional information about this publication is available at https://csrc.nist.gov/pubs/ir/8183/r2/ipd, including related content, potential updates, and document history.

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

This document provides the Cybersecurity Framework (CSF) Version 2.0 Community Profile developed for supporting manufacturing environments. This "Manufacturing Profile" is aligned with manufacturing sector goals and industry best practices and can be used as a roadmap for reducing cybersecurity risk for manufacturers. The Manufacturing Profile provides a voluntary, risk-based approach for managing cybersecurity activities and reducing cyber risk to manufacturing systems and is meant to enhance but not replace current cybersecurity standards and industry guidelines.

Keywords

Computer security; Cybersecurity Framework (CSF); operational technologies (OT); industrial control systems (ICS); information security; manufacturing; network security; risk management; security controls; distributed control systems (DCS); programmable logic controllers (PLC); supervisory control and data acquisition (SCADA) systems.

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.

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

   i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or

   ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: CSF_Manufacturing_Profile@nist.gov

Table of Contents

List of Tables

Acknowledgments

The authors gratefully acknowledge and appreciate the significant contributions from individuals and organizations in the public and private sectors, whose thoughtful and constructive comments improved the overall quality, thoroughness, and usefulness of this publication.

Executive Summary

This document provides a Cybersecurity Framework 2.0 Community Profile created for manufacturing environments. This "Manufacturing Profile" aligns with manufacturing sector goals and industry best practices and can serve as a guide for reducing cybersecurity risks for manufacturers.

The Profile gives manufacturers:

- A method to identify opportunities for improving the current cybersecurity posture of the manufacturing system
- An evaluation of their ability to operate the manufacturing environment at their acceptable risk level
- A standardized approach to preparing the cybersecurity plan for ongoing assurance of the manufacturing system's security

The Profile is structured around the functional areas of the Cybersecurity Framework 2.0: Govern, Identify, Protect, Detect, Respond, and Recover. These main areas form a foundation for developing manufacturer-specific or sector-specific profiles to support different levels of manufacturing operational criticality (e.g., Low, Moderate, and High).

This Manufacturing "Target" Profile aims to guide organizations in achieving key cybersecurity outcomes by providing a roadmap to identify opportunities for improving the cybersecurity of manufacturing systems. It offers a voluntary, risk-based approach for managing cybersecurity activities and lowering cyber risks to manufacturing systems. This profile is meant to supplement, not replace, existing cybersecurity standards and industry guidelines that the manufacturer adopts.

1. Introduction

Executive Order 13636, “Improving Critical Infrastructure Cybersecurity,” [1] directed the development of the voluntary CSF that provides a prioritized, flexible, repeatable, performance-based, and cost-effective approach to manage cybersecurity risk for those processes, information, and systems directly involved in the delivery of critical infrastructure services. Executive Order 13800 [2] expands the use of the CSF to federal agencies, requiring them to use it to manage their cybersecurity risk. In response, NIST has established the Cybersecurity Framework 2.0 (CSF) [3] to help organizations of all sizes and sectors manage and reduce their cybersecurity risks.

This CSF Community Profile uses a common language to address and manage cybersecurity risks for manufacturing organizations. Specifically, the Manufacturing Community Profile (Profile) outlines specific cybersecurity activities and outcomes to protect a manufacturing system, its components, facilities, and environment. Using the Profile, manufacturers can align cybersecurity efforts with business needs, risk tolerances, and available resources. The Profile recognizes that each organization has both common and unique risks, varying risk appetites and tolerances, specific missions, and objectives to achieve those missions and offers a manufacturing sector-specific approach to cybersecurity based on standards, guidelines, and industry best practices.

1.1. Purpose & Scope

This document represents a CSF Community Profile that describes shared interests, goals, and outcomes for reducing cybersecurity risk among several organizations. Community Profiles provide a way to reflect a consensus point of view about cybersecurity risk management. Organizations in the community can use a Community Profile as the basis of, or to inform, their Organizational Target Profiles. Some communities may develop more than one Community Profile, based on the scope of their needs [3].

This Profile provides a voluntary, risk-based approach to managing cybersecurity activities and reducing cyber risk to manufacturing systems. It maps the CSF Subcategories with implementation guidance based on the criticality of the manufacturing systems and processes. Additionally, the Profile provides an opportunity for improving the current cybersecurity posture of manufacturing systems by allowing organizations to establish a common language and set of expectations that support comparing the target and current cybersecurity posture. These gap analyses can then be utilized by organizations to plan and prioritize remediation efforts to achieve cybersecurity risk management objectives.

1.2. Audience

This document covers details specific to manufacturing systems. Readers of this document should be acquainted with industrial control systems (ICS), general computer security concepts, and communication protocols such as those used in networking. The intended audience is varied and includes the following:

- Control engineers, integrators, and architects who design or implement secure manufacturing systems.
- System administrators, Network administrators, cybersecurity personnel, physical security, and OT operators and engineers who administer, patch, or secure manufacturing systems and environments.
- Managers who are responsible for manufacturing systems.
- Senior management who are trying to understand implications and consequences as they justify and implement a manufacturing systems cybersecurity program to help mitigate impacts to business functionality.
- Researchers, academic institutions, and analysts who are trying to understand the unique security needs of manufacturing systems.

1.3. Document Structure

The remainder of this guide is divided into the following major sections:

- Section 2 provides an overview of manufacturing systems.
- Section 3 provides an overview of the *NIST Cybersecurity Framework 2.0*.
- Section 4 discusses the Manufacturing Profile development approach.
- Section 5 provides the manufacturing specific guidance for the CSF subcategories.
- References provide a list of references used in the development of this document.
- Appendix A provides a list of acronyms and abbreviations used in this document.
- Appendix B provides a glossary of terms used in this document.
- Appendix C provides a change log for revisions of the Profile.

2. Overview of Manufacturing Systems

Manufacturing systems represent different types of control systems (e.g., supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), programmable logic controllers (PLCs)) and are often found in the industrial sectors and critical infrastructures. Manufacturing systems usually include a mix of control components (e.g., electrical, mechanical, hydraulic, and pneumatic) that work together to fulfill an industrial goal (like manufacturing or transporting matter or energy). These ICSs support the large and diverse manufacturing industrial sector and can be categorized as either *process-based, discrete-based,* or a combination of both [4].

Process-based manufacturing industries typically utilize two main process types:

- **Continuous Manufacturing Processes.** These processes run continuously, often with phases to make different grades of a product. Typical continuous manufacturing processes include fuel or steam flow in a power plant, petroleum in a refinery, and distillation in a chemical plant.
- **Batch Manufacturing Processes.** These processes have distinct processing steps, conducted on a quantity of material. There is a distinct start and end to a batch process with the possibility of brief steady state operations during intermediate steps. Typical batch manufacturing processes include food, beverage, and biotech manufacturing.

Discrete-based manufacturing industries typically conduct a series of operations on a product to create a distinct product. Electronic and mechanical parts assembly and parts machining are typical examples of this type of industry. Both process-based and discrete-based industries utilize similar types of control systems, sensors, and networks. Some facilities are a hybrid of discrete and process-based manufacturing.

Additionally, manufacturers must also manage the supply chain for both technology-based inputs used in their final products (e.g., PLCs, sensors, robotics, data collection systems, and other information technologies), technology-based products used by the organization, and non-technology input products (e.g., non-IT components manufactured by third-party suppliers that are used to manufacture the final product).

The Manufacturing sector of the critical infrastructure community includes public and private owners and operators, along with other entities operating in the manufacturing domain. Members of this distinct sector perform functions that are supported by OT and IT. This reliance on technology, communication, and the interconnectivity of OT and IT has changed and expanded the potential vulnerabilities and increased the potential risk to manufacturing system operations.

3. Overview of the Cybersecurity Framework

The manufacturing sector is a critical component of the global economy, and its cybersecurity is essential to ensuring the reliability and safety of production systems. This Community Profile is based on the NIST Cybersecurity Framework (CSF) 2.0 [3], which provides a flexible and risk-based approach to managing cybersecurity.

The CSF helps organizations of any size, sector, or level of cyber maturity address their unique cybersecurity risks while improving communication and collaboration across stakeholders. For the manufacturing community, the CSF provides a foundation to:

- Establish a common understanding of cybersecurity risks, threats, and priorities.
- Align on desired outcomes and target states for cybersecurity practices.
- Identify and prioritize opportunities for improvement in a consistent, repeatable manner.
- Support cross-organization communication and coordination to manage cybersecurity risk effectively.

The CSF Core is a taxonomy of high-level cybersecurity outcomes that can help organizations manage their cybersecurity risks. The Core components are a hierarchy of Functions, Categories, and Subcategories that detail each outcome. These outcomes can be understood by a broad audience, including executives, managers, and practitioners, regardless of their cybersecurity expertise [3].

The CSF Core Functions (Govern, Identify, Protect, Detect, Respond, Recover) organize cybersecurity outcomes at their highest level. The Core then identifies underlying key Categories and Subcategories for each Function and matches them with example Informative References [3]. The six Functions of the CSF 2.0 Core are composed of 22 Categories, which are further broken down into 106 Subcategories of more specific outcomes

Section 5 provides more detailed guidance on each Function, Category, and Subcategory as part of defining the Community Profile. Additionally, NIST provides supplemental resources to help organizations understand, adopt, and use CSF 2.0 and achieve the desired outcome of each Subcategory, including Implementation Examples and Informative References. The NIST CSF website contains the most current information regarding available Implementation Examples and Informative References. Communities and organizations can choose to add their own Implementation Examples and Informative References that are unique to the manufacturing context in the future.

3.1. Govern (GV)

The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.

Table 1 Govern (GV) Cybersecurity Framework Categories

Category	Objective
GV.OC	The circumstances—mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements—surrounding the organization's cybersecurity risk management decisions are understood
GV.RM	The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions
GV.RR	Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated
GV.PO	Organizational cybersecurity policy is established, communicated, and enforced
GV.OV	Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy
GV.SC	Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders

3.2. Identify (ID)

The organization's current cybersecurity risks are understood.

Table 2 Identify (ID) Cybersecurity Framework Categories

Category	Objective
ID.AM	Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy
ID.RA	The cybersecurity risk to the organization, assets, and individuals is understood by the organization
ID.IM	Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions

3.3. Protect (PR)

Safeguards to manage the organization's cybersecurity risk are used.

Table 3 Protect (PR) Cybersecurity Framework Categories

Category	Objective
PR.AA	Access to physical and logical assets is limited to authorized users, services, and hardware, and is managed commensurate with the assessed risk of unauthorized access
PR.AT	The organization's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks
PR.DS	Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
PR.PS	The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability.
PR.IR	Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience

3.4. Detect (DE)

Possible cybersecurity attacks and compromises are found and analyzed.

Table 4 Detect (DE) Cybersecurity Framework Categories

Category	Objective
DE.CM	Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events
DE.AE	Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents.

3.5. Respond (RS)

Actions regarding a detected cybersecurity incident are taken

Table 5 Response (RS) Cybersecurity Framework Categories

Category	Objective
Respond (RS)	Actions regarding a detected cybersecurity incident are taken
RS.MA	Responses to detected cybersecurity incidents are managed
RS.AN	Investigations are conducted to ensure effective response and support forensics and recovery activities
RS.CO	Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies
RS.MI	Activities are performed to prevent expansion of an event and mitigate its effects

3.6. Recover (RC)

Assets and operations affected by a cybersecurity incident are restored

Table 6 Recover (RC) Cybersecurity Framework Categories

Category	Objective
Recover (RC)	Assets and operations affected by a cybersecurity incident are restored
RC.RP	Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents
RC.CO	Restoration activities are coordinated with internal and external parties

4. Manufacturing Profile Development Approach

The Profile offers guidance on implementing the CSF in a manufacturing setting, including examples and recommendations for customizing CSF implementations to address specific risks and challenges faced by manufacturing organizations. The statements in the subcategories in Section 5 are derived from the security controls in NIST SP 800-53 Rev. 5 [5]. Additional input was obtained from NIST SP 800-82, Rev. 3 [4], Section 6 and Appendix F. The section provides the tailoring factors used to support the CSF subcategory Community Profile guidance for the manufacturing domain.

4.1. Manufacturing Business/Mission Objectives

The development of the Profile included consideration for common business/mission objectives in the manufacturing sector. These business/mission objectives provide the necessary context for identifying and managing applicable cybersecurity risk mitigation pursuits [3]. Five common business/mission objectives for the manufacturing sector were initially identified along with key cybersecurity practices for supporting each business/mission objective. This information allows users to better prioritize actions and resources according to their defined needs.

The Business/Mission Objectives Are Not Listed in Priority Order.

Maintain Environmental Safety
Manage cybersecurity risks that could adversely affect the environment, including both accidental and deliberate damage. Personnel should understand the interdependencies between cybersecurity and environmental safety.

Maintain Human Safety
Manage cybersecurity risks that could potentially impact human safety. Personnel should understand the interdependencies between cybersecurity and safety.

Maintain Production Goals
Manage cybersecurity risks that could adversely affect production goals (e.g., asset damage, could potentially adversely affect production goals). Personnel should understand cybersecurity and production goal interdependencies.

Maintain Quality of Product
Manage cybersecurity risks that could adversely affect the quality of the product. Protect against compromise of the integrity of the manufacturing process and associated data.

Maintain Sensitive Information
Manage cybersecurity risks that could lead to the loss or compromise of the organization’s
Manufacturing System Categorization and Risk Management

The Manufacturing Community Profile is structured into three impact levels based on risks and their impact on an organization’s manufacturing systems and processes.

4.2. Categorization Process

Manufacturing systems support an organization's most critical and, sometimes, most sensitive operations and assets. Applying cybersecurity controls in these environments demands the greatest attention and effort to ensure appropriate operational security and risk mitigation. Categorizing systems allows an organization to apply increasing levels of protection for its systems due to the risks in the system and its environment.

NIST Federal Information Processing Standard (FIPS) 199 defines a categorization process. The process is used by the federal government but can be applied to any organization with modifications. FIPS 199 sets the expectation that categorization "must take place within the context of each organization" [7]. There are three levels of potential impact (e.g., LOW, MODERATE, or HIGH) if an incident or event jeopardizes the manufacturing system or components, [7]. The Profile defines the three impact levels as follows:

1. The *potential impact* is **LOW** if the loss of integrity, availability, or confidentiality could be expected to have a **limited** adverse effect on manufacturing operations, manufactured product, assets, brand image, finances, personnel, the public, or the environment.
2. The *potential impact* is **MODERATE** if the loss of integrity, availability, or confidentiality could be expected to have a **serious** adverse effect on manufacturing operations, manufactured product, assets, brand image, finances, personnel, the public, or the environment.
3. The *potential impact* is **HIGH** if the loss of integrity, availability, or confidentiality could be expected to have a **severe or catastrophic** adverse effect on manufacturing operations, manufactured product, assets, brand image, finances, personnel, the public, or the environment.

A limited adverse effect means the loss of an impact category (e.g., injury, financial loss, environmental release, interruption of production, or impact to public image) may:

- cause a degradation in mission capability to an extent and duration that the system can perform its primary functions, but the effectiveness of the functions is noticeably reduced
- result in minor damage to operational assets that is repairable without further disruption to operations
- result in minor financial loss
- result in minor harm to individuals requiring only basic first aid

A serious adverse effect means the loss of an impact category may:

- cause a significant degradation in mission capability to an extent and duration that the system can perform its primary functions, but the effectiveness of the functions is significantly reduced
- result in significant damage to operational assets that are repairable (or replaceable) with limited impact on operational capabilities
- result in significant financial loss

- result in significant harm to individuals requiring hospitalization, but does not involve loss of life or serious life-threatening injuries

A severe or catastrophic adverse effect means the loss of an impact category may:

- cause a severe degradation in or loss of mission capability to an extent and duration that the system is not able to perform one or more of its primary functions
- result in major damage to operational assets that requires significant time to repair or replace, resulting in extended downtime
- result in major financial loss
- result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries

The impact on the organization is determined by the extent of injuries, financial loss, damage caused by environmental release, the interruption of production, damage to public image, and the products produced. Tables 7 and 8 provide examples of mission-based rationale for selecting the security category of the manufacturing system. Table 8 also includes representative examples of industries by impact level. The Profile provides guidance for each potential impact level (e.g., low, moderate, and high) associated with the security category, allowing for increased protection based on risk.

Table 7 Manufacturing System Impact Levels [4]

Category	High	Moderate	Low
Outage at Multiple Sites	Significant disruption to operations at multiple sites, with restoration expected to require 1 or more days	Operations are disrupted at multiple sites, with restoration expected to require more than 1 hour	Operations are partially disrupted at multiple sites, with restoration to full capability requiring less than 1 hour.
National Infrastructure and Services	Impacts multiple sectors or disrupts community services in a major way	Potential to impact the sector at a level beyond the company	Little to no impact on sectors beyond the individual company. Little to no impact on the community.
Cost (% of Revenue)	> 25%	> 5%	< 5%
Legal	Felony criminal offense or compliance violation affecting the license to operate	Misdemeanor criminal offense or compliance violation resulting in fines.	None
Public Confidence	Loss of brand image	Loss of customer confidence	None

361 **Table 8 Manufacturing System Impact Levels Based on Product Produced and Industry Concerns**

Category	Low Impact	Moderate Impact	High Impact
Product Produced	Non-hazardous materials or products Non-ingested consumer products	Some hazardous products or steps during production High amount of proprietary information	Critical infrastructure Hazardous materials Ingested products
Industry Examples	Plastic injection molding Warehousing	Automotive metal stamping Pulp and paper Semiconductors Automotive production	Utilities Petrochemical Food and beverage Pharmaceutical

362 ## 4.3. Risk Management

363 The Manufacturing Profile is meant to enhance but not replace current cybersecurity standards
364 and industry guidelines that the manufacturer is currently embracing. Manufacturers can
365 determine activities that are important to critical service delivery and can prioritize investments
366 to maximize the impact of each dollar spent. Ultimately, the Profile is aimed at reducing and
367 better managing cybersecurity risks. The Profile, along with the CSF, is not a one-size-fits-all
368 approach to managing cybersecurity risk for critical infrastructure. Manufacturers will continue
369 to have unique risks – different threats, different vulnerabilities, different risk tolerances – and
370 how they implement security practices will vary.

5. Manufacturing Profile Subcategory Guidance

The Profile guidance is scalable, supporting enhanced security protections beyond a baseline. Each impact level builds upon the previous, starting with Low as the baseline. Unless specified, Moderate and High levels include all requirements from the levels below.

- **Low:** Serves as the starting baseline for all manufacturing systems.
- **Moderate:** Incorporates Low and Moderate security measures.
- **High:** Includes Low, Moderate, and High security requirements.

This structure ensures that higher impact levels encompass relevant security implementations necessary for their designation.

5.1. Govern

Note: In NIST SP 800-53, controls relevant to the Govern (GV) function of NIST CSF are spread across each of the twenty (20) control families and associated -01 controls. Therefore, mappings across each of these -01 controls is not included in the "Informative References and Mappings" column due to the large number of mappings required.

Table 9 Subcategory-level Guidance for the Govern Function

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
GV.OC-01: The organizational mission is understood and informs cybersecurity risk management	Low, Moderate, & High	Define the organization's mission regarding manufacturing-specific objectives (e.g., human safety, environmental safety, quality, production goals, and protection of sensitive information). Prioritize cybersecurity risks that could impact manufacturing systems based on the organization's mission objectives. Document how mission requirements (e.g., operational continuity, product integrity) shape cybersecurity risk decisions (e.g., patch deferrals, remote access policies). Communicate the relationship between the organizational mission and cybersecurity risk to production, engineering, and IT teams to ensure a unified understanding and decision-making.	

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	Low, Moderate, & High	Identify internal and external stakeholders (such as engineering teams, operators, IT staff, executive leadership, and suppliers) who influence or are impacted by cybersecurity risk management decisions. Engage stakeholders through interviews, surveys, or involvement in risk assessments to understand their cybersecurity concerns, constraints, and objectives. Incorporate cybersecurity responsibilities into broader safety and quality management systems to reflect the interconnected nature of cyber-physical risks in manufacturing. Document and integrate stakeholder needs and expectations into the development of cybersecurity policies, risk acceptance thresholds, and incident response plans. Communicate how stakeholder priorities (e.g., uptime for production managers, compliance for QA leads) are reflected in cybersecurity risk management decisions.	
GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity—including privacy and civil liberties obligations—are understood and managed	Low, Moderate, & High	Identify and document applicable legal, regulatory, contractual, and external cybersecurity requirements that impact the manufacturing system, including obligations related to privacy and civil liberties (e.g., logging, video surveillance, remote access) into the cybersecurity control objectives and governance decisions. Assess how cybersecurity practices intersect with regulated manufacturing functions (e.g., safety, product quality, environmental controls) and integrate this understanding into compliance activities. Document procedures to meet contractual cybersecurity obligations (e.g., incident reporting timelines, audit or data protection requirements), and monitor for updates to relevant laws, industry standards, or customer-driven requirements. Communicate changes in these requirements to affected personnel.	
GV.OC-04: Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated	Low, Moderate, & High	Identify capabilities and services that external stakeholders (e.g., customers, supply chain partners) rely on and expect. Engage with stakeholders to document the relative criticality of these services (e.g., availability expectations, service continuity, recovery time objective (RTO), recovery point objective (RPO)). Prioritize the protection and resilience of manufacturing processes, assets, and supporting systems (e.g., backup generators, uninterruptible power supplies) that support these services. Embed service continuity and availability expectations in internal governance processes (e.g., risk prioritization, resource planning, policy development).	

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
GV.OC-05: Outcomes, capabilities, and services that the organization depends on are understood and communicated	Low, Moderate, & High	Identify, prioritize, and document external services and capabilities that support manufacturing system processes and components (e.g., cloud services, vendor support, power, shipping, materials). Communicate with external service providers to define availability and service continuity expectations, including service-level requirements and recovery objectives. Incorporate these external dependencies into governance processes (e.g., risk assessments, procurement oversight, third-party management policies).	
GV.RM-01: Risk management objectives are established and agreed to by organizational stakeholders	Low, Moderate, & High	Establish an executive-level oversight committee that includes both OT and IT leadership to regularly review cyber risk objectives and adjust risk management strategies based on manufacturing requirements and the changing threat landscape. Use these objectives to establish metrics and measures of cybersecurity effectiveness and any impacts on manufacturing system performance.	
GV.RM-02: Risk appetite and risk tolerance statements are established, communicated, and maintained	Low, Moderate, & High	Define and communicate acceptable levels of cybersecurity risk (risk appetite or risk tolerance) for the manufacturing environment, including detailed cyber risk tolerance statements that address critical aspects of manufacturing operations (e.g., automated assembly lines, process control systems, quality inspection systems, inventory management, control logic changes, configuration changes) and the interdependencies between IT and OT systems, networks, physical processes, and safety systems. As appropriate, include specific risk tolerance levels for various manufacturing zones and system types (e.g., PLCs, industrial robots, CNC machines). Review and update risk parameters regularly to reflect changing manufacturing needs and the evolving threat landscape.	
GV.RM-03: Cybersecurity risk management activities and outcomes are included in enterprise risk management processes	Low, Moderate, & High	Integrate manufacturing cybersecurity risk management activities, metrics, and reports with enterprise risk management (ERM) processes. Assign roles and responsibilities for monitoring and evaluating manufacturing cybersecurity risks within the organization. Ensure that governance committees review and approve relevant manufacturing system risk reports and mitigation strategies. Maintain a manufacturing system risk register mapping control system vulnerability to business impacts, with designated owners responsible for updates and oversight. Ensure regular reporting to senior management to facilitate informed decision-making and oversight.	

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
GV.RM-04: Strategic direction that describes appropriate risk response options is established and communicated	Low, Moderate, & High	Develop a risk response strategy that includes IT and manufacturing systems. Document and communicate the organization's approaches and criteria for managing cybersecurity risks related to manufacturing operations, including its stance on risk response options associated with: • Accepting certain cybersecurity risks, taking into consideration the potential impact of the risk against the cost of mitigating. • Mitigating certain cybersecurity risks by reducing the likelihood or impact of identified risks through targeted mitigation measures (e.g., network segmentation, ICS-compatible intrusion detection systems, controlled patch management processes) that minimize the impact or disruption to the manufacturing system. • Transferring certain cybersecurity risks through mechanisms such as cybersecurity insurance or contractual agreements with suppliers and third-party service providers. • Avoiding certain cybersecurity risks through informed mitigation measures (e.g., decommissioning unsupported legacy systems, isolating manufacturing system network segments or devices from the internet) that take into consideration the potential operational impacts.	
GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties	Low, Moderate, & High	Document the communication strategy for providing cybersecurity risk information related to the organization's manufacturing system, suppliers, and other third-party service providers to internal stakeholders. The strategy should outline the reporting frequency and content for the different stakeholder groups (e.g., management, operational engineers, ICS managers, internal auditors, legal, acquisition, physical security, human resources) considering the sensitivity of the information and the recipients' needs (e.g., presented in a format that is usable and actionable).	

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
GV.RM-06: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated	Low, Moderate, & High	Establish a standardized risk management approach for the manufacturing system that is informed by industry standards and guidelines specific or adaptable to ICS environments (e.g., NIST RMF, NIST SP 800-82, ISA/IEC 62443 [6]). The approach should include a methodology for calculating, documenting, categorizing, and prioritizing cybersecurity risks associated with the manufacturing system while considering the unique safety, environmental, and operational impacts of cybersecurity events (e.g., potential production downtime, equipment damage). Document the templates and tools that the organization will utilize to support consistent risk evaluation, categorization, and tracking for the manufacturing system.	
GV.RM-07: Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions	Low, Moderate, & High	Update the organization's risk management approach to support positive risks associated with cybersecurity in the manufacturing system. Establish guidance and support mechanisms that encourage stakeholders throughout the organization to identify and discuss potential improvement opportunities (e.g., improving operational efficiency, enhancing product quality, eliminating redundant or outdated components).	
GV.RR-01: Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving	Low, Moderate, & High	Designate and document senior leadership roles (e.g., Plant Manager, OT/IT Leader(s), Chief Information Security Officer (CISO)) and responsibilities in developing, implementing, and assessing the organization's cybersecurity strategy for the manufacturing system. Integrate cybersecurity into the broader safety, quality, and operational capabilities of the manufacturing system to promote a culture of ethical behavior and continuous improvement.	

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced	Low, Moderate, & High	Designate, document, and communicate roles, responsibilities, and authorities for supporting the manufacturing system cybersecurity risk management program. Integrate the cybersecurity roles, responsibilities, and authorities into organizational structures such as position descriptions, performance reviews, and accountability frameworks to reinforce their importance across the organization and for supporting the manufacturing system.	
GV.RR-03: Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies	Low, Moderate, & High	Identify and prioritize cybersecurity resource needs based on the criticality of manufacturing assets and processes. Allocate resources in alignment with the organization's risk tolerance, ensuring that personnel have the necessary manufacturing system expertise and that critical systems are adequately protected. Conduct periodic reviews to ensure that those with responsibilities for cybersecurity of the manufacturing system have the authority, training, and tools needed to manage risks effectively.	
GV.RR-04: Cybersecurity is included in human resources practices	Low, Moderate, & High	Integrate cybersecurity considerations into human resources practices across the manufacturing organization, including training and awareness programs for personnel who interact with manufacturing systems. Conduct background checks for personnel with access to critical systems or sensitive information. Clearly define and communicate cybersecurity expectations and responsibilities to all personnel, ensuring they understand their roles in maintaining cybersecurity.	
GV.PO-01: Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced	Low, Moderate, & High	Develop, communicate, and enforce cybersecurity policies that provide guidance for the security requirements for the manufacturing system based on organizational context, cybersecurity strategy, and priorities. The policies (e.g., the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, compliance) cover the full life cycle of the manufacturing system and are reviewed and approved by senior management responsible for risk management including organizational entities responsible for the different aspects of security (e.g., technical, physical, personnel, cyber-physical, use of resources, access control, media protection, vulnerability management, maintenance, monitoring).	

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
GV.PO-02: Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission	Low, Moderate, & High	Review and update cybersecurity risk management policies to address changes in manufacturing system requirements, cybersecurity risks, technological advancements (e.g., AI, IIoT, Digital Twins), and significant business changes (e.g., mergers, new contracts). Ensure that the cybersecurity policy is approved by senior management accountable for managing cybersecurity risks in manufacturing operations and is communicated to all relevant stakeholders.	
GV.OV-01: Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction	Low, Moderate, & High	Review and analyze the outcomes of the cybersecurity risk management strategy to determine the effectiveness in supporting manufacturing operations and achieving organizational objectives. Adjust the cybersecurity risk management strategy to address any identified gaps, enhance risk management, and ensure alignment with manufacturing mission objectives and operational performance. Ensure that senior management is informed and involved in adjusting strategies to achieve cybersecurity risk management objectives. Communicate the results of these reviews and any necessary adjustments to stakeholders.	
GV.OV-02: The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks.	Low, Moderate, & High	Review assessment (e.g., audit revies, post-incident reviews) findings to determine whether the existing cybersecurity strategy, policy, and programs are effective in meeting internal and external requirements. Adjust the strategy, policies, and roles and responsibilities as necessary to address identified gaps.	

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
GV.OV-03: Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed	Low, Moderate, & High	Review and analyze cybersecurity risk management metrics alongside manufacturing operational metrics (e.g., respective KPIs and KRIs) to assess the effectiveness of the risk management strategy. Document the potential impact of adverse cybersecurity events on manufacturing mission objectives and operational performance. Evaluate whether current cybersecurity risk strategies and policies are impacting manufacturing operations and identify opportunities for adjustment. Ensure that senior management is informed and involved in adjusting strategies to minimize adverse impacts on operational performance. Communicate the results of these reviews and any necessary adjustments to stakeholders to enhance both cybersecurity risk management and manufacturing operational performance.	
GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders	Low, Moderate, & High	Establish a cybersecurity supply chain risk management (C-SCRM) program for the manufacturing systems, including strategy, objective, program, policies, and processes that address the unique risks associated with supply chain dependencies and the industrial control systems supporting manufacturing. Ensure the C-SCRM program is aligned and approved with organizational stakeholders (e.g. IT, operations, legal, human resources, engineering).	
GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally	Low, Moderate, & High	Establish and maintain cybersecurity roles and responsibilities for external personnel (e.g., third-party providers, contractors) supporting the manufacturing system. Require third-party providers to notify the organization of any personnel changes (e.g., transfers, terminations) that could impact the manufacturing system or components. Include C-SCRM responsibilities and performance requirements in external position descriptions to ensure clarity and accountability. Create responsibility matrices to document roles, responsibilities, and communication protocols for C-SCRM activities associated with the manufacturing system or processes.	

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes	Low, Moderate, & High	Integrate C-SCRM into the organization's cybersecurity and enterprise risk management (ERM) programs to ensure a consistent approach to managing risks for the manufacturing system. Establish integrated security controls that address supply chain risks for the manufacturing system. Ensure C-SCRM is part of continuous improvement processes and that significant supply chain cybersecurity risks are escalated to senior management for review and action at the ERM level.	
GV.SC-04: Suppliers are known and prioritized by criticality	Low, Moderate, & High	Develop and maintain criteria (e.g., importance of supplier-sourced products or services, sensitivity of data processed or held by suppliers, the level of access to the organization's systems, and availability requirements) for assessing supplier criticality to the organization's manufacturing mission objectives. Maintain a record of all suppliers and prioritize them based on the established criticality criteria.	
GV.SC-05: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties	Low, Moderate, & High	Establish and prioritize cybersecurity and supply chain risk management requirements for suppliers and third-party providers supporting the manufacturing systems, components, products, and services, considering the criticality of the supplied products or services, the potential impact on production continuity, and the sensitivity of data handled. Include these requirements in contracts and other agreements, specifying how compliance will be verified through mechanisms such as regular audits, security assessments, or certifications. Define rules and protocols for information sharing between the organization, suppliers, and sub-tier suppliers, particularly for incidents that could impact manufacturing operations. Require suppliers to disclose cybersecurity features, functions, and known vulnerabilities of their products and services, and to maintain a current software and hardware bill of materials for critical components. Ensure that contracts specify the rights and responsibilities of all parties regarding cybersecurity risks, including provisions for incident response and recovery.	

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships	Low, Moderate, & High	Establish a due diligence process for evaluating the cybersecurity posture of suppliers and third-party providers before entering formal relationships, considering factors such as the criticality of the supplied products or services to manufacturing operations, the supplier's cybersecurity practices, and the potential risks associated with their products or services. Ensure that the due diligence process is commensurate with the level of risk and is aligned with the organization's risk management objectives.	
GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship	Low, Moderate, & High	Establish a process for ongoing monitoring and assessment of the cybersecurity risks posed by suppliers, their products and services, and other third parties for the manufacturing system and processes. Ensure that this process is aligned with the organization's risk management objectives and is commensurate with the level of risk. Require regular reporting and updates from suppliers on their cybersecurity posture and any changes to their risk profiles. Ensure that findings and recommendations are communicated to relevant stakeholders, including those responsible for manufacturing operations and cybersecurity.	
GV.SC-08: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities	Low, Moderate, & High	Define and coordinate crisis communication methods and protocols between the organization and its suppliers. Establish rules and protocols for reporting incident response and recovery activities between the organization and its suppliers. Include critical suppliers in incident response exercises and simulations. Identify and document key personnel from suppliers and third-party partners who will be involved in incident response and recovery planning and execution. Conduct collaborative lessons-learned sessions with critical suppliers to identify areas for improvement and coordinate action items to improve incident response and recovery capabilities.	

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
GV.SC-09: Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and performance is monitored throughout the technology product and service life cycle	Low, Moderate, & High	Establish a process for monitoring and reporting manufacturing system C-SCRM performance throughout the technology and service life cycles. Ensure that manufacturing system- and process-specific C-SCRM metrics are integrated into the organization's cybersecurity risk management and ERM programs. Require regular reporting on C-SCRM performance to senior leadership, including any identified risks and actions taken to mitigate them.	
GV.SC-10: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement	Low, Moderate, & High	Ensure that cybersecurity supply chain risk management plans include provisions for managing risks associated with the termination or transition of supplier relationships, including processes for evaluating cyber risk to manufacturing operations and processes. Define plans for maintaining production continuity and mitigating risks to manufacturing systems and processes created by supplier termination or transition.	

5.2. Identify

Table 10 Subcategory-level Guidance for the Identify Function

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
ID.AM-01: Inventories of hardware managed by the organization are maintained	Low	Document an inventory of manufacturing system components that reflects the current system. Manufacturing system components include, for example, PLCs, sensors, actuators, robots, machine tools, firmware, network switches, routers, power supplies, and other networked components or devices. System component inventory is reviewed and updated as defined by the organization. Information deemed necessary for effective accountability of manufacturing system components includes hardware inventory specifications, component owners, networked components or devices, machine names, and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location.	CM-08 PM-05
	Moderate	Identify individuals who are both responsible and accountable for administering manufacturing system components. Identify and implement mechanisms for detecting changes to hardware and firmware components within the manufacturing system to validate the current inventory.	
	High	Where safe and feasible, these mechanisms should be automated.	
ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained	Low	Document an inventory of manufacturing system software and firmware components that reflect the current system. Manufacturing system software components include for example software license information, software version numbers, HMI and other ICS component applications, software, operating systems. System software inventory is reviewed and updated as defined by the organization.	AC-20 PM-05 SA-05 SA-09
	Moderate	Identify individuals who are both responsible and accountable for administering manufacturing system software. Identify and implement mechanisms for detecting changes to software within the manufacturing system to validate the current inventory.	
	High	Where safe and feasible, these mechanisms should be automated.	

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained.	Low & Moderate	Document, review, and authorize all connections and data flows within the manufacturing systems, and between the manufacturing systems and other systems. Document, review, and authorize connections and data flows with third-party external systems such as maintenance providers and vendor support systems. Review and authorize any changes to the network connections and data flows and update documentation. Connection information includes, for example, the interface characteristics, data characteristics, ports, protocols, addresses, description of the data, security requirements, and the nature of the connection.	AC-04 CA-03 CA-09 PL-02 PL-08 PM-07
	High	Where safe and feasible, automate the identification of the network connections and data flows.	
ID.AM-04: Inventories of services provided by suppliers are maintained	Low	Identify and document all external services used by the manufacturing system. Examples of external services include predictive maintenance and prognostics services, remote asset monitoring, supplier-managed inventory systems, outsourced calibration and testing services, third-party SCADA hosting, and external cloud-based analytics platforms.	AC-20 SA-09 SR-02
	Moderate & High	Require external service providers to identify the functions, addresses, ports, protocols, and other services required for use with the manufacturing system.	
ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission	Low, Moderate, & High	Identify and prioritize manufacturing system assets (e.g., data, hardware, software, systems, facilities, services, people) based on their classification, criticality, and impact on the mission. Identify the types of information in possession, custody, or control for which security safeguards are needed (e.g., sensitive or protected information).	RA-02 RA-03 RA-09
ID.AM-07: Inventories of data and corresponding metadata for designated data types are maintained	Low & Moderate	Document an inventory of data present in the manufacturing system. The inventory should include ownership and corresponding metadata based on designated data types (e.g., intellectual property, controlled unclassified information (CUI), device configurations, engineering data).	CM-12 CM-13 SI-12
	High	Use automated tools to discover and catalog instances of designated data types across the manufacturing system, where feasible and safe.	

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
ID.AM-08: Systems, hardware, software, services, and data are managed throughout their life cycles	Low	Implement comprehensive lifecycle tracking for manufacturing systems, encompassing hardware, software, services, and data. Establish clear accountability for all system components throughout their lifecycle, including processes for removal, transfer, and disposition. Ensure that all components entering or exiting the facility are properly authorized, monitored, and controlled, with detailed records maintained for each item. Prioritize the sanitization of portable media before disposal, release, or reuse, and ensure that manufacturing system data is securely destroyed in accordance with established policies. Integrate security requirements into the acquisition process for manufacturing systems and their components. Adopt a system development lifecycle approach that incorporates robust security measures for managing the manufacturing system. Regularly schedule, perform, document, and review maintenance and repair activities for all system components to ensure operational integrity and compliance.	CM-09 CM-13 MA-02 MA-06 PL-02 PM-22 PM-23 SA-03 SA-04 SA-08 SA-22 SI-12 SI-18 SR-05 SR-12
	Moderate	Update the inventory of manufacturing system components as an integral part of component installations, removals, and system updates. Implement formal change management processes for manufacturing systems including security reviews of system upgrades, software updates, and configuration changes. Identify and document redundant systems and consolidate where it is feasible to reduce attack surface. Perform preventative maintenance at defined intervals. Enforce approval requirements, control, and monitoring of maintenance tools for use on the manufacturing system. Maintenance tools can include, for example, hardware/software diagnostic test equipment, hardware/software packet sniffers and laptops.	
	High	Integrate cybersecurity requirements throughout the complete lifecycle of all manufacturing assets from procurement through decommissioning. Maintain detailed transition plans for technology upgrades, including security controls for legacy systems. Automate lifecycle processes. Implement automated mechanisms, where it is feasible, to schedule, conduct, and document maintenance and repairs; and to produce records of maintenance activity. Prevent the unauthorized removal of maintenance equipment containing manufacturing system information. Require that diagnostic services pertaining to remote maintenance be performed from a system that implements a security capability that is comparable to the capability implemented on the manufacturing system.	

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded	Low & Moderate	Formulate a comprehensive plan to identify, document, and report vulnerabilities within the manufacturing system. Perform vulnerability scans on the system where it is both safe and feasible, ensuring the process includes thorough analysis, remediation efforts, and the sharing of relevant information. Employ control system-specific vulnerability scanning tools and techniques tailored to the manufacturing system, its components, or representative systems, while prioritizing safety and feasibility. Exercise caution with active vulnerability scanning that generates network traffic, ensuring it does not disrupt critical system functions or operations. Establish a strategy for continuous monitoring of the manufacturing system's security posture to maintain ongoing awareness of vulnerabilities. Develop and maintain a structured process for regularly reviewing vulnerabilities and defining actionable mitigation strategies. Conduct risk assessments that evaluate vulnerabilities in the context of their potential impact on manufacturing operations and assets. Implement strict access controls to safeguard privileged vulnerability data and prevent unauthorized disclosure.	CA-02 CA-07 CA-08 RA-03 RA-05 SA-11(02) SA-15(07) SA-15(08) SI-04 SI-05
	High	Conduct performance/load testing and penetration testing on the manufacturing system with care to ensure that manufacturing operations are not adversely impacted by the testing process. Identify where manufacturing system vulnerabilities may be exposed to adversaries. Production systems may need to be taken offline before testing can be conducted. If the manufacturing system is taken offline for testing, tests are scheduled to occur during planned manufacturing outages whenever possible. If penetration testing is performed on non-manufacturing networks, extra care is taken to ensure that tests do not propagate into the manufacturing network. Identify where manufacturing system vulnerabilities may be exposed to adversaries.	
ID.RA-02: Cyber threat intelligence is received from information sharing forums and sources	Low, Moderate, & High	Establish and maintain ongoing contact with security groups and associations to receive security alerts and advisories. Security groups and associations include, for example, information sharing and analysis centers (ISACs), special interest groups, forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations. Implement a threat awareness program that includes a cross-organization information-sharing capability. Organizations should consider having both an unclassified and classified information-sharing capability. Collaborate and share information about potential vulnerabilities and incidents. Identify where automated mechanisms can be implemented to make security alert and advisory information available to relevant organization stakeholders.	PM-15 PM-16 SI-05

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
ID.RA-03: Internal and external threats to the organization are identified and recorded	Low, Moderate, & High	Conduct and document periodic assessments of risks to the manufacturing system to identify indicators of compromise, threats, and the likelihood of impact on manufacturing operations and assets. Include threats from both insiders and external parties.	PM-12 PM-16 RA-03 SI-05
ID.RA-04: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded	Low, Moderate, & High	Conduct criticality reviews of the manufacturing system that define the likelihood of the threats exploiting the vulnerabilities and the potential adverse impacts to manufacturing operations, assets, and individuals.	PM-09 PM-11 RA-02 RA-03 RA-08 RA-09
ID.RA-05: Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization.	Low, Moderate, & High	Conduct risk assessments of the manufacturing system incorporating threats, vulnerabilities, likelihoods, and impacts to manufacturing operations, assets, and individuals. Disseminate risk assessment results to relevant stakeholders.	PM-16 RA-02 RA-03 RA-07
ID.RA-06: Risk responses are chosen, prioritized, planned, tracked, and communicated.	Low, Moderate, & High	Establish a comprehensive strategy to manage risk to the manufacturing system that includes the identification, prioritization, and implementation of risk responses. Ensure that newly identified vulnerabilities are mitigated or documented as accepted risks.	PM-09 PM-18 PM-30 RA-07
ID.RA-07: Changes and exceptions are managed, assessed for risk impact, recorded, and tracked	Low	Conduct security impact analyses and risk assessments in connection with change control reviews. Record and track the findings from these risk assessments.	CA-07 CM-03 CM-04

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
	Moderate	Test, validate, and document changes to the manufacturing system before implementing the changes on the operational system. Evaluate potential security impact and assess cyber risk as a result of these changes. Review and authorize proposed changes prior to implementing them on the manufacturing system.	
	High	Conduct a security impact analysis (SIA) in a separate test environment before implementation into an operational environment for planned changes to the manufacturing system.	
ID.RA-08: Processes for receiving, analyzing, and responding to vulnerability disclosures are established	Low	Establish processes and assign responsibilities for receiving, analyzing, and responding to vulnerability disclosures by suppliers, vendors, customers, partners, and government cybersecurity organizations.	RA-05
	Moderate	Restrict access to vulnerability data (e.g., unmitigated vulnerabilities).	
	High	Implement automated mechanisms to assign responsibilities for receiving, analyzing, and responding to vulnerability disclosures. Identify where manufacturing system vulnerabilities may be exposed to adversaries.	
ID.RA-09: The authenticity and integrity of hardware and software are assessed prior to acquisition and use	Low & Moderate	Assess the authenticity and cybersecurity of critical components and services prior to acquisition and use.	SA-04 SA-05 SA-10 SA-11 SA-15 SA-17 SI-07 SR-05 SR-06 SR-10 SR-11
	High	Implement hardware integrity checks prior to use of critical components to detect unauthorized tampering (e.g., tamper-detection seals, anti-tamper coatings). Implement software integrity checks for critical components when they are acquired, installed, and updated.	

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
ID.RA-10: Critical suppliers are assessed prior to acquisition	Low, Moderate, & High	Conduct and document cybersecurity supply chain risk assessments on each critical supplier prior to acquisition of hardware and software. These assessments should identify and prioritize potential negative impacts on the organization resulting from the sharing of sensitive information or the use of information technology, operational technology, services, and both technology-based and non-technology-based input products that support the manufacturing system. Disseminate the results of these assessments with relevant stakeholders, including those responsible for information technology and operational technology systems.	SR-06

ID.IM-01: Improvements are identified from evaluations	Low	Regularly perform self-assessments of critical services, considering current threats and TTPs, and identify improvements needed from a cybersecurity perspective. Evaluate current industry standards and regulations applicable to the manufacturing system and identify cybersecurity program improvements.	AC-01 AT-01 AU-01 CA-01 CM-01 CP-01 IA-01 IR-01 MA-01 MP-01 PE-01 PL-01 PM-01 PS-01 PT-01 RA-01 SA-01 SC-01 SI-01 SR-01 CA-02 CA-05 CA-07 CA-08 CP-02 IR-04 IR-08 PL-02 RA-03 RA-05 RA-07 SA-08 SA-11 SA-17(06) SI-02 SI-04 SR-05

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
	Moderate	Invest in third-party assessments or independent audits to help identify areas for improvement in the cybersecurity program.	
	High	Where safe and feasible, continuously evaluate compliance with cybersecurity requirements. Implement automated tools.	
ID.IM-02: Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties	Low	Identify improvements for future manufacturing system incident detection, response, and recovery activities based on findings from incident assessments (e.g., tabletop exercises and simulations, tests, internal reviews, independent audits).	AC-01 AT-01 AU-01 CA-01 CM-01 CP-01 IA-01 IR-01 MA-01 MP-01 PE-01 PL-01 PM-01 PS-01 PT-01 RA-01 SA-01 SC-01 SI-01 SR-01 CA-02 CA-05 CA-07 CA-08 CP-02 CP-04 IR-03 IR-04 IR-08 PL-02

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
			PM-04 PM-31 RA-03 RA-05 RA-07 SA-08 SA-11 SI-02 SI-04 SR-05
	Moderate	Exercise contingency plans (e.g., business continuity plans, disaster recovery plans, continuity of operations plans, crisis communications plans, critical infrastructure plans, cyber incident response plans, and occupant emergency plans) periodically and identify improvements. Coordinate testing with critical external service providers, suppliers, and key internal stakeholders (e.g., senior executives, legal departments, and human resources). Collect and analyze performance metrics to refine and enhance the overall cybersecurity program.	
	High	Where safe and feasible, conduct penetration testing on critical manufacturing systems and components, as approved by leadership.	

ID.IM-03: Improvements are identified from execution of operational processes, procedures, and activities	Low & Moderate	Identify improvements based on lessons learned from protection, detection, response, and recovery activities. Use metrics to assess operational cybersecurity performance (e.g., time to detect, time to respond, time to recover).	AC-01 AT-01 AU-01 CA-01 CM-01 CP-01 IA-01 IR-01 MA-01 MP-01 PE-01 PL-01 PM-01 PS-01 PT-01 RA-01 SA-01 SC-01 SI-01 SR-01 CA-02 CA-05 CA-07 CA-08 CP-02 IR-04 IR-08 PL-02 PM-04 PM-31 RA-03 RA-05 RA-07 SA-04 SA-08 SA-11 SI-02 SI-04

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
			SR-05
	High	Implement independent teams to assess the protection, detection, response, and recovery processes to identify improvements. Independent teams, for example, may include internal or external impartial personnel.	
ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved	Low, Moderate, & High	Develop, communicate, maintain, and improve contingency plans (e.g., incident response, business continuity, disaster recovery, vulnerability management). Plans should define event types and incorporate recovery objectives, restoration priorities, resources, metrics, contingency roles, personnel assignments, management support, and contact information. Review and test contingency plans with relevant stakeholders to determine their effectiveness and readiness for execution. Address maintaining essential operational functions despite system disruption and the eventual restoration of the manufacturing system.	CP-02 IR-08 PL-02 SR-02

5.3. Protect

Table 11 Subcategory-level Guidance for the Protect Function

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization	Low	Establish and manage identification mechanisms and credentials for authorized users, services, and hardware of the manufacturing system. Physically label authorized hardware with an identifier for inventory and servicing purposes.	AC-01 AC-02 AC-14 IA-01 IA-02 IA-03 IA-04 IA-05 IA-06 IA-07 IA-08 IA-09 IA-10 IA-11
	Moderate	Implement automated mechanisms where feasible to support the management and auditing of user, services, and hardware accessing the manufacturing system environment. Disable system credentials after a specified period of inactivity, where safe and feasible.	
	High	Monitor the manufacturing system for atypical use of system credentials. Disable credentials associated with significant risk.	
PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions	Low & Moderate	Implement procedures for verifying the identity of individuals before issuing credentials that provide access to the manufacturing systems.	IA-12
	High	Issue unique credentials bound to each verified user, device, and process specific to each type of interaction with the manufacturing system (e.g., read-only access, write access).	

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
PR.AA-03: Users, services, and hardware are authenticated	Low	Authenticate manufacturing system users. Enforce policies for the minimum strength of passwords, PINs, use of multi-factor authentication, and similar authenticators.	AC-07 AC-12 IA-02 IA-03 IA-05 IA-07 IA-08 IA-09 IA-10 IA-11
	Moderate	Authenticate manufacturing system services and hardware.	
	High	Implement periodic reauthentication of manufacturing system users, services, and hardware. Implement multi-factor authentication for remote access to the manufacturing system.	
PR.AA-04: Identity assertions are protected, conveyed, and verified	Low & Moderate	None.	IA-13
	High	Protect identity assertions that are used to convey authentication and user information between federated systems.	
PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	Low	Define a policy, manage, and periodically review access permissions, entitlements, and authorizations for users of the manufacturing system. Incorporate the principles of least privilege for users of the manufacturing system. Identify and document actions that can be performed on the manufacturing system without identification or authentication (e.g., emergency stop). Review logical and physical access privileges periodically and whenever someone changes roles or leaves the organization and promptly rescind privileges that are no longer needed. Disable accounts of users posing a significant risk.	AC-01 AC-02 AC-03 AC-05 AC-06 AC-10 AC-16 AC-17 AC-18 AC-19 AC-24 IA-13

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
	Moderate	Implement separation of duties for manufacturing system users. Review user privileges periodically to maintain separation of duties (e.g., separating operational functions and system support functions, separating administration and audit functions). Minimize the number of privileged users of the manufacturing system. Audit the execution of privileged functions on the manufacturing system. Implement automated mechanisms where feasible to support the management of manufacturing system user accounts, entitlements, and authorizations, including the auditing, notification, disabling, and removal of user accounts. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed. Authorize each type of remote access to the system prior to allowing such connections.	
	High	Enforce account usage restrictions for specific time periods and locality (e.g., restricting usage to certain days of the week, time of day, or durations of time). Privileged user access through non-local connections to the manufacturing system is restricted and managed.	
PR.AA-06: Physical access to assets is managed, monitored, and enforced commensurate with risk	Low	Protect physical access to the manufacturing facility. Determine access requirements during emergency situations. Physical access controls may include, for example, lists of authorized individuals, identity credentials, escort requirements, guards, fences, turnstiles, locks, monitoring of facility access. Maintain and review visitor access records to the facility where the manufacturing system resides. Identify areas of the manufacturing system where guests, vendors, and other third parties should be escorted.	PE-02 PE-03 PE-04 PE-05 PE-06 PE-08 PE-18 PE-19 PE-20
	Moderate	Protect power equipment, power cabling, network cabling, and network access interfaces for the manufacturing system from accidental damage, disruption, and physical tampering. Ensure availability and integrity of wireless systems, especially safety related systems. Implement redundant and physically separated power systems for critical manufacturing operations.	
	High	Control physical access to the manufacturing system in addition to the physical access for the facility.	

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind	Low	Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind.	AT-02 AT-03
	Moderate & High	Provide all manufacturing system employees, contractors, partners, and suppliers periodic cybersecurity awareness and training (e.g., cybersecurity policies and procedures, personnel responsibilities, reporting suspected cybersecurity incidents, basic operational security).	
PR.AT-02: Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind	Low, Moderate, & High	Ensure that users and third-party providers with specialized roles and privileged access to the manufacturing system are provided with periodic role-based awareness training so they understand the requirements, responsibilities, and cybersecurity risks of their assignments. Ensure that senior executives understand the requirements for the security and protection of the manufacturing system, and their responsibilities for achieving them. Ensure that personnel responsible for the physical protection and security of the manufacturing system and facility are trained and understand their responsibilities.	AT-03

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected	Low	Protect the confidentiality, integrity, and availability of manufacturing system data-at-rest, including data stored on portable storage devices (e.g., USB memory sticks, compact disks, digital video disks, external/removable hard disk drives).	CA-03 CP-09 MP-08 SC-04 SC-07 SC-12 SC-13 SC-28 SC-32 SC-39 SC-43 SI-03 SI-04 SI-07
	Moderate	Protect and control portable storage devices containing manufacturing system data-at-rest while in storage. Perform a risk analysis to determine how data-at-rest is protected by vendor or third-party service providers and whether additional countermeasures should be implemented.	
	High	Implement automated tools where safe and feasible to detect loss of integrity or availability of data-at-rest. Implement automatic response capability where safe and feasible with pre-defined safeguards when integrity violations are discovered. Perform a risk analysis to determine how data-at-rest is protected and whether additional countermeasures should be implemented.	

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected	Low	Protect the confidentiality, integrity, and availability of manufacturing system data-in-transit. Monitor the manufacturing system at the external boundary and at key internal points to detect unauthorized information flows.	AU-16 CA-03 SC-04 SC-07 SC-08 SC-11 SC-12 SC-13 SC-16 SC-40 SC-43 SI-03 SI-04 SI-07
	Moderate	Regulate the information flow within the manufacturing system and to outside systems. Enforce controls restricting connections to only authorized interfaces. Heighten system monitoring activity whenever there is an indication of increased risk to manufacturing operations and assets. Protect and control portable storage devices containing manufacturing system data while in transit.	
	High	Protect the system from information leakage due to electromagnetic signals emanations (e.g., wireless communications).	

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected	Low	Protect the confidentiality, integrity, and availability of manufacturing system data-in-use. Monitor the manufacturing system at the external boundary and at key internal points to detect unauthorized use.	AC-02 AC-03 AC-04 AU-09 AU-13 CA-03 CP-09 SA-08 SC-04 SC-07 SC-11 SC-13 SC-24 SC-32 SC-39 SC-40 SC-43 SI-03 SI-04 SI-07 SI-10 SI-16
	Moderate	Heighten system monitoring activity whenever there is an indication of increased risk to manufacturing operations and assets. When safe and feasible, utilize memory-safe programming languages and technologies to minimize the risk that data-in-use is exploited.	
	High	Protect the system from information leakage due to electromagnetic signals emanations (e.g., wireless communications).	
PR.DS-11: Backups of data are created, protected, maintained, and tested	Low	Protect, maintain, and test backups for manufacturing system data (e.g., software, configurations and settings, documentation, system configuration data including computer configuration backups, application configuration backups, operational control limits, control bands, and set points).	CP-06 CP-09

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
	Moderate	Verify the reliability and integrity of backups periodically. Coordinate backup testing with organizational stakeholders. Establish a separate alternate storage site geographically separate from the manufacturing system source for manufacturing system data backups and ensure comparable security safeguards are employed as established for on-site data.	
	High	Conduct restorations from backup data as part of testing. Store critical manufacturing system backup information offline and offsite to limit damage exposure during an event or disaster.	
PR.PS-01: Configuration management practices are established and applied	Low	Implement configuration management practices for the manufacturing system and its components. Develop, document, and maintain a baseline configuration for the manufacturing system. Baseline configurations include, for example, information about manufacturing system components (e.g. software license information, software version numbers, HMI and other ICS component applications, software, operating systems, current version numbers and patch information on operating systems and applications, and configuration settings and parameters), network topology, and the logical placement of those components within the system architecture. Configure the manufacturing system to provide only essential capabilities. Review the baseline configuration and disable unnecessary capabilities. Conduct SIAs in connection with change control reviews.	CM-01 CM-02 CM-03 CM-04 CM-05 CM-06 CM-07 CM-08 CM-09 CM-10 CM-11
	Moderate	Review, authorize, test, validate, and document configuration changes to the manufacturing system before and after implementation on the operational system. Periodically review the manufacturing system for unauthorized changes. Review and update the baseline configuration of the manufacturing system as an integral part of system component installations and upgrades. Retain previous versions of the baseline configuration to support rollback. Develop a configuration management plan for the manufacturing system. The plan includes, for example, configuration processes, roles, lifecycle definition, configuration items, and control methods. Define configuration parameters, capabilities, and fail to known state procedures such that, upon a system failure (or failure conditions), assets revert to a state that achieves a predetermined mode of operation. Disable unnecessary functions, ports, protocols, and services within the manufacturing system.	

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
	High	Implement automated mechanisms where feasible to support the change management process and maintain an up-to-date, complete, accurate, and readily available baseline configuration of the manufacturing system. Automated system support includes for example, documentation, notification, and management of the change control process on the manufacturing system.	
PR.PS-02: Software is maintained, replaced, and removed commensurate with risk	Low	Establish and maintain a process to continuously perform routine and emergency vulnerability mitigation of manufacturing systems within the timeframes specified in the vulnerability management plan. Establish and maintain a process to manage (e.g., maintain, replace, remove) software and services supporting the manufacturing system. Implement access controls for remote maintenance and troubleshooting (e.g., vendors, third-party integrators).	CM-11 MA-03(06) SA-10(01) SI-02 SI-07
	Moderate & High	Remove any unnecessary or unauthorized software from the manufacturing system. Implement a remote maintenance management platform for software support that utilizes credentialed accounts, access authorization management, and access and activity logging. Restrict remote maintenance activities to only the assets being serviced and only for the duration required to perform the work.	
PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk	Low	Schedule, perform, document and review records of maintenance and repairs on manufacturing system components. Enforce accountability for all manufacturing system components throughout the system lifecycle, including during removal, transfer, and disposition steps. All system components entering and exiting the facility are authorized, monitored, and controlled, and records are maintained of those items. Sanitize portable media (e.g., wipe and verify integrity and fit-for-use) prior to disposal, release, or reuse. Define and implement a plan and process to manage hardware components within the manufacturing system that reach end-of-life or obsolescence (e.g., replacement with current, supported, and maintainable versions). Ensure that the maintenance, replacement, and removal of hardware are aligned with identified risks (e.g., in cases where hardware cannot be upgraded or removed, organizations should consider measures that mitigate associated risks). Establish a process for maintenance personnel authorization and monitoring the work performed. Enforce approval requirements, control, and monitoring of maintenance activities. Verify restoration and functionality of impacted security controls following maintenance or repairs.	CM-07(09) SA-10(03) SC-03(01) SC-39(01) SC-49 SC-51

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
	Moderate	Enforce approval requirements, control, and monitoring of maintenance tools for use on the manufacturing system. Inspect maintenance tools brought into the facility (e.g., diagnostic test equipment, network taps, and laptops). Scan maintenance tools and portable storage devices for malicious code before they are used on the manufacturing system. Update the manufacturing system inventory as part of hardware deployment and management (e.g., installations, removals, and system updates).	
	High	Implement automated mechanisms, where feasible, to schedule and document maintenance and repair activities. Prevent the unauthorized removal of maintenance equipment containing manufacturing system information. Ensure that hardware disposal actions are approved, tracked, documented, and verified.	
PR.PS-04: Log records are generated and made available for continuous monitoring	Low	Generate log records containing information that establishes the event type, timestamp, location, source, outcome, and identities associated with the event. Configure manufacturing system devices log generators to use a common time zone (e.g., Coordinated Universal Time (UTC)).	AU-02 AU-03 AU-06 AU-07 AU-11 AU-12
	Moderate	Generate alerts and trigger defined responses when log generators fail. Review and update log events. Implement automated mechanisms to integrate audit review, analysis, and reporting. Compare and synchronize the internal system clocks to an authoritative time source (e.g., NTP server, radio clock, GPS) to maintain consistent timestamps across all systems.	
	High	Extend system logging as required to address specific threat situations.	
PR.PS-05: Installation and execution of unauthorized software are prevented	Low	Monitor for the installation or execution of unauthorized software in the manufacturing system. Perform verification and integrity checks on authorized software prior to installation in the manufacturing system.	CM-07(02) CM-07(04) CM-07(05) SC-34
	Moderate & High	Configure systems to prevent the execution of unauthorized software. Prevent access to unauthorized or known-malicious domains.	

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
PR.PS-06: Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle	Low	Manage organization-developed and organization-managed manufacturing system software using a secure software development life cycle.	SA-03 SA-08 SA-10 SA-11 SA-15 SA-17
	Moderate & High	Apply security engineering principles into the specification, design, development, implementation, and modification of the manufacturing system software. Implement configuration management and change control for manufacturing system software. Protect all software and software components from tampering and unauthorized access. Review source code for vulnerabilities and develop mitigations for identified vulnerabilities.	
PR.IR-01: Networks and environments are protected from unauthorized logical access and usage	Low	Establish usage restrictions, connection requirements, implementation guidance, and authorizations for logical access to the manufacturing system networks and components (e.g., dial-up, broadband, Virtual Private Network (VPN) connections, mobile device connections). Incorporate network segmentation and segregation where appropriate. Identify connections and communications between system components. Implement boundary protection devices (e.g., routers, gateways, unidirectional gateways, data diodes, and firewalls) to separate system components into logically separate networks. Monitor and control network connections and communications at the external boundary and at key internal boundaries within the manufacturing system.	AC-03 AC-04 SC-04 SC-05 SC-07
	Moderate	Limit external connections to the manufacturing system through approved and managed access points. Establish agreements and verify security for connections with external systems. Implement deny-all, permit-by-exception network traffic policy to managed interfaces. Disable split tunneling and covert channel options in conjunction with remote devices. Implement an off-line development and testing environment for implementing and testing changes to the manufacturing system. Ensure external boundary protection devices fail securely, where safe and feasible, in the event of a critical device failure.	

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
	High	Require physical access controls to manage manufacturing system components identified as critical.	
PR.IR-02: The Organization's technology assets are protected from environmental threats	Low & Moderate	Protect the manufacturing systems from known environmental threats, such as flooding, fire, wind, and excessive heat and humidity. Implement and enforce policies and regulations regarding environment protection systems (e.g., emergency and safety systems, fire protection systems, and environment controls) for the manufacturing system. Protection mechanisms should consider impacts to the manufacturing system (e.g., water sprinkler systems could be hazardous in specific environments). Ensure service providers include environmental threat protections and provisions for adequate operating infrastructure.	CP-02 PE-09 PE-10 PE-11 PE-12 PE-13 PE-14 PE-15 PE-18 PE-23
	High	Implement protection systems that activate and notify key personnel automatically in the event of an incident.	
PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations	Low	None.	CP IR SA-08 SC-06 SC-24 SC-36 SC-39 SI-13
	Moderate	Identify and mitigate single points of failure within the systems and networks supporting the manufacturing system to maintain availability, data integrity, security, and operational resiliency.	
	High	Use high-availability networks and components (e.g., redundant power supplies, controllers, sensors) to improve system reliability.	
PR.IR-04: Adequate resource capacity to ensure availability is maintained	Low	Monitor and manage resource consumption (e.g., power consumption, computing resources, memory, storage, network bandwidth) of systems and networks supporting the manufacturing system.	CP-06 CP-07 CP-08 PM-03 PM-09

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
	Moderate & High	Protect the manufacturing system against denial-of-service attacks or limit its impact on manufacturing operation. Forecast future needs and scale resources accordingly to meet anticipated demands.	

5.4. Detect

Table 12 Subcategory-level Guidance for the Detect Function

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
DE.CM-01: Networks and network services are monitored to find potentially adverse events	Low	Enable logging on network devices to support monitoring. Monitor networks and network services at external boundaries and key internal boundaries within the manufacturing system to detect deviations from baselines (e.g., unauthorized or unexpected communications). Heighten network monitoring activity whenever there is an indication of increased risk.	AC-02 AU-12 CA-07 CM-03 SC-05 SC-07 SI-04
	Moderate	Continuously monitor networks and network services to detect potentially adverse events (e.g., indicators of compromise, unauthorized or unexpected communications, unauthorized access points, rogue devices) within the manufacturing system. Generate alerts when potentially adverse events or deviations from baselines are identified.	
	High	Use automated tools capable of analyzing industrial communication protocols to support continuous monitoring of networks and network services and alerting, where safe and feasible.	
DE.CM-02: The physical environment is monitored to find potentially adverse events	Low	Monitor physical access to manufacturing areas (e.g., entry logs, visitor registration). Inspect and maintain physical security controls (e.g., locks, gates, fences) during routine facility maintenance.	CA-07 PE-03 PE-06 PE-20
	Moderate	Implement environmental monitoring to detect conditions that could affect the manufacturing system (e.g., temperature, humidity, water, smoke). Implement physical access controls, surveillance, and automated alerts (e.g., badge readers, motion sensors, door sensors, video surveillance) to monitor critical areas of the manufacturing system (e.g., production areas, control rooms, areas containing sensitive equipment).	
	High	Correlate physical security events with cybersecurity events when performing incident investigations.	

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events	Low	Conduct ongoing security monitoring on the manufacturing system for unauthorized activities, unusual access patterns, and failed access attempts.	AC-02 AU-12 AU-13 CA-07 CM-10 CM-11
	Moderate & High	Detect anomalous user activity to mitigate insider threats.	
DE.CM-06: External service provider activities and services are monitored to find potentially adverse events	Low	Conduct ongoing security monitoring remote and onsite activities of external service providers on the manufacturing system (e.g., unauthorized external personnel, activities, connections, devices, access points, software). Generate alerts for adverse events and indicators of potentially adverse events from external service providers.	CA-07 PS-07 SA-04 SA-09 SI-04
	Moderate & High	Monitor compliance of external providers with personnel security policies and procedures, and contract security requirements.	
DE.CM-09: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	Low	Conduct ongoing security status monitoring on the manufacturing system for unauthorized connections, peripheral devices (e.g., removable media), and software. Deploy malicious code detection mechanisms where safe and feasible within the manufacturing environment. Update malicious code detection mechanisms periodically in accordance with configuration management policies and procedures for the manufacturing system. Monitor for system inventory discrepancies and unauthorized configuration changes to the manufacturing system.	AC-04 AC-09 AU-12 CA-07 CM-03 CM-06 CM-10 CM-11 SC-34 SC-35 SI-04 SI-07

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
	Moderate	Where safe and feasible, update malicious code detection and protection mechanisms automatically. Enforce usage restrictions and establish implementation guidance for acceptable mobile code (e.g., browser-based applications) for use within the manufacturing system. The use of mobile code technologies is determined after careful consideration. Deploy monitoring mechanisms strategically within the manufacturing system to collect essential information to detect specific events of interest. Implement integrity checks for hardware, software, firmware, and data to detect unauthorized changes to manufacturing system components.	
	High	Implement automated tools where feasible to provide notification upon discovering discrepancies during software integrity verification. Implement hardware integrity checks to detect unauthorized tampering (e.g. tamper-evident tape or labels, computer port protection, power-on self-tests, etc.) to manufacturing system hardware determined to be critical.	
DE.AE-02: Potentially adverse events are analyzed to better understand associated activities	Low	Review and analyze detected adverse events within the manufacturing system to understand attack targets, methods, and associated activities.	AU-06 CA-07 IR-04 SI-04
	Moderate & High	Implement automated mechanisms where feasible to review and analyze detected adverse events within the manufacturing system.	
DE.AE-03: Information is correlated from multiple sources	Low	Collect and aggregate log data from a variety of sources across the manufacturing system (e.g., authentication and access control systems, network devices, critical OT devices, and physical access systems).	AU-06 CA-07 PM-16 IR-04 IR-05 IR-08 SI-04
	Moderate	Correlate event data from multiple sources.	
	High	Implement event correlation technologies (e.g., SIEM, SOAR, XDR) to reduce the time to detect adverse events.	

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
DE.AE-04: The estimated impact and scope of adverse events are understood	Low	Determine negative impacts to manufacturing operations, assets, and individuals resulting from adverse events.	PM-09 PM-11 PM-18 PM-28 PM-30
	Moderate	Implement mechanisms to support impact analysis.	
	High	Correlate adverse event information to estimate impact across the organization.	
DE.AE-06: Information on adverse events is provided to authorized staff and tools	Low	Communicate adverse event detection information (e.g., atypical account usage, unauthorized remote access, wireless connectivity, mobile device connectivity, altered configuration settings, contrasting system component inventory, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, malware disclosure) to defined personnel.	IR-04 PM-15 PM-16 RA-03 RA-10
	Moderate & High	Implement automated mechanisms and system-generated alerts to communicate adverse event detection information.	
DE.AE-07: Cyber threat intelligence and other contextual information are integrated into the analysis	Low	None.	PM-16 RA-03 RA-10
	Moderate & High	Integrate and correlate cyber threat intelligence (CTI) feeds and manufacturing system vulnerabilities to analyze adverse events.	
DE.AE-08: Incidents are declared when adverse events meet the defined incident criteria	Low	Define incident criteria for the manufacturing system. Declare an incident when adverse events meet the defined incident criteria.	IR-04 IR-08
	Moderate & High	Implement automated mechanisms where feasible to assist in the identification of security alert criteria.	

5.5. Respond

Table 13 Subcategory-level Guidance for the Respond Function

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared	Low	Designate a lead for each incident. Execute the incident response plan once a manufacturing system cybersecurity incident is declared. Coordinate incident response actions with all relevant stakeholders (e.g., manufacturing system owners, integrators, vendors, human resources, physical and personnel security, legal departments, operations personnel, and procurement offices).	IR-06 IR-07 IR-08 SR-03 SR-08
	Moderate & High	Employ automated mechanisms to support stakeholder coordination.	
RS.MA-02: Incident reports are triaged and validated	Low, Moderate, & High	Review incident reports to confirm that they are cybersecurity-related and necessitate incident response activities. Apply criteria to estimate the severity of an incident.	IR-04 IR-05 IR-06
RS.MA-03: Incidents are categorized and prioritized	Low, Moderate, & High	Categorize cybersecurity incidents based on the type of incident (e.g., data breach, ransomware, DDoS, account compromise) and the level of severity and impact consistent with the response plan. Prioritize incidents based on their scope, likely impact, and time-critical nature.	IR-04 IR-05 IR-06
RS.MA-04: Incidents are escalated or elevated as needed	Low, Moderate, & High	Track and validate the status of all ongoing incidents and escalate as needed. Coordinate incident escalation or elevation with designated internal and external stakeholders.	IR-04 IR-05 IR-06 IR-07
RS.MA-05: The criteria for initiating incident recovery are applied	Low, Moderate, & High	Apply incident recovery criteria to known and assumed characteristics of the incident to determine whether incident recovery processes should be initiated.	IR-04 IR-08
RS.AN-03: Analysis is performed to establish what has taken place during an incident and the root cause of the incident	Low, Moderate, & High	Conduct analysis on collected cybersecurity event information to determine root cause. Determine the sequence of adversarial behavior and events that resulted in the incident. Identify which assets and resources were involved in each event. Determine what vulnerabilities, threats, and threat actors were directly or indirectly involved in the incident.	AU-07 IR-04

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
RS.AN-06: Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved	Low, Moderate, & High	Require incident responders (e.g., system administrators, cybersecurity engineers) to record their actions. Require the incident lead to be responsible for preserving the integrity of the records.	AU-07 IR-04 IR-06
RS.AN-07: Incident data and metadata are collected, and their integrity and provenance are preserved	Low, Moderate, & High	Collect, preserve, and safeguard the integrity of all pertinent incident data and metadata (e.g., data source, date/time of collection) based on evidence preservation and chain-of-custody procedures. Require the incident lead to be responsible for preserving the integrity of the data.	AU-07 IR-04 IR-06
RS.AN-08: An incident's magnitude is estimated and validated	Low	Understand the full implication of the manufacturing system cybersecurity incident to estimate the magnitude of the impact. Review other potential targets of the incident to search for indicators of compromise and evidence of persistence.	IR-04 IR-08 RA-03 RA-07
	Moderate & High	Implement automated mechanisms, where safe and feasible, to search for indicators of compromise and evidence of persistence.	
RS.CO-02: Internal and external stakeholders are notified of incidents	Low	Follow the organization's notification procedures after a manufacturing system cybersecurity incident is declared. Notify all relevant stakeholders (e.g., affected customers business partners, law enforcement agencies, regulatory bodies) of the incident in accordance with contractual requirements, incident response plan criteria, and management approval.	IR-04 IR-06 IR-07 SR-03 SR-08
	Moderate & High	Employ automated mechanisms to assist in the reporting of manufacturing system cybersecurity incidents.	

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
RS.CO-03: Information is shared with designated internal and external stakeholders	Low, Moderate, & High	Share cybersecurity incident information with relevant stakeholders per the response plan. Regularly update senior leadership on the status of major incidents. Share cybersecurity incident information, as appropriate, with relevant industry security groups (e.g., Information Sharing and Analysis Center (ISAC)) to achieve broader cybersecurity.	IR-04 IR-06 IR-07 SR-03 SR-08
RS.MI-01: Incidents are contained	Low	Contain cybersecurity incidents to minimize impact on the manufacturing system.	IR-04
	Moderate & High	Configure cybersecurity technologies (e.g., antivirus software, intrusion protection systems) to contain incidents and minimize impact on the manufacturing system, where safe and feasible. Coordinate with third party service providers (e.g., managed security service providers) to perform incident containment actions.	
RS.MI-02: Incidents are eradicated	Low	Mitigate cybersecurity incidents to minimize impact on the manufacturing system.	IR-04
	Moderate & High	Configure cybersecurity technologies (e.g., antivirus software, intrusion protection systems) to eradicate incidents and minimize impact on the manufacturing system, where safe and feasible. Coordinate with third party service providers (e.g., managed security service providers) to perform incident eradication actions.	

5.6. Recover

Table 14 Subcategory-level Guidance for the Recover Function

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
RC.RP-01: The recovery portion of the incident response plan is executed once initiated from the incident response process	Low & Moderate	Execute the recovery portion of the incident response plan during or after a cybersecurity incident on the manufacturing system.	CP-10 IR-04 IR-08
	High	Continue essential manufacturing functions and services with minimal or no loss of operational continuity and sustain continuity until full system restoration.	
RC.RP-02: Recovery actions are selected, scoped, prioritized, and performed	Low, Moderate, & High	Select, scope, and prioritize the recovery actions to be performed during the recovery phase of the incident response based on the criteria defined in the incident response plan and availability of resources. Perform the prioritized recovery actions, ensuring they align with the organization's needs, and adjust the planned recovery actions based on evolving requirements. Restore the manufacturing system within a predefined time-period from configuration-controlled and integrity-protected backup representing a known, operational state for the components.	CP-10 IR-04 IR-08
RC.RP-03: The integrity of backups and other restoration assets is verified before using them for restoration	Low, Moderate, & High	Verify the integrity of backups and other restoration assets (e.g., software, configurations and settings, documentation, operational control limits, control bands, set points) before using them for restoration. Check backups for indicators of compromise, file corruption, and other integrity issues before restoration.	CP-02 CP-04 CP-09
RC.RP-04: Critical mission functions and cybersecurity risk management are considered to establish post-	Low, Moderate, & High	Establish post-incident operational norms for essential manufacturing system services, functions, and assets. Prioritize and sequence the restoration of essential services that support the manufacturing system.	PM-08 PM-09 PM-11 IR-01 IR-08

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
incident operational norms			
RC.RP-05: The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed	Low, Moderate, & High	Verify the integrity of restored assets for indicators of compromise and remediation of root causes of the incident. Verify the correctness and adequacy of the restoration actions taken for assets before these systems are placed in production. Confirm successful restoration and operation of the manufacturing system and monitor its performance.	CP-10
RC.RP-06: The end of incident recovery is declared based on criteria, and incident-related documentation is completed	Low, Moderate, & High	Declare the end of the recovery portion of the incident response plan when the criteria are met. Prepare incident-related documentation, including after-action reports, response and recovery actions taken, and lessons learned.	IR-04 IR-08
RC.CO-03: Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders	Low, Moderate, & High	Communicate recovery activities (e.g., key milestones, restoration progress) to internal stakeholders and senior leadership. Communicate incident-related information to external stakeholders and critical suppliers consistent with established agreements and obligations.	IR-04 IR-06 SR-08
RC.CO-04: Public updates on incident recovery are shared using approved methods and messaging	Low	Centralize and coordinate information distribution to the public and follow organizational procedures for information sharing (e.g., handling and triaging phone calls and e-mail requests, screening all of information provided to the media, managing media interactions and interviews, ensuring personnel are familiar with public relations and privacy policies). Implement a response strategy (e.g., actions to shape attributions of the incident, change perceptions of the organization in incident) to protect against negative impact and repair organizational reputation.	CP-02 IR-04
	Moderate	Assign a Public Relations Officer.	

CSF Element and Description	L/M/H	Recommendations, Considerations, Notes	Informative References and Mappings
	High	Establish media contacts and third parties to manage public relations.	

References

[1] Executive Order 13636 (2013) Improving Critical Infrastructure Cybersecurity. (The White House, Washington, DC), DCPD-201300091, February 12, 2013. https://www.govinfo.gov/app/details/DCPD-201300091

[2] Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. (2017, May 16). Federal Register. https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure

[3] National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework 2.0 . (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.29

[4] Stouffer, K. , Pease, M. , Tang, C. , Zimmerman, T. , Pillitteri, V. , Lightman, S. , Hahn, A. , Saravia, S. , Sherule, A. and Thompson, M. (2023), Guide to Operational Technology (OT) Security, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD. https:/doi.org/10.6028/NIST.SP.800-82r3

[5] Joint Task Force Transformation Initiative (2020) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5. https://doi.org/10.6028/NIST.SP.800-53r5

[6] The International Society of Automation (2020) *ISA99, Industrial Automation and Control Systems Security*. https://www.isa.org/isa99/ [ISA/IEC 62443 Series of Standards on Industrial Automation and Control Systems (IACS) Security.]

[7] Computer Security Division Information Technology Laboratory (2004) Standards for Security Categorization of Federal Information and Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Federal Information Processing Standard (FIPS) Publication (PUB) 199. https://doi.org/10.6028/NIST.FIPS.199

Appendix A. List of Symbols, Abbreviations, and Acronyms

Selected acronyms and abbreviations used in the Profile are defined below.

AI
Artificial Intelligence

C-SCRM
Cybersecurity Supply Chain Risk Management

CAN
Controller Area Network

CISO
Chief Information Security Officer

CNC
Computer Numerical Control

CSF
Cybersecurity Framework

CTI
Cyber Threat Intelligence

CUI
Controlled Unclassified Information

DCS
Distributed Control System

DDoS
Distributed Denial of Service

EDR
Endpoint Detection and Response

ERM
Enterprise Risk Management

FIPS
Federal Information Processing Standards

GPS
Global Positioning System

HMI
Human Machine Interface

ICS
Industrial Control System

IEC
International Electrotechnical Commission

IIoT
Industrial Internet of Things

ISA
The International Society of Automation

ISAC
Information Sharing and Analysis Center

IT
Information Technology

KPI
Key Performance Indicator

KRI
Key Risk Indicator

LAN
Local Area Network

NIST
National Institute of Standards and Technology

NTP
Network Time Protocol

NVD
National Vulnerability Database

OT
Operational Technology

PLC
Programmable Logic Controller

QA
Quality Assurance

RF
Radio Frequency

RPO
Recovery Point Objective

RTU
Remote Terminal Unit

SCADA
Supervisory Control and Data Acquisition

SIA
Security Impact Analysis

SIEM
Security Information and Event Management

493 **SOAR**
494 Security Orchestration, Automation and Response

495 **SP**
496 (NIST) Special Publication

497 **TTPs**
498 Tactics, Techniques, and Procedures

499 **US-CERT**
500 United States Computer Emergency Readiness Team

501 **USB**
502 Universal Serial Bus

503 **UTC**
504 Coordinated Universal Time

505 **VPN**
506 Virtual Private Network

507 **XDR**
508 eXtended Detection and Response

Appendix B. Glossary

Selected terms used in the Profile are defined below.

business/mission objectives
Broad expression of business goals. Specified target outcome for business operations.

capacity planning
Systematic determination of resource requirements for the projected output, over a specific period. [businessdictionary.com]

category
The subdivision of a CSF function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities.

critical infrastructure
Essential services and related assets that underpin American society and serve as the backbone of the nation's economy, security, and health. [DHS]

criticality reviews
A determination of the ranking and priority of manufacturing system components, services, processes, and inputs in order to establish operational thresholds and recovery objectives.

critical services
The subset of mission essential services required to conduct manufacturing operations. Function or capability that is required to maintain health, safety, the environment and availability for the equipment under control. [62443]

cyber risk
Risk of financial loss, operational disruption, or damage, from the failure of the digital technologies employed for informational and/or operational functions introduced to a manufacturing system via electronic means from the unauthorized access, use, disclosure, disruption, modification, or destruction of the manufacturing system.

cybersecurity
The process of protecting information by preventing, detecting, and responding to attacks. [CSF]

defense-in-depth
The application of multiple countermeasures in a layered or stepwise manner to achieve security objectives. The methodology involves layering heterogeneous security technologies in the common attack vectors to ensure that attacks missed by one technology are caught by another. [62443 1-1]

environmental support
Any environmental factor for which the organization determines that it needs to continue to provide support in a contingency situation, even if in a degraded state. This could include factors such as power, air conditioning, humidity control, fire protection, lighting, etc.

For example, while developing the contingency plan, the organization may determine that it is necessary to continue to ensure the appropriate temperature and humidity during a contingency situation so they would plan for the capacity to support that via supplemental/mobile air conditioning units, backup power, etc. and the associated procedures to ensure cutover operations. Such determinations are based on an assessment of risk, system categorization (impact level), and organizational risk tolerance.

event
Any observable occurrence on a manufacturing system. Events can include cybersecurity changes that may have an impact on manufacturing operations (including mission, capabilities, or reputation). [CSF]

fail to known state
Upon a disruption event that causes the system to fail, it fails to a pre-determined state. Failure in a known safe state helps to prevent systems from failing to a state that may cause injury to individuals or destruction to property. Preserving manufacturing system state information facilitates system restart and return to the operational mode of organizations with less disruption of mission/business processes. [NVD.NIST]

firmware
Software program or set of instructions programmed on the flash ROM of a hardware device. It provides the necessary instructions for how the device communicates with the other computer hardware. [Techterms.com]

framework
The Cybersecurity Framework developed for defining protection of critical infrastructure. It provides a common language for understanding, managing, and expressing cybersecurity risk both internally and externally. Includes activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes.

function
Primary unit within the Cybersecurity Framework. Exhibits basic cybersecurity activities at their highest level.

incident
An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. [CSF]

informative references
Specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory in the Cybersecurity Framework.

integrator
A value-added engineering organization that focuses on industrial control and information systems, manufacturing execution systems, and plant automation, that has application knowledge and technical expertise, and provides an integrated solution to an engineering problem. This solution includes final project engineering, documentation, procurement of hardware, development of custom software, installation, testing, and commissioning. [CSIA.com]

manufacturing operations
Activities concerning the facility operation, system processes, materials input/output, maintenance, supply and distribution, health, and safety, emergency response, human resources, security, information technology and other contributing measures to the manufacturing enterprise.

manufacturing system data
Software, configurations and settings, documentation, system configuration data including computer configuration backups, application configuration backups, operational control limits, control bands, and set points.

network access
Any access across a network in lieu of local access (i.e., user being physically present at the device).

non-local connection
A connection to the manufacturing system affording the user access to system resources and system functionality while physically not present.

non-technology-based input product
Manufactured component parts or materials used in the organization manufacturing process that do not incorporate information technology and are provided by third parties.

overlay
A fully specified set of security controls, control enhancements, and supplemental guidance derived from tailoring a security baseline to fit the user's specific environment and mission. [800-53]

operational technology
Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise. [Gartner.com]

programmable logic controller
A solid-state control system that has a user-programmable memory for storing instructions for the purpose of implementing specific functions such as I/O control, logic, timing, counting, three mode (PID) control, communication, arithmetic, and data and file processing. [800-82]

port
The entry or exit point from a computer for connecting communications or peripheral devices. [800-82]

profile
A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories. [CSF]

Target Profile: The desired outcome or 'to be' state of cybersecurity implementation.

Current Profile: The 'as is' state of system cybersecurity.

protocol
A set of rules (i.e., formats and procedures) to implement and control some type of association (e.g., communication) between systems. [800-82]

remote access
Access by users (or information systems) communicating external to an information system security perimeter. Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device). [800-53]

resilience requirements
The business-driven availability and reliability characteristics for the manufacturing system that specify recovery tolerances from disruptions and major incidents.

risk assessment
The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis. Incorporates threat and vulnerability analyses. [800-82]

risk tolerance
The level of risk that the Manufacturer is willing to accept in pursuit of strategic goals and objectives. [800-53]

router
A computer that is a gateway between two networks at OSI layer 3 and that relays and directs data packets through that inter-network. The most common form of router operates on IP packets. [800-82]

security control
The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for a system to protect the confidentiality, integrity, and availability of the system, its components, processes, and data. [800-82]

subcategory
The subdivision of a Category into specific outcomes of technical and/or management activities. Examples of Subcategories include “External information systems are catalogued,” “Data-at-rest is protected,” and “Notifications from detection systems are investigated.” [CSF]

supporting services
Providers of external system services to the manufacturer through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges. Supporting services include, for example, Telecommunications, engineering services, power, water, software, tech support, and security. [800-53]

switch
A device that channels incoming data from any of multiple input ports to the specific output port that will take the data toward its intended destination. [Whatis.com]

system categorization
The characterization of a manufacturing system, its components, and operations, based on an assessment of the potential impact that a loss of availability, integrity, or confidentiality would have on organizational operations, organizational assets, or individuals. [FIPS 199]

technology-based input product
Manufactured components used in the organization manufacturing process incorporating information technology and provided by third-parties (e.g. PLC, Sensors, Data Collection Systems, Workstations, Servers, etc).

third-party relationships
Relationships with external entities. External entities may include, for example, service providers, vendors, supply-side partners, demand-side partners, alliances, consortiums, and investors, and may include both contractual and non-contractual parties. [DHS]

third-party providers
Service providers, integrators, vendors, telecommunications, and infrastructure support that are external to the organization that operates the manufacturing system.

thresholds
Values used to establish concrete decision points and operational control limits to trigger management action and response escalation.

Appendix C. Change Log

This revision of the CSF Manufacturing Profile provides the following updates:

- Realigned guidance to CSF 2.0 Functions, including guidance for the new Govern Function
- Realigned guidance to CSF 2.0 Categories (changed from 23 in CSF 1.1 to 22 in CSF 2.0)
- Realigned guidance to CSF 2.0 Subcategories (changed from 108 in CSF 1.1 to 106 in CSF 2.0)
- Added guidance for CSF 2.0 supply chain risk management, platform security, and technology infrastructure resilience Categories