NISTIR 8183
Revision 1

Cybersecurity Framework Version 1.1 Manufacturing Profile

Keith Stouffer
Timothy Zimmerman
CheeYee Tang
Joshua Lubell
Jeffrey Cichonski
Michael Pease
John McCarthy

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8183r1

National Institute of
Standards and Technology
U.S. Department of Commerce

NISTIR 8183
Revision 1

Cybersecurity Framework Version 1.1 Manufacturing Profile

Keith Stouffer
Timothy Zimmerman
CheeYee Tang
Michael Pease
Intelligent Systems Division
Engineering Laboratory

Joshua Lubell
Systems Integration Division
Engineering Laboratory

Jeffrey Cichonski
Applied Cybersecurity Division
Information Technology Laboratory

John McCarthy
Dakota Consulting, Inc.
Silver Spring, MD

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8183r1

October 2020

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

National Institute of Standards and Technology Internal Report 8183 Revision 1
60 pages (October 2020)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8183r1

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment 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. All NIST Computer Security Division publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

Comments on this publication may be submitted to:

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

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

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.

Abstract

This document provides the Cybersecurity Framework (CSF) Version 1.1 implementation details developed for the manufacturing environment. The "Manufacturing Profile" of the CSF can be used as a roadmap for reducing cybersecurity risk for manufacturers that is aligned with manufacturing sector goals and industry best practices. This Manufacturing Profile provides a voluntary, risk-based approach for managing cybersecurity activities and reducing cyber risk to manufacturing systems. The Manufacturing Profile is meant to enhance but not replace current cybersecurity standards and industry guidelines that the manufacturer is embracing.

Keywords

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

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. A special acknowledgement to the members of the Department of Homeland Security Industrial Control System Joint Working Group (ICSJWG) for their exceptional contributions to this publication.

Note to Readers on the Update

NISTIR 8183 Revision 1 updates the Manufacturing Profile to include the sub-category enhancements established in NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. These updates include managing cybersecurity within the supply chain, self-assessing cybersecurity risk, vulnerability disclosure, system integrity, and more comprehensive controls for identity management. Additional changes include updating language to change references from “security levels” to “impact levels.”

Patent Disclosure Notice

NOTICE: ITL has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

Executive Summary

This document provides the Cybersecurity Framework implementation details developed for the manufacturing environment. The "Manufacturing Profile" of the Cybersecurity Framework can be used as a roadmap for reducing cybersecurity risk for manufacturers that is aligned with manufacturing sector goals and industry best practices.

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 control 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 built around the primary functional areas of the Cybersecurity Framework which enumerate the most basic functions of cybersecurity activities. The five primary functional areas are: Identify, Protect, Detect, Respond, and Recover. These primary functional areas comprise a starting point from which to develop a manufacturer-specific or sector-specific Profile at the defined risk levels of Low, Moderate and High.

This Manufacturing "Target" Profile focuses on desired cybersecurity outcomes and can be used as a roadmap to identify opportunities for improving the current cybersecurity posture of the manufacturing system. The Manufacturing Profile provides a prioritization of security activities to meet specific business/mission goals. Relevant and actionable security practices that can be implemented to support key business/mission goals are then identified.

This Manufacturing Profile provides a voluntary, risk-based approach for managing cybersecurity activities and reducing cyber risk to manufacturing systems. The Manufacturing Profile is meant to enhance but not replace current cybersecurity standards and industry guidelines that the manufacturer is embracing.

Table of Contents

1. Introduction

The Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," [1] directed the development of the voluntary Cybersecurity Framework that provides a prioritized, flexible, repeatable, performance-based, and cost-effective approach to manage cybersecurity risk [1] for those processes, information, and systems directly involved in the delivery of critical infrastructure services.

The Cybersecurity Framework is a voluntary, risk-based assemblage of industry standards and best practices designed to help organizations manage cybersecurity risks [2]. The Framework, created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without imposing additional regulatory requirements.

The Manufacturing Profile (Profile) defines specific cybersecurity activities and outcomes for the protection of the manufacturing system, its components, facility, and environment. Through use of the Profile, the manufacturer can align cybersecurity activities with business requirements, risk tolerances, and resources. The Profile provides a manufacturing sector-specific approach to cybersecurity from standards, guidelines, and industry best practices.

1.1 Purpose and Scope

This document represents a "Target" Profile that focuses on the desired cybersecurity outcomes and provides an approach to the desired state of cybersecurity posture of the manufacturing system. It can be used to identify opportunities for improving a cybersecurity posture by comparing the current state with the desired (Target) state. Creating a Target Profile is Step 5 of Section 3.2: Establishing or Improving a Cybersecurity Program of the Cybersecurity Framework, Version 1.1 [2]. The Target Profile can also be used for comparison with the current state to influence process improvement priorities for the organization. The manufacturing system's "Current" Profile represents the outcomes from the Framework Core that are currently being achieved.

The Manufacturing "Target" Profile focuses on desired cybersecurity outcomes and can be used as a guideline to identify opportunities for improving the current cybersecurity posture of the manufacturing system. The Manufacturing Profile provides a prioritization of security activities to meet specific business/mission goals. Relevant and actionable security practices that can be implemented to support key business/mission goals are then identified.

Comparison of Profiles (e.g., the Current Profile and Target Profile) may reveal gaps to be addressed to meet cybersecurity risk management objectives. Prioritization of gap mitigation is driven by the organization's business needs and risk management processes. This risk-based approach enables an organization to gauge resource estimates (e.g., staffing, funding) to achieve cybersecurity goals in a cost-effective, prioritized manner. The following are examples of how the Target Profile may be used:

- A manufacturer may utilize the Target Profile to express cybersecurity risk management requirements to an external service provider.

- A manufacturer may express a system's cybersecurity state through a Current Profile to report results relative to the Target Profile, or to compare with acquisition requirements.
- A critical infrastructure owner/operator, having identified an external partner upon whom that infrastructure depends, may use the Target Profile to convey required cybersecurity outcomes.
- A critical infrastructure sector may establish a baseline that can be used among its constituents as a sector-specific starting point from which to build tailored Target Profiles.

The Manufacturing Profile provides a voluntary, risk-based approach for managing cybersecurity activities and reducing cyber risk to manufacturing systems.

1.2 Audience

This document covers details specific to manufacturing systems. Readers of this document should be acquainted with operational technology, 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, engineers, and other information technology (IT) professionals who administer, patch, or secure manufacturing systems.
- 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 *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework).
- Section 4 discusses the manufacturing profile development approach.
- Section 5 provides rationale for integrating cybersecurity into manufacturing Business/mission objectives.
- Section 6 discusses cyber risk management and the risk categorization of the manufacturing system.
- Section 7 provides the manufacturing implementation of the CSF subcategories.
- References provides 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.

2. Overview of Manufacturing Systems

Industrial Control Systems (ICS), which include manufacturing systems, represent different types of control systems including supervisory control and data acquisitions (SCADA) systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLCs) often found in the industrial sectors and critical infrastructures. An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, and pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy). ICS support the large and diverse manufacturing industrial sector and can be categorized as either *process-based, discrete-based,* or a combination of both [3].

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 the distinct end 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, to support both process-based and discrete-based manufacturing processes, manufacturers must also manage the supply chain for both technology-based inputs used in their final products (e.g. programmable logic controllers, 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 utilized to manufacture the final product).

Manufacturing industries are usually located within a confined factory or plant-centric area. Communications in manufacturing industries are typically performed using fieldbus and local area network (LAN) technologies that are reliable and high speed. Wireless networking technologies are gaining popularity in manufacturing industries. Fieldbus includes, for example, DeviceNet, Modbus, and Controller Area Network (CAN) bus.

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 the distinct critical infrastructure sector perform functions that are supported by ICS and by information technology (IT). This reliance on technology, communication, and the interconnectivity of ICS and IT has changed and expanded the potential vulnerabilities and increased potential risk to manufacturing system operations.

3. Overview of the Cybersecurity Framework

The Profile defines specific practices to address the Framework Core. It is the next layer of detail for implementing cybersecurity best practices for each category expressed in the Framework.

3.1 Framework Core

The Framework Core is a set of cybersecurity activities and desired outcomes determined to be essential across critical infrastructure sectors [2]. The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level. The Framework Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the organization's management of cybersecurity risk. The Framework Core then identifies underlying key Categories and Subcategories for each Function and matches them with example Informative References such as existing standards, guidelines, and practices for each Subcategory [2].

The five Framework Functions can be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk.

Table 1 Cybersecurity Framework Functions and Categories

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Management
PR	Protect	PR.AC	Identity Management, Authentication and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

The five "functions" of the Framework Core are:

Identify – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

Protect – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The activities in the Protect Function support the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

Detect – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The activities in the Detect Function enable timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

Respond – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. The activities in the Respond Function support the ability to contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

Recover – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. The activities in the Recover Function support timely recovery to normal operations to reduce the impact from a cybersecurity event. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.

The Manufacturing Profile for the Cybersecurity Framework presents detailed implementation language for the cybersecurity standards expressed in the Framework categories and subcategories. The Profile is intended to support cybersecurity outcomes based on business needs that the manufacturer has selected from the Framework Categories and Subcategories [2]. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a practical implementation scenario.

4. Manufacturing Profile Development Approach

The Profile was developed to be an actionable approach for implementing the CSF subcategories into a manufacturing system and its environment. The specific statements in the subcategories in Section 7 are derived from the security controls from ISA/IEC 62443 [5] and the NIST SP 800-53 Rev. 4 [4] and are customized to the manufacturing domain using relevant informative references. Control Objectives for Information and Related Technologies (COBIT) 5 is sourced for subcategories that have no corresponding 800-53 or ISA/IEC 62443 references. Additional input came from NIST SP 800-82, Rev. 2, both in section 6.2 (Guidance on the Application of Security Controls to ICS) and in Appendix G (ICS Overlay) [3]. For informative references to an entire control family or set of controls (such as subcategory ID.GV-1's informative reference to all "policy and procedures" controls), the approach took a holistic view of the controls comprising the family/set.

Section 7 provides the customized CSF subcategory language developed using informative references relevant to the manufacturing domain. In the Reference column in Section 7, hyperlinks are provided to the specific and relevant source influences for the subcategory statements.

The Profile expresses tailored values for cybersecurity controls for the manufacturing system environment. These represent the application of the Categories and Subcategories from the Framework based on domain-specific relevance, business drivers, risk assessment, and the manufacturer's priorities. Users of the Profile can also add Categories and Subcategories as needed to address unique and specific risks.

5. Manufacturing Business/Mission Objectives

The development of the Profile included the identification of common business/mission objectives to the manufacturing sector. These business/mission objectives provide the necessary context for identifying and managing applicable cybersecurity risk mitigation pursuits [2]. Five common business/mission objectives for the manufacturing sector were initially identified: *Maintain Human Safety, Maintain Environmental Safety, Maintain Quality of Product, Maintain Production Goals,* and *Maintain Trade Secrets.* Other business/mission objectives were identified for the manufacturing sector but not included in this initial profile. Key cybersecurity practices are identified for supporting each business/mission objective, allowing users to better prioritize actions and resources according to the user's defined needs.

These Business/Mission Objectives Are Not Listed in Prioritized Order.

Maintain Environmental Safety
Manage cybersecurity risks that could adversely affect the environment, including both accidental and deliberate damage. Cybersecurity risk on the manufacturing system could potentially adversely affect environmental safety. Personnel should understand cybersecurity and environmental safety interdependencies.

Maintain Human Safety
Manage cybersecurity risks that could potentially impact human safety. Cybersecurity risk on the manufacturing system could potentially adversely affect human safety. Personnel should understand cybersecurity and safety interdependencies.

Maintain Production Goals
Manage cybersecurity risks that could adversely affect production goals. Cybersecurity risk on the manufacturing system, including 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 product. Protect against compromise of 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 intellectual property and sensitive business data including personally identifiable information (PII).

5.1 Alignment of Subcategories to Meet Mission Objectives

To align cybersecurity goals with overall mission success, the Profile subcategories are prioritized in order to support specific business/mission objectives. This allows the manufacturer to focus on implementing those cybersecurity measures against threats that could directly and severely compromise their ability to perform their essential mission.

For each business/mission objective, the most critical Subcategories initially determined to support the objective are highlighted in the tables under each Function. The selection of Subcategories to business/mission objectives was based on a broad range of manufacturing sectors and operations. The most critical Subcategories may differ for individual manufacturers.

Identify *- The Identify Function is critical in the development of the foundation for cybersecurity management, and in the understanding of cyber risk to systems, assets, data, and capabilities.*

Table 2 *IDENTIFY Business Mission Objectives*

		Maintain Human Safety	Maintain Environmental Safety	Maintain Quality of Product	Maintain Production Goals	Maintain Trade Secrets
	Category	Subcategories				
ID	Asset Management	ID.AM-1	ID.AM-1	ID.AM-1	ID.AM-1	ID.AM-1
		ID.AM-2	ID.AM-2	ID.AM-2	ID.AM-2	ID.AM-2
		ID.AM-3	ID.AM-3	ID.AM-3	ID.AM-3	ID.AM-3
		ID.AM-4	ID.AM-4	ID.AM-4	ID.AM-4	ID.AM-4
		ID.AM-5	ID.AM-5	ID.AM-5	ID.AM-5	ID.AM-5
		ID.AM-6	ID.AM-6	ID.AM-6	ID.AM-6	ID.AM-6
	Business Environment	ID.BE-1	ID.BE-1	ID.BE-1	ID.BE-1	ID.BE-1
		ID.BE-2	ID.BE-2	ID.BE-2	ID.BE-2	ID.BE-2
		ID.BE-3	ID.BE-3	ID.BE-3	ID.BE-3	ID.BE-3
		ID.BE-4	ID.BE-4	ID.BE-4	ID.BE-4	ID.BE-4
		ID.BE-5	ID.BE-5	ID.BE-5	ID.BE-5	ID.BE-5
	Governance	ID.GV-1	ID.GV-1	ID.GV-1	ID.GV-1	ID.GV-1
		ID.GV-2	ID.GV-2	ID.GV-2	ID.GV-2	ID.GV-2
		ID.GV-3	ID.GV-3	ID.GV-3	ID.GV-3	ID.GV-3
		ID.GV-4	ID.GV-4	ID.GV-4	ID.GV-4	ID.GV-4
	Risk Assessment	ID.RA-1	ID.RA-1	ID.RA-1	ID.RA-1	ID.RA-1
		ID.RA-2	ID.RA-2	ID.RA-2	ID.RA-2	ID.RA-2
		ID.RA-3	ID.RA-3	ID.RA-3	ID.RA-3	ID.RA-3
		ID.RA-4	ID.RA-4	ID.RA-4	ID.RA-4	ID.RA-4
		ID.RA-5	ID.RA-5	ID.RA-5	ID.RA-5	ID.RA-5
		ID.RA-6	ID.RA-6	ID.RA-6	ID.RA-6	ID.RA-6
	Risk Management Strategy	ID.RM-1	ID.RM-1	ID.RM-1	ID.RM-1	ID.RM-1
		ID.RM-2	ID.RM-2	ID.RM-2	ID.RM-2	ID.RM-2
		ID.RM-3	ID.RM-3	ID.RM-3	ID.RM-3	ID.RM-3
	Supply Chain Management	ID.SC-1	ID.SC-1	ID.SC-1	ID.SC-1	ID.SC-1
		ID.SC-2	ID.SC-2	ID.SC-2	ID.SC-2	ID.SC-2
		ID.SC-3	ID.SC-3	ID.SC-3	ID.SC-3	ID.SC-3
		ID.SC-4	ID.SC-4	ID.SC-4	ID.SC-4	ID.SC-4
		ID.SC-5	ID.SC-5	ID.SC-5	ID.SC-5	ID.SC-5

Protect *– The Protect Function is critical to limit the impact of a potential cybersecurity event.*

Table 3 *PROTECT Business Mission Objectives*

		Maintain Human Safety	Maintain Environmental Safety	Maintain Quality of Product	Maintain Production Goals	Maintain Trade Secrets
Category		Subcategories				
PR	Identity Management, Authentication and Access Control	PR.AC-1	PR.AC-1	PR.AC-1	PR.AC-1	PR.AC-1
		PR.AC-2	PR.AC-2	PR.AC-2	PR.AC-2	PR.AC-2
		PR.AC-3	PR.AC-3	PR.AC-3	PR.AC-3	PR.AC-3
		PR.AC-4	PR.AC-4	PR.AC-4	PR.AC-4	PR.AC-4
		PR.AC-5	PR.AC-5	PR.AC-5	PR.AC-5	PR.AC-5
		PR.AC-6	PR.AC-6	PR.AC-6	PR.AC-6	PR.AC-6
		PR.AC-7	PR.AC-7	PR.AC-7	PR.AC-7	PR.AC-7
	Awareness and Training	PR.AT-1	PR.AT-1	PR.AT-1	PR.AT-1	PR.AT-1
		PR.AT-2	PR.AT-2	PR.AT-2	PR.AT-2	PR.AT-2
		PR.AT-3	PR.AT-3	PR.AT-3	PR.AT-3	PR.AT-3
		PR.AT-4	PR.AT-4	PR.AT-4	PR.AT-4	PR.AT-4
		PR.AT-5	PR.AT-5	PR.AT-5	PR.AT-5	PR.AT-5
	Data Security	PR.DS-1	PR.DS-1	PR.DS-1	PR.DS-1	PR.DS-1
		PR.DS-2	PR.DS-2	PR.DS-2	PR.DS-2	PR.DS-2
		PR.DS-3	PR.DS-3	PR.DS-3	PR.DS-3	PR.DS-3
		PR.DS-4	PR.DS-4	PR.DS-4	PR.DS-4	PR.DS-4
		PR.DS-5	PR.DS-5	PR.DS-5	PR.DS-5	PR.DS-5
		PR.DS-6	PR.DS-6	PR.DS-6	PR.DS-6	PR.DS-6
		PR.DS-7	PR.DS-7	PR.DS-7	PR.DS-7	PR.DS-7
		PR.DS-8	PR.DS-8	PR.DS-8	PR.DS-8	PR.DS-8
	Information Protection Processes and Procedures	PR.IP-1	PR.IP-1	PR.IP-1	PR.IP-1	PR.IP-1
		PR.IP-2	PR.IP-2	PR.IP-2	PR.IP-2	PR.IP-2
		PR.IP-3	PR.IP-3	PR.IP-3	PR.IP-3	PR.IP-3
		PR.IP-4	PR.IP-4	PR.IP-4	PR.IP-4	PR.IP-4
		PR.IP-5	PR.IP-5	PR.IP-5	PR.IP-5	PR.IP-5
		PR.IP-6	PR.IP-6	PR.IP-6	PR.IP-6	PR.IP-6
		PR.IP-7	PR.IP-7	PR.IP-7	PR.IP-7	PR.IP-7
		PR.IP-8	PR.IP-8	PR.IP-8	PR.IP-8	PR.IP-8
		PR.IP-9	PR.IP-9	PR.IP-9	PR.IP-9	PR.IP-9
		PR.IP-10	PR.IP-10	PR.IP-10	PR.IP-10	PR.IP-10
		PR.IP-11	PR.IP-11	PR.IP-11	PR.IP-11	PR.IP-11
		PR.IP-12	PR.IP-12	PR.IP-12	PR.IP-12	PR.IP-12
	Maintenance	PR.MA-1	PR.MA-1	PR.MA-1	PR.MA-1	PR.MA-1
		PR.MA-2	PR.MA-2	PR.MA-2	PR.MA-2	PR.MA-2
	Protective Technology	PR.PT-1	PR.PT-1	PR.PT-1	PR.PT-1	PR.PT-1
		PR.PT-2	PR.PT-2	PR.PT-2	PR.PT-2	PR.PT-2
		PR.PT-3	PR.PT-3	PR.PT-3	PR.PT-3	PR.PT-3
		PR.PT-4	PR.PT-4	PR.PT-4	PR.PT-4	PR.PT-4
		PR.PT-5	PR.PT-5	PR.PT-5	PR.PT-5	PR.PT-5

Detect *– The Detect Function enables timely discovery of cybersecurity events. Real time awareness and continuous monitoring of the systems is critical to detect cybersecurity events.*

Table 4 *DETECT Business Mission Objectives*

		Maintain Human Safety	Maintain Environmental Safety	Maintain Quality of Product	Maintain Production Goals	Maintain Trade Secrets
Category		Subcategories				
DE	Anomalies and Events	DE.AE-1	DE.AE-1	DE.AE-1	DE.AE-1	DE.AE-1
		DE.AE-2	DE.AE-2	DE.AE-2	DE.AE-2	DE.AE-2
		DE.AE-3	DE.AE-3	DE.AE-3	DE.AE-3	DE.AE-3
		DE.AE-4	DE.AE-4	DE.AE-4	DE.AE-4	DE.AE-4
		DE.AE-5	DE.AE-5	DE.AE-5	DE.AE-5	DE.AE-5
	Security Continuous Monitoring	DE.CM-1	DE.CM-1	DE.CM-1	DE.CM-1	DE.CM-1
		DE.CM-2	DE.CM-2	DE.CM-2	DE.CM-2	DE.CM-2
		DE.CM-3	DE.CM-3	DE.CM-3	DE.CM-3	DE.CM-3
		DE.CM-4	DE.CM-4	DE.CM-4	DE.CM-4	DE.CM-4
		DE.CM-5	DE.CM-5	DE.CM-5	DE.CM-5	DE.CM-5
		DE.CM-6	DE.CM-6	DE.CM-6	DE.CM-6	DE.CM-6
		DE.CM-7	DE.CM-7	DE.CM-7	DE.CM-7	DE.CM-7
		DE.CM-8	DE.CM-8	DE.CM-8	DE.CM-8	DE.CM-8
	Detection Processes	DE.DP-1	DE.DP-1	DE.DP-1	DE.DP-1	DE.DP-1
		DE.DP-2	DE.DP-2	DE.DP-2	DE.DP-2	DE.DP-2
		DE.DP-3	DE.DP-3	DE.DP-3	DE.DP-3	DE.DP-3
		DE.DP-4	DE.DP-4	DE.DP-4	DE.DP-4	DE.DP-4
		DE.DP-5	DE.DP-5	DE.DP-5	DE.DP-5	DE.DP-5

***Respond** – The Respond Function supports the ability to contain the impact of a potential cybersecurity event.*

Table 5 *RESPOND Business Mission Objectives*

		Maintain Human Safety	Maintain Environmental Safety	Maintain Quality of Product	Maintain Production Goals	Maintain Trade Secrets
Category		Subcategories				
RS	Response Planning	RS.RP-1	RS.RP-1	RS.RP-1	RS.RP-1	RS.RP-1
	Communications	RS.CO-1	RS.CO-1	RS.CO-1	RS.CO-1	RS.CO-1
		RS.CO-2	RS.CO-2	RS.CO-2	RS.CO-2	RS.CO-2
		RS.CO-3	RS.CO-3	RS.CO-3	RS.CO-3	RS.CO-3
		RS.CO-4	RS.CO-4	RS.CO-4	RS.CO-4	RS.CO-4
		RS.CO-5	RS.CO-5	RS.CO-5	RS.CO-5	RS.CO-5
	Analysis	RS.AN-1	RS.AN-1	RS.AN-1	RS.AN-1	RS.AN-1
		RS.AN-2	RS.AN-2	RS.AN-2	RS.AN-2	RS.AN-2
		RS.AN-3	RS.AN-3	RS.AN-3	RS.AN-3	RS.AN-3
		RS.AN-4	RS.AN-4	RS.AN-4	RS.AN-4	RS.AN-4
		RS.AN-5	RS.AN-5	RS.AN-5	RS.AN-5	RS.AN-5
	Mitigation	RS.MI-1	RS.MI-1	RS.MI-1	RS.MI-1	RS.MI-1
		RS.MI-2	RS.MI-2	RS.MI-2	RS.MI-2	RS.MI-2
		RS.MI-3	RS.MI-3	RS.MI-3	RS.MI-3	RS.MI-3
	Improvements	RS.IM-1	RS.IM-1	RS.IM-1	RS.IM-1	RS.IM-1
		RS.IM-2	RS.IM-2	RS.IM-2	RS.IM-2	RS.IM-2

***Recover** – The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Defined Recovery objectives are needed when recovering from disruptions.*

Table 6 *RECOVER Business Mission Objectives*

		Maintain Human Safety	Maintain Environmental Safety	Maintain Quality of Product	Maintain Production Goals	Maintain Trade Secrets
Category		Subcategories				
RC	Recovery Planning	RC.RP-1	RC.RP-1	RC.RP-1	RC.RP-1	RC.RP-1
	Improvements	RC.IM-1	RC.IM-1	RC.IM-1	RC.IM-1	RC.IM-1
		RC.IM-2	RC.IM-2	RC.IM-2	RC.IM-2	RC.IM-2
	Communications	RC.CO-1	RC.CO-1	RC.CO-1	RC.CO-1	RC.CO-1
		RC.CO-2	RC.CO-2	RC.CO-2	RC.CO-2	RC.CO-2
		RC.CO-3	RC.CO-3	RC.CO-3	RC.CO-3	RC.CO-3

6. Manufacturing System Categorization and Risk Management

In addition to the Business/Mission Objectives for aligning a focused set of cybersecurity controls to support critical business goals, the Manufacturing Profile is also structured into three impact levels based on the categorization of the information and processes within the manufacturing system.

6.1 Categorization Process

Manufacturing systems support the most critical and, sometimes, most sensitive operations and assets within an organization. The application of cybersecurity controls in these environments demands the greatest level of attention and effort to ensure that appropriate operational security and risk mitigation are achieved. The categorization process is the first step in the NIST Risk Management Framework (RMF) and provides organizations with information to support tailoring cybersecurity control implementation [3]. As defined by NIST Federal Information Processing Standard (FIPS) 199, the categorization process is based on the potential impact (e.g. LOW, MODERATE, or HIGH) if an incident or event jeopardizes the manufacturing system or components, operational assets, individuals, or the organization [8]. The Profile guidance provides LOW, MODERATE, and HIGH impact level configurations that may be utilized to identify the security capability, functionality, and specificity for supporting manufacturing systems based on the categorization of the manufacturing system.

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 general 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 general 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 general public, or the environment.

The tables below provide examples of mission-based rationale for selecting the security categorization of the manufacturing system:

Table 7 Manufacturing System Impact Levels [3]

Impact Category	Low Impact	Moderate Impact	High Impact
Injury	Cuts, bruises requiring first aid	Requires hospitalization	Loss of life or limb
Financial Loss ($)	Tens of thousands	Hundreds of thousands	Millions
Environmental Release	Temporary damage	Lasting damage	Permanent damage, off-site damage
Interruption of Production	Temporary reductions without impacting quarterly production	Temporary reductions requiring additional shifts or overtime to meet quarterly production	Significant reduction and impact to meet quarterly production
Public Image	Temporary damage	Lasting damage	Permanent damage

Table 8 Manufacturing System Impact Levels Based on Product Produced and Industry Concerns [3]

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

A limited adverse effect means that, for example, the loss of integrity, availability, or confidentiality might:

- 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 that, for example, the loss of integrity, availability, or confidentiality might:

- 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 is 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 that, for example, the loss of integrity, availability, or confidentiality might:

- 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.

6.2 Profile's Hierarchical Supporting Structure

The Profile guidance is scalable and supports intensifying security protections where needed, while maintaining a conventional baseline. Each higher impact level builds from the baseline starting with the Low designation. Unless otherwise noted, the Moderate and High each include or enhance all of the stipulations from the levels below.

- A Moderate categorization includes all Moderate and Low security implementations
- A High categorization includes all High, Moderate, and Low security implementations

Each impact level is positioned as the platform to support the next higher impact level implementation, or categorization. The impact level implementation starts with Low and increases in rigor through the Moderate and High implementations. The Low impact level represents the starting baseline for all manufacturing systems. The Moderate impact level will implement the Low security guidance as well as the Moderate. The High impact level will implement all of the Low and Moderate guidance as well as the High inputs. Section 7 provides CSF subcategory language for each impact level customized to the manufacturing domain.

6.3 Risk Management

The Profile relies on the manufacturer's risk management processes to inform and prioritize decisions regarding cybersecurity. It supports recurring risk assessments and validation of business drivers to help manufacturers select target states for cybersecurity activities that reflect desired outcomes.

To manage cybersecurity risks, a clear understanding of the business drivers and security considerations specific to the Manufacturing system and its environment is required. Each organization's risk is unique, along with its use of ICS and IT, thus the implementation of the profile will vary.

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

7. Manufacturing Profile Subcategory Guidance

Function	Category	Subcategory	Manufacturing Profile Guidance	Reference
IDENTIFY	**Asset Management (ID.AM)**	**ID.AM-1**	**Low Impact** 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, for example, 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.	ISA/IEC 62443-2-1:2009 4.2.3.4 ISA/IEC 62443-3-3:2013 SR 7.8 CM-8
			Moderate Impact Identify individuals who are both responsible and accountable for administering manufacturing system components.	CM-8 (1)(3)(5)
			High Impact Identify mechanisms for detecting the presence of unauthorized hardware and firmware components within the manufacturing system. Where safe and feasible, these mechanisms should be automated.	CM-8 (2)(4)
		ID.AM-2	**Low Impact** Document an inventory of manufacturing system software and firmware components that reflects the current system. Manufacturing system software components include for example software license information, software version numbers, Human Machine Interface (HMI) and other ICS component applications, software, operating systems. System software inventory is reviewed and updated as defined by the organization.	ISA/IEC 62443-2-1:2009 4.2.3.4 ISA/IEC 62443-3-3:2013 SR 7.8 CM-8
			Moderate Impact Identify individuals who are both responsible and accountable for administering manufacturing system software.	CM-8 (1)(3)(5)
			High Impact Identify mechanisms for detecting the presence of unauthorized software within the manufacturing system. Where safe and feasible, these mechanisms should be automated.	CM-8 (2)(4)

Function	Category	Subcategory	Manufacturing Profile Guidance	Reference
IDENTIFY	**Asset Management (ID.AM)**	**ID.AM-3**	**Low Impact**	ISA/IEC 62443-2-1:2009 4.2.3.4
			Document all connections within the manufacturing system, and between the manufacturing system and other systems. All connections are documented, authorized, and reviewed.	CA-3
			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.	
			Moderate and High Impact	AC-4
			Map the flow of information within the manufacturing system and to external systems.	
		ID.AM-4	**Low Impact**	
			Identify and document all external connections for the manufacturing system.	AC-20
			Examples of external systems include engineering design services, and those that are controlled under separate authority, personal devices, and other hosted services.	
			Moderate and High Impact	SA-9(2)
			Require external providers to identify the functions, ports, protocols, and other services required for use with the manufacturing system.	
		ID.AM-5	**Low, Moderate and High Impact**	ISA/IEC 62443-2-1:2009 4.2.3.6
			Identify and prioritize manufacturing system components and functions based on their classification, criticality, and business value.	CP-2
			Identify the types of information in possession, custody, or control for which security safeguards are needed (e.g. sensitive or protected information).	
		ID.AM-6	**Low, Moderate and High Impact**	ISA/IEC 62443-2-1:2009 4.3.2.3.3
			Establish and maintain personnel cybersecurity roles and responsibilities for the manufacturing system. Include cybersecurity roles and responsibilities for third-party providers.	CP-2
			Require third-party providers to notify the organization of any personnel transition (including transfers or terminations) involving personnel with physical or logical access to the manufacturing system components.	PS-7
			Third-party providers include, for example, service providers, contractors, and other organizations providing manufacturing system development, technology services, outsourced applications, or network and security management.	

Function	Category	Subcategory	Manufacturing Profile Guidance	Reference
IDENTIFY	**Business Environment (ID.BE)**	**ID.BE-1**	**Low and Moderate Impact**	
			Define and communicate the organization's role in the supply chain. Identify the upstream and downstream supply channels that are outside of the organization's operations. Identify the overall mission supported by the manufacturing system.	CP-2(1)(3)(8)
			High Impact	
			Protect against supply chain threats to the manufacturing system, system components, or system services by employing security safeguards as part of a comprehensive, defense-in-depth security strategy.	SA-12
		ID.BE-2	**Low, Moderate and High Impact**	
			Define and communicate the manufacturer's place in critical infrastructure and its industry sector. Define and communicate critical infrastructure and key resources relevant to the manufacturing system. Develop, document, and maintain a critical infrastructure and key resources protection plan.	PM-8
		ID.BE-3	**Low, Moderate and High Impact**	ISA/IEC 62443-2-1:2009 4.2.2.1
			Define and communicate priorities for manufacturing missions, objectives, and activities with consideration for security and the resulting risk to manufacturing operations, components, and individuals. Identify critical manufacturing system components and functions by performing a criticality analysis.	PM-11
		ID.BE-4	**Low Impact**	
			Identify and prioritize supporting services for critical manufacturing system processes and components.	PM-8
			Provide an uninterruptable power supply for identified critical manufacturing system components to facilitate the transition of the manufacturing system to long-term alternate power in the event of a primary power source loss.	PE-11
			Moderate and High Impact	
			Identify alternate and redundant supporting services for critical manufacturing system processes and components.	PE-9(1)

Function	Category	Subcategory	Manufacturing Profile Guidance	Reference
IDENTIFY	Business Environment (ID.BE)	ID.BE-5	**Low Impact**	
			Define resilience requirements for the manufacturing system to support delivery of critical services.	CP-2
			Moderate Impact	
			Define recovery time objective and recovery point objective for the resumption of essential manufacturing system processes.	CP-2(3)
			Identify critical manufacturing system assets that support essential manufacturing system processes.	CP-2(8)
			High Impact	
			Conduct capacity planning for manufacturing system processing, telecommunications, and environmental support as required during contingency operations.	CP-2(2)
			Conduct contingency planning for the continuance of essential manufacturing functions and services with little or no loss of operational continuity and sustain that continuity until full system restoration.	CP-2(4)(5)
	Governance (ID.GV)	ID.GV-1	**Low, Moderate and High Impact**	ISA/IEC 62443-2-1:2009 4.3.2.6
			Develop and disseminate a security policy that provides an overview of the security requirements for the manufacturing system. The policy includes, for example, the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance. It also reflects coordination among organizational entities responsible for the different aspects of security (i.e., technical, physical, personnel, cyber-physical, access control, media protection, vulnerability management, maintenance, monitoring), and covers the full life cycle of the manufacturing system. Review and update the security policy as determined necessary.	800-53 Security Policies-1
			Ensure the security policy is approved by a senior official with responsibility and accountability for the risk being incurred by manufacturing operations.	
		ID.GV-2	**Low, Moderate and High Impact**	ISA/IEC 62443-2-1:2009 4.3.2.3.3
			Develop and disseminate a security program for the manufacturing system that includes, for example, the identification of personnel security roles and assignment of responsibilities, management commitment, coordination among organizational entities, and compliance. This includes security requirements, roles and responsibilities for third-party providers. Review and update the security program as determined necessary.	PM-1, PS-7
		ID.GV-3	**Low, Moderate and High Impact**	ISA/IEC 62443-2-1:2009 4.4.3.7 800-53 Security Policies-1
			Ensure that legal and regulatory requirements affecting the manufacturing operations regarding cybersecurity are understood and managed.	
		ID.GV-4	**Low, Moderate and High Impact**	ISA/IEC 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9
			Develop a comprehensive strategy to manage risk to manufacturing operations. Include cybersecurity considerations in the risk management strategy. Review and update the risk management strategy as determined necessary.	PM-9, PM-11
			Determine and allocate required resources to protect the manufacturing system.	

Function	Category	Subcategory	Manufacturing Profile Guidance	Reference
IDENTIFY	**Risk Assessment (ID.RA)**	**ID.RA-1**	**Low and Moderate Impact**	ISA/IEC 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12
			Develop a plan to identify, document, and report vulnerabilities that exist on the manufacturing system. Include the use of vulnerability scanning where safe and feasible on the manufacturing system, its components, or a representative system.	CA-2
			Develop a plan for continuous monitoring of the security posture of the manufacturing system to facilitate ongoing awareness of vulnerabilities.	CA-7
			Conduct risk assessments on the manufacturing system that take into account vulnerabilities and potential impact to manufacturing operations and assets.	RA-3
			High Impact	
			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.	CA-2(2)
			Identify where manufacturing system vulnerabilities may be exposed to adversaries.	RA-5(4)
			Production systems may need to be taken off-line before testing can be conducted. If the manufacturing system is taken off-line 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.	
		ID.RA-2	**Low and Moderate Impact**	ISA/IEC 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12
			Establish and maintain ongoing contact with security groups and associations to receive security alerts and advisories. Security groups and associations include, for example, 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.	PM-15
			Collaborate and share information about potential vulnerabilities and incidents. The Department of Homeland Security (DHS) National Cybersecurity & Communications Integration Center (NCCIC) [6] serves as a centralized location where operational elements involved in cybersecurity and communications reliance are coordinated and integrated. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) [7] collaborates with international and private sector Computer Emergency Readiness Teams (CERTs) to share control systems-related security incidents and mitigation measures.	PM-16
			High Impact	SI-5(1)
			Identify where automated mechanisms can be implemented to make security alert and advisory information available to relevant organization stakeholders.	
		ID.RA-3	**Low, Moderate and High Impact**	ISA/IEC 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12
			Conduct and document periodic assessment of risk to the manufacturing system to identify threats and likelihood of impact to manufacturing operations and assets. The risk assessment includes threats from insiders and external parties.	RA-3

Function	Category	Subcategory	Manufacturing Profile Guidance	Reference
IDENTIFY	**Risk Assessment (ID.RA)**	**ID.RA-4**	**Low, Moderate and High Impact** Conduct criticality reviews of the manufacturing system that define the likelihood and potential adverse impacts to manufacturing operations, assets, and individuals if compromised or disabled.	ISA/IEC 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 RA-2
		ID.RA-5	**Low, Moderate and High Impact** Conduct risk assessments of the manufacturing system incorporating threats, vulnerabilities, likelihood, and impact to manufacturing operations, assets, and individuals. Disseminate risk assessment results to relevant stakeholders.	RA-3 PM-16
		ID.RA-6	**Low, Moderate and High Impact** Develop and implement a comprehensive strategy to manage risk to the manufacturing system that includes the identification and prioritization of risk responses.	PM-9
	Risk Management Strategy (ID.RM)	**ID.RM-1**	**Low, Moderate and High Impact** Establish a risk management process for the manufacturing system that effectively identifies, communicates, and facilitates addressing risk-related issues and information among key stakeholders internally and externally.	ISA/IEC 62443-2-1:2009 4.3.4.2 PM-9
		ID.RM-2	**Low, Moderate and High Impact** Define the risk tolerance for the manufacturing system.	ISA/IEC 62443-2-1:2009 4.3.2.6.5 PM-9
		ID.RM-3	**Low, Moderate and High Impact** Ensure the risk tolerance for the manufacturing system is informed by the organization's role in critical infrastructure and sector-specific risk analysis.	PM-9, PM-8
	Supply Chain (ID.SC)	**ID.SC-1**	**Low, Moderate and High Impact** Implement a cyber supply chain risk management process that effectively identifies, assesses, communicates, and facilitates addressing risk-related issues associated with the sharing of sensitive information or the use of information technology, operational technology, services, technology-based input products, and non-technology-based input products supporting the manufacturing system. The cyber supply chain risk management process should be approved by organizational stakeholders including those responsible for informational technology and operational technology systems.	SA-9
		ID.SC-2	**Low, Moderate and High Impact** Conduct and document cyber supply chain risk assessments at least annually or when a change to the manufacturing system, operational environment, or supply chain occurs. This assessment should identify and prioritize potential negative impacts to the organization from the sharing of sensitive information or the use of information technology, operational technology, services, technology-based input products, or non-technology-based input products supporting the manufacturing system. Disseminate results to relevant stakeholders including those responsible for informational technology and operational technology systems.	RA-3

Function	Category	Subcategory	Manufacturing Profile Guidance	Reference
IDENTIFY	Supply Chain (ID.SC)	ID.SC-3	**Low Impact**	
			Implement contractual cybersecurity requirements for suppliers and third-party partners requiring access to sensitive information or providing information technology, operational technology, services, technology-based input products, or non-technology-based input products supporting the manufacturing system. Cyber supply chain risk assessment results should be used in the development of cybersecurity requirements.	SA-9
			Moderate Impact	
			Implement contract cybersecurity requirements for suppliers and third-party partners to implement a verifiable flaw remediation process, and correct flaws identified during cybersecurity testing and evaluation.	SA-11
			High Impact	
			Implement contract requirements permitting the organization to review the cybersecurity programs implemented by suppliers and third-party partners. Implement contract requirements for suppliers and third-party partners to implement a documented development life cycle for the information technology, operational technology, services, technology-based input products, or non-technology-based input products supporting the manufacturing system.	SA-12
		ID.SC-4	**Low and Moderate Impact**	
			Review assessments of suppliers and third-party partner compliance with contractual obligations by routinely reviewing audits, test results, and other evaluations.	AU-2 AU-6
			High Impact	
			Review assessments of suppliers and third-party partner compliance with contractual obligations by routinely reviewing third-party independent audits, test results, and other evaluations.	PS-7
		ID.SC-5	**Low and Moderate Impact**	
			Identify and document key personnel from suppliers and third-party partners to include as stakeholders in response and recovery planning activities.	CP-4, IR-3, IR-4
			High Impact	
			Identify and document key personnel from suppliers and third-party partners to include as stakeholders in testing and execution of the response and recovery plans.	CP-4, IR-3, IR-4

Function	Category	Subcategory	Manufacturing Profile Guidance	Reference
PROTECT	Identity Management, Authentication and Access Control (PR.AC)	PR.AC-1	**Low Impact**	ISA/IEC 62443-2-1:2009 4.3.3.5.1; SR 1.1, 1.2, 1.3, 1.4, 1.5,1.7 IA-Family AC-2(1)
			Establish and manage identification mechanisms and credentials for users of the manufacturing system.	
			Moderate Impact	
			Establish and manage identification mechanisms and credentials for users and devices of the manufacturing system. Implement automated mechanisms where feasible to support the management and auditing of information system credentials.	AC-2(5)
			High Impact	
			Deactivate system credentials after a specified time period of inactivity, unless this would result in a compromise to safe operation of the process. Monitor the manufacturing system for atypical use of system credentials. Credentials associated with significant risk are disabled.	AC-2(12)(13)
		PR.AC-2	**Low Impact**	ISA/IEC 62443-2-1:2009 4.3.3.3.2
			Protect physical access to the manufacturing facility. Determine access requirements during emergency situations. Maintain and review visitor access records to the facility where the manufacturing system resides. Physical access controls may include, for example, lists of authorized individuals, identity credentials, escort requirements, guards, fences, turnstiles, locks, monitoring of facility access.	PE-Family
			Moderate Impact	
			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.	PE-9 (1)
			Implement redundant and physically separated power systems for critical manufacturing operations.	PE-3 (1)
			High Impact	
			Control physical access to the manufacturing system in addition to the physical access for the facility.	

Function	Category	Subcategory	Manufacturing Profile Guidance	Reference
PROTECT	Identity Management, Authentication and Access Control (PR.AC)	PR.AC-3	**Low Impact**	ISA/IEC 62443-2-1:2009 4.3.3.6.6 ISA/IEC 62443-3-3:2013 SR 1.13,2.6
			Establish usage restrictions, connection requirements, implementation guidance, and authorizations for remote access to the manufacturing system.	
			Provide an explicit indication of active remote access connections to users physically present at the devices.	AC-17, AC-19, AC-20
			Remote access methods include, for example, wireless, dial-up, broadband, Virtual Private Network (VPN) connections, mobile device connections, and communications through external networks.	SC-15
			Moderate and High Impact	
			Allow remote access only through approved and managed access points.	AC-17(1)(2)(3)(4)
			Monitor remote access to the manufacturing system and implement cryptographic mechanisms where determined necessary. Allow only authorized use of privileged functions from remote access. Establish agreements and verify security for connections with external systems.	AC-20(1)(2)
		PR.AC-4	**Low Impact**	ISA/IEC 62443-2-1:2009 4.3.3.7.3; 62443-3-3:2013 SR 2.1
			Define and manage access permissions for users of the manufacturing system. Identify and document user actions that can be performed on the manufacturing system without identification or authentication (e.g. during emergencies).	AC-Family
			Moderate Impact	

			Implement automated mechanisms where feasible to support the management of manufacturing system user accounts, including the disabling, auditing, notification, and removal of user accounts. Implement separation of duties for manufacturing system users. Limit, document, and explicitly authorize privileged user access to the manufacturing system. Audit the execution of privileged functions on the manufacturing system.	AC-2(1)(3)
				AC-5
				AC-6(1)(2)(5)(9)

			Separation of duties includes, for example: dividing operational functions and system support functions among different roles; conducting system support functions with different individuals; and ensuring security personnel administering access control functions do not also administer audit functions.	
			High Impact	
			Enforce account usage restrictions for specific time periods and locality. Monitor manufacturing system usage for atypical use. Disable accounts of users posing a significant risk.	AC-2(11)(12)(13)
			Specific restrictions can include, for example, restricting usage to certain days of the week, time of day, or specific durations of time. Privileged user access through non-local connections to the manufacturing system is restricted and managed.	

Function	Category	Subcategory	Manufacturing Profile Guidance	Reference
PROTECT	Identity Management, Authentication and Access Control (PR.AC)	PR.AC-5	**Low Impact**	ISA/IEC 62443-2-1:2009 4.3.3.4 62443-3-3:2013 SR 3.1, 3.8
			Protect network integrity of the manufacturing system, incorporating network segmentation and segregation where appropriate. Identify and control connections between system components. Monitor and control connections and communications at the external boundary and at key internal boundaries within the manufacturing system. Implement boundary protection devices.	SC-7
			Boundary protection mechanisms include, for example, routers, gateways, unidirectional gateways, data diodes, and firewalls separating system components into logically separate networks or subnetworks.	
			Moderate Impact	
			Limit external connections to the manufacturing system. Monitor and use managed interfaces to conduct external system connections. Deny by default connections to the managed interface. Disable split tunneling and covert channel options in conjunction with remote devices. Ensure the manufacturing system fails securely in the event of the operational failure of a boundary protection device.	AC-4
			High Impact	
			Implement, where feasible, authenticated proxy servers for defined communications traffic between the manufacturing system and external networks.	SC-7(8)
			Isolate manufacturing system components performing different missions.	SC-7(21)
		PR.AC-6	**Low and Moderate Impact**	
			Implement procedures for verifying identity of individuals before issuing credentials that provide access to the manufacturing systems.	IA-5
			High Impact	
			Issue unique credentials bound to each verified user, device, and process interacting with the manufacturing systems.	IA-5
			Ensure credentials are authenticated and the unique identifiers are captured when performing system interactions.	
		PR.AC-7	**Low Impact**	
			Perform a risk assessment on manufacturing user transactions to document and implement the authentication mechanisms required (e.g. single- or multi-factor) for each transaction.	IA-1, IA-2, IA-4, IA-5, IA-8
			Moderate Impact	
			Perform a risk assessment on manufacturing system transactions and the associated user, device, or other asset authentication mechanism to document and implement the authentication mechanisms required (e.g. single- or multi-factor) for each transaction.	IA-1, IA-2, IA-4, IA-5, IA-8
			High Impact	IA-2 (1) (2) (3)
			Implement multi-factor or certificate-based authentication for transactions within the manufacturing systems determined to be critical.	

Function	Category	Subcategory	Manufacturing Profile Guidance	Reference
PROTECT	Awareness and Training (PR.AT)	PR.AT-1	**Low Impact**	
			Provide security awareness training for all manufacturing system users and managers. Training could include, for example, a basic understanding of the protections and user actions needed to maintain security of the system, responding to suspected cybersecurity incidents, and awareness of operational security.	ISA/IEC 62443-2-1:2009 4.3.2.4.2 AT-2
			Moderate and High Impact	
			Incorporate insider threat recognition and reporting into security awareness training.	AT-2(2)
		PR.AT-2	**Low, Moderate and High Impact**	
			Ensure that users with privileged access to the manufacturing system understand the requirements and responsibilities of their assignments. Establish standards for measuring, building, and validating individual qualifications for privileged users.	ISA/IEC 62443-2-1:2009 4.3.2.4.2 AT-3 PM-13
		PR.AT-3	**Low Impact**	
			Establish and enforce security requirements for third-party providers and users. Ensure that third-party providers understand their responsibilities regarding the security of the manufacturing system and the responsibilities of their assignments. Require notifications be given for any personnel transfers, termination, or transition involving personnel with physical or logical access to the manufacturing system components. Ensure that providers of external system services comply with defined security requirements. Monitor and audit external service providers for security compliance.	ISA 62443-2-1:2009 4.3.2.4.2 PS-7 SA-9_
			Moderate and High Impact	
			Require external service providers to identify the functions, ports, protocols, and services necessary for the connection services.	SA-9(2)
		PR.AT-4	**Low, Moderate and High Impact**	
			Ensure that senior executives understand the requirements for the security and protection of the manufacturing system, and their responsibilities for achieving them.	ISA/IEC 62443-2-1:2009 4.3.2.4.2 AT-3
		PR.AT-5	**Low, Moderate and High Impact**	
			Ensure that personnel responsible for the physical protection and security of the manufacturing system and facility are trained and understand their responsibilities. Establish standards for measuring, building, and validating individual qualifications for physical security personnel.	ISA/IEC 62443-2-1:2009 4.3.2.4.2 AT-3 PM-13

Function	Category	Subcategory	Manufacturing Profile Guidance	Reference
PROTECT	Data Security (PR.DS)	PR.DS-1	**Low Impact**	ISA/IEC 62443-3-3:2013 SR 3.4, 4.1
			None	
			Moderate and High Impact	
			Protect manufacturing system information determined to be critical while at rest.	SC-28
		PR.DS-2	**Low Impact**	ISA/IEC 62443-3-3:SR 3.1,3.8,4.1
			None	
			Moderate and High Impact	
			Protect manufacturing system information determined to be critical when in transit.	SC-8 SC-8(1)
			Implement cryptographic mechanisms where determined necessary to prevent unauthorized access, distortion, or modification of system data and audit records.	
		PR.DS-3	**Low Impact**	ISA/IEC 62443-2-1:2009 4. 4.3.3.3.9 ISA/IEC 62443-3-3:2013 SR 4.2
			Enforce accountability for all manufacturing system components throughout the system lifecycle, including removal, transfers, and disposition.	
			Sanitize portable media prior to disposal, release, or reuse. All system components entering and exiting the facility are authorized, monitored, and controlled, and records are maintained of those items.	PE-16 MP-6
			Moderate Impact	
			Update the inventory of manufacturing system components as an integral part of component installations, removals, and system updates.	
			High Impact	

			Implement automated mechanisms where safe and feasible to maintain an up-to-date, complete, accurate, and readily available inventory of manufacturing system components.	CM-8(1)
				CM-8(2)
				MP-6(1)

			Ensure that disposal actions are approved, tracked, documented, and verified.	
		PR.DS-4	**Low Impact**	ISA/IEC 62443-3-3:2013 SR 7.1, 7.2
			Ensure that adequate resources are maintained for manufacturing system information processing, networking, telecommunications, and data storage.	CP-2
			Off-load audit records from the manufacturing system for processing to an alternate system.	
			Moderate and High Impact	
			Protect the manufacturing system against, or limit the effects of, denial of service attacks.	AU-4(1) SC-5

Function	Category	Subcategory	Manufacturing Profile Guidance	Reference
PROTECT	Data Security (PR.DS)	PR.DS-5	**Low Impact**	ISA/IEC 62443-3-3:2013 SR 5.2
			Protect the manufacturing system against data leaks.	
			Monitor the manufacturing system at the external boundary and at key internal points to detect unauthorized access and use.	SI-4 SC-7
			Develop and document access agreements for all users of the manufacturing system.	
			Moderate and High Impact	PS-6
			Regulate the information flow within the manufacturing system and to outside systems.	AC-4
			Enforce controls restricting connections to only authorized interfaces.	SC-7(3)(4), SI-4(4)
			Heighten system monitoring activity whenever there is an indication of increased risk to manufacturing operations and assets.	PE-19
			Protect the system from information leakage due to electromagnetic signals emanations.	
		PR.DS-6	**Low Impact**	ISA/IEC 62443-3-3:SR 3.1, 3.3, 3.4,
			None	
			Moderate Impact	
			Implement software, firmware, and information integrity checks to detect unauthorized changes to manufacturing system components during storage, transport, startup and when determined necessary.	SI-7(1)
			Incorporate the detection of unauthorized changes to the manufacturing system into the system's incident response capability.	
			High Impact	

			Implement automated tools where feasible to provide notification upon discovering discrepancies during integrity verification.	SI-7(7)
				SI-7(2)
				SI-7(5)

			Implement automatic response capability with pre-defined security safeguards when integrity violations are discovered.	
		PR.DS-7	**Low and Moderate Impact**	
			None	
			High Impact	
			Implement an off-line development and testing system for implementing and testing changes to the manufacturing system.	CM-2

Function	Category	Subcategory	Manufacturing Profile Guidance	Reference
PROTECT	Data Security (PR.DS)	PS.DS-8	**Low and Moderate Impact**	
			None	
			High Impact	
			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.	SI-7
			Incorporate the detection of unauthorized tampering to the manufacturing system hardware into the organization incident response capability.	
	Information Protection Processes and Procedures (PR.IP)	PR.IP-1	**Low Impact**	ISA/IEC 62443-2-1:2009 4.3.4.3.2, ISA/IEC 62443-3-3:2013 SR 7.6
			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/parameters), network topology, and the logical placement of those components within the system architecture.	CM-2 CM-6
			Configure the manufacturing system to provide only essential capabilities.	
			Review the baseline configuration and disable unnecessary capabilities.	
			Moderate Impact	
			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.	CM-7 CM-7(1)
			Implement software program usage restrictions.	
			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.	CM-2(1)(3)
			Implement a deny-all, permit-by-exception policy to allow the execution of only authorized software programs.	
			High Impact	

			Implement automated mechanisms where feasible to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the manufacturing system.	CM-7(2)
				CM-9
				SC-24
				CM-7(5)
				CM-2(2)
				CM-3(1)
				CM-5(1)(2)

			Automated system support includes for example, documentation, notification, and management of the change control process on the manufacturing system.	
			Review system changes to determine whether unauthorized changes have occurred.	

Function	Category	Subcategory	Manufacturing Profile Guidance	Reference
PROTECT	**Information Protection Processes and Procedures (PR.IP)**	**PR.IP-2**	**Low Impact**	ISA/IEC 62443-2-1:2009 4.3.4.3.3
			Manage the manufacturing system using a system development life cycle that includes security considerations.	SA-3
			Include security requirements into the acquisition process of the manufacturing system and its components.	SA-4
			Moderate and High Impact	
			Require the developer of the manufacturing system and system components to provide a description of the functional properties of security controls, and design and implementation information for security-relevant system interfaces.	SA-4(1)(2)
			Apply security engineering principles into the specification, design, development, implementation, and modification of the manufacturing system.	SA-8
			Implement configuration management and change control during the development of the manufacturing system and its components, and include flaw tracking and resolution, and security testing.	SA-10
		PR.IP-3	**Low Impact**	ISA/IEC 62443-2-1:2009 4.3.4.3.2 ISA/IEC 62443-3-3:2013 SR 7.6
			Implement configuration change control for the manufacturing system and its components.	CM-3
			Conduct security impact analyses in connection with change control reviews.	CM-4
			Moderate Impact	
			Test, validate, and document changes to the manufacturing system before implementing the changes on the operational system.	
			Review and authorize proposed configuration-controlled changes prior to implementing them on the manufacturing system.	CM-3(2)
			High Impact	
			Implement automated mechanisms where feasible to support the change control process.	CM-3(1)
			Conduct security impact analysis in a separate test environment before implementation into an operational environment for planned changes to the manufacturing system.	CM-4(1)

Function	Category	Subcategory	Manufacturing Profile Guidance	Reference
PROTECT	Information Protection Processes and Procedures (PR.IP)	PR.IP-4	**Low Impact**	ISA/IEC 62443-2-1:2009 4.3.4.3.9 ISA/IEC 62443-3-3:2013 SR 7.3, 7.4 CP-9 CP-4
			Conduct and maintain backups for manufacturing system data.	
			Manufacturing system data includes for example software, configurations and settings, documentation, system configuration data including computer configuration backups, application configuration backups, operational control limits, control bands and set points for pre-incident operation for all ICS programmable equipment	
			Moderate Impact	
			Verify the reliability and integrity of backups.	CP-9(1)
			Coordinate backup testing with organizational elements responsible for related plans.	CP-4(1)
			Establish a separate alternate storage site for system backups and ensure the same security safeguards are employed.	CP-6
			High Impact	
			Include into contingency plan testing the conducting of restorations from backup data.	CP-9(2)
			Store critical manufacturing system backup information separately.	CP-9(3)
		PR.IP-5	**Low and Moderate Impact**	ISA/IEC 62443-2-1:2009 4.3.3.3.1 PE-Family
			Define, implement, and enforce policy and regulations regarding emergency and safety systems, fire protection systems, and environment controls for the manufacturing system.	
			Fire suppression mechanisms should take the manufacturing environment into account (e.g., water sprinkler systems could be hazardous in specific environments).	
			High Impact	PE-13(1)(2)
			Implement fire detection devices that activate and notify key personnel automatically in the event of a fire.	
		PR.IP-6	**Low and Moderate Impact**	ISA/IEC 62443-2-1:4.3.3.3.1 ISA/IEC 62443-3-3:2013 SR 4.2 MP-6
			Ensure that manufacturing system data is destroyed according to policy.	
			High Impact	
			Ensure that media sanitization actions are approved, tracked, documented, and verified. Test sanitation equipment and procedures.	MP-6(1)(2)(3)
			Apply nondestructive sanitization techniques to portable storage devices connecting to the manufacturing system.	

Function	Category	Subcategory	Manufacturing Profile Guidance	Reference
PROTECT	Information Protection Processes and Procedures (PR.IP)	PR.IP-7	**Low Impact**	
			Incorporate improvements derived from the monitoring, measurements, assessments, and lessons learned into protection process revisions.	ISA/IEC 62443-2-1:2009 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4,
			Ensure that the security plan for the manufacturing system facilitates the review, testing, and continual improvement of the security protection processes.	PM-6, CA-2, CA-7, SI-4, PL-2, PM-14
			Moderate and High Impact	
			Implement independent teams to assess the protection process.	
			Independent teams, for example, may include internal or external impartial personnel.	
			Impartiality implies that assessors are free from any perceived or actual conflicts of interest regarding the development, operation, or management of the manufacturing system under assessment or to the determination of security control effectiveness.	CA-2(1), CA-7(1)
		PR.IP-8	**Low, Moderate and High Impact**	
			Collaborate and share information about manufacturing system related security incidents and mitigation measures with designated sharing partners.	AC-21
			Implement automated mechanisms where feasible to assist in information collaboration.	AC-21(1)
		PR.IP-9	**Low Impact**	ISA/IEC 62443-2-1:2009 4.3.2.5.3,
			Develop and maintain response and recovery plans that identify essential functions and associated contingency requirements, as well as providing a roadmap for implementing incident response. Plans should incorporate recovery objectives, restoration priorities, metrics, contingency roles, personnel assignments and contact information. Address maintaining essential functions despite system disruption, and the eventual restoration of the manufacturing system.	CP-2 IR-8
			Define incident types, resources and management support needed to effectively maintain and mature the incident response and contingency capabilities.	
			Moderate and High Impact	
			Coordinate contingency plan development with stakeholders responsible for related plans.	CP-2(1)

Function	Category	Subcategory	Manufacturing Profile Guidance	Reference
PROTECT	Information Protection Processes and Procedures (PR.IP)	PR.IP-10	**Low Impact** Review response and recovery plans to determine the effectiveness of the plans, and the readiness to execute the plans.	ISA/IEC 62443-2-1:2009 4.3.2.5.7 ISA/IEC 62443-3-3:2013 SR 3.3 CP-4, PM-14

			Moderate and High Impact
			Test response and recovery plans to determine the effectiveness of the plans, and the readiness to execute the plans.
			Coordinate testing of response and recovery plans with relevant stakeholders.
			Related plans include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, and Occupant Emergency Plans.
				CP-4(1)
				IR-3(2)

		PR.IP-11	**Low, Moderate and High Impact** Develop and maintain a personnel security program for the manufacturing system. Personnel security program should include policy, position risk designations, personnel screening, terminations and transfers, access agreements, third-party roles and responsibilities, and personnel sanctions.	ISA/IEC 62443-2-1:2009 4.3.3.2.1 PS- Family
		PR.IP-12	**Low Impact** Establish and maintain a process that allows continuous review of vulnerabilities and defines strategies to mitigate them.	RA-3, SI-2
			Moderate Impact Restrict access to privileged vulnerability data.	RA-5(5)
			High Impact Identify where manufacturing system vulnerabilities may be exposed to adversaries.	RA-5(4)

Function	Category	Subcategory	Manufacturing Profile Guidance	Reference
PROTECT	Maintenance (PR.MA)	PR.MA-1	**Low Impact**	ISA/IEC 62443-2-1:2009 4.3.3.3.7
			Schedule, perform, document and review records of maintenance and repairs on manufacturing system components.	MA-2
			Establish a process for maintenance personnel authorization, and escort non-authorized maintenance personnel.	MA-5
			Verify impacted security controls following maintenance or repairs.	MA-2
			Moderate Impact	
			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.	MA-3
			Perform preventative maintenance at defined intervals.	MA-6
			Inspect maintenance tools brought into the facility.	MA-3(1)
			Scan maintenance tools and portable storage devices for malicious code before they are used on the manufacturing system.	MA-3(2)
			High Impact	
			Implement automated mechanisms where feasible to schedule, conduct, and document maintenance and repairs; and to produce records of maintenance activity.	MA-2(2)
			Prevent the unauthorized removal of maintenance equipment containing manufacturing system information.	MA-3(3)
		PR.MA-2	**Low and Moderate Impact**	ISA/IEC 62443-2-1:2009 4.3.3.6.5
			Enforce approval requirements, control, and monitoring, of remote maintenance activities.	MA-4
			Implement strong authenticators, record keeping, and session termination for remote maintenance.	
			High Impact	
			Require that diagnostic services pertaining to remote maintenance be performed from a system that implements a security capability comparable to the capability implemented on the manufacturing system.	MA-4(3)

Function	Category	Subcategory	Manufacturing Profile Guidance	Reference
PROTECT	Protective Technology (PR.PT)	PR.PT-1	**Low Impact**	ISA/IEC 62443-2-1:2009 4.3.3.3.9, ISA/IEC 62443-3-3:2013 SR 2.8, AU-3
			Generate audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or manufacturing components associated with the event.	
			Generate time stamps from an internal system clock that is mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).	AU-5
			Moderate Impact	
			Ensure that audit processing failures on the manufacturing system generate alerts and trigger defined responses.	AU-8
			Review and update audit events.	AU-5
			Implement automated mechanisms to integrate audit review, analysis, and reporting.	AU-2(3)
			Compare and synchronize the internal system clocks to an authoritative time source. Authoritative time sources include for example, an internal Network Time Protocol (NTP) server, radio clock, atomic clock, GPS time source.	

			High Impact	AU-6(1)
				AU-7(1)

			Integrate analysis of audit records with physical access monitoring.	AU-6(6)

			Conduct time correlation of audit records.	AU-12(1)
				AU-12(3)

			Enable authorized individuals to extend audit capabilities when required by events.	
		PR.PT-2	**Low Impact**	ISA/IEC 62443-3-3:2013 SR 2.3 MP-2
			Implement safeguards to restrict the use of portable storage devices.	
			Moderate and High Impact	
			Protect and control portable storage devices containing manufacturing system data while in transit and in storage. Scan all portable storage devices for malicious code before they are used on the manufacturing system	MP-4 MP-7
		PR.PT-3	**Low Impact**	ISA/IEC 62443-2-1:2009 4.3.3.5.1, ISA/IEC 62443-3-3:2013 SR 1.1, SR AC-3
			Configure the manufacturing system to provide only essential capabilities.	
			Moderate and High Impact	
			Disable defined functions, ports, protocols, and services within the manufacturing system deemed to be unnecessary.	CM-7(1)
			Implement technical safeguards to enforce a deny-all, permit-by-exception policy to only allow the execution of authorized software programs.	CM-7(5)

Function	Category	Subcategory	Manufacturing Profile Guidance	Reference
PROTECT	Protective Technology (PR.PT)	PR.PT-4	**Low Impact**	ISA/IEC 62443-3-3:2013 SR 3.1, SR SC-7
			Monitor and control communications at the external boundary and at key internal boundaries within the manufacturing system.	
			Moderate and High Impact	
			Control the flow of information within the manufacturing system and between interconnected systems.	
			Information flow may be supported, for example, by labeling or coloring physical connectors as an aid to manual hookup. Inspection of message content may enforce information flow policy. For example, a message containing a command to an actuator may not be permitted to flow between the control network and any other network. Physical addresses (e.g., a serial port) may be implicitly or explicitly associated with labels or attributes (e.g., hardware I/O address). Manual methods are typically static. Label or attribute policy mechanisms may be implemented in hardware, firmware, and software that controls or has device access, such as device drivers and communications controllers.	AC-4 SC-7(3)
			Limit external connections to the system.	
			Manage the interface for external telecommunication services by establishing a traffic flow policy, protecting the confidentiality and integrity of the information being transmitted, reviewing and documenting each exception to the traffic flow policy.	SC-7(4)
		PR.PT-5	**Low Impact**	
			None	
			Moderate Impact	
			Implement IT resiliency mechanisms to support normal and adverse manufacturing situations.	PL-8
			High Impact	
			Implement OT resiliency mechanisms to support normal and adverse manufacturing situations.	PL-8
DETECT	Anomalies and Events (DE.AE)	DE.AE-1	**Low, Moderate and High Impact**	ISA/IEC 62443-2-1:2009 4.4.3.3 CM-2
			Ensure that a baseline of network operations and expected data flows for the manufacturing system is developed, documented, and maintained to detect events.	
		DE.AE-2	**Low Impact**	ISA/IEC 62443-2-1:2009 4.3.4.5.6, ISA/IEC 62443-3-3:2013 SR 2.8, 2.9 AU-6, IR-4
			Review and analyze detected events within the manufacturing system to understand attack targets and methods.	
			Moderate and High Impact	

			Implement automated mechanisms where feasible to review and analyze detected events within the manufacturing system.	AU-6(1)
				IR-4(1)

Function	Category	Subcategory	Manufacturing Profile Guidance	Reference
DETECT	**Anomalies and Events (DE.AE)**	**DE.AE-3**	**Low and Moderate Impact** Ensure that event data is compiled and correlated across the manufacturing system using various sources such as event reports, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.	ISA/IEC 62443-3-3:2013 SR 6.1 IR-5

			High Impact
			Integrate analysis of events where feasible with the analysis of vulnerability scanning information; performance data; manufacturing system monitoring, and facility monitoring to further enhance the ability to identify inappropriate or unusual activity.
				AU-6(5)(6)
				AU-12(1)

		DE.AE-4	**Low Impact** Determine negative impacts to manufacturing operations, assets, and individuals resulting from detected events, and correlate with risk assessment outcomes.	RA-3
			Moderate Impact Implement automated mechanisms to support impact analysis.	IR-4(1), SI-4(2)
			High Impact Correlate detected event information and responses to achieve perspective on event impact across the organization.	IR-4(4)
		DE.AE-5	**Low Impact** Define incident alert thresholds for the manufacturing system.	ISA/IEC 62443-2-1:2009 4.2.3.10 IR-4, IR-5, AU-2, AU-3, IR-8
			Moderate and High Impact Implement automated mechanisms where feasible to assist in the identification of security alert thresholds.	IR-4(1), IR-5(1)

Function	Category	Subcategory	Manufacturing Profile Guidance	Reference
DETECT	**Security Continuous Monitoring (DE.CM)**	**DE.CM-1**	**Low Impact**	ISA/IEC 62443-3-3:2013 SR 6.2
			Conduct ongoing security status monitoring of the manufacturing system network to detect defined cybersecurity events and indicators of potential cybersecurity events.	CA-7
			Detect unauthorized local, network, and remote connections, and identify unauthorized use of the manufacturing system.	AC-2 SI-4
			Generate audit records for defined cybersecurity events.	AU-12
			Monitor network communications at the external boundary of the system and at key internal boundaries within the system.	SC-7, SI-4(4)
			Heighten system monitoring activity whenever there is an indication of increased risk.	SI-4
			Moderate Impact	
			Implement automated mechanisms to support detection of cybersecurity events.	AC-2 (1)(2)(3)(4), SI-4(2)
			Generate system alerts when indications of compromise or potential compromise occur.	SI-4(5)
			High Impact	
			Monitor for and report atypical usage of the manufacturing system.	AC-2(12)
		DE.CM-2	**Low Impact**	ISA/IEC 62443-2-1:2009 4.3.3.3.8
			Conduct ongoing security status monitoring of the manufacturing system facility to detect physical security incidents.	CA-7, PE-6, PE-3
			Moderate and High Impact	
			Implement independent teams to monitor the security of the physical environment.	CA-7(1)
			Monitor physical intrusion alarms and surveillance equipment.	PE-6(1), PE-6(4)
			Monitor physical access to the manufacturing system and devices in addition to the facility.	PE-3(1)
		DE.CM-3	**Low, Moderate and High Impact**	ISA/IEC 62443-3-3:2013 SR 6.2
			Conduct security status monitoring of personnel activity associated with the manufacturing system.	CA-7
			Enforce software usage and installation restrictions.	CM-10, CM-11

Function	Category	Subcategory	Manufacturing Profile Guidance	Reference
DETECT	**Security Continuous Monitoring (DE.CM)**	**DE.CM-4**	**Low Impact**	
			Deploy malicious code protection mechanisms throughout the manufacturing system where safe and feasible to detect and eradicate malicious code.	ISA/IEC 62443-2-1:2009 4.3.4.3.8 ISA/IEC 62443-3-3:2013 SR 3.2
			Update malicious code protection mechanisms whenever new releases are available in accordance with the configuration management policy and procedures for the manufacturing system.	SI-3
			Moderate and High Impact	
			Manage for false positives during malicious code detection and eradication.	SI-3d SI-3(2)
			Automatically update malicious code protection mechanisms where safe and feasible.	
		DE.CM-5	**Low Impact**	ISA/IEC 62443-3-3:2013 SR 2.4
			None	
			Moderate and High Impact	
			Define acceptable and detect unacceptable mobile code and mobile code technologies.	SC-18
			Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript.	
			Enforce usage restrictions and establish implementation guidance for acceptable mobile code and mobile code technologies for use with the manufacturing system.	
			The use of mobile code technologies is determined after careful consideration and after verification that it does not adversely impact the operational performance of the manufacturing system.	
		DE.CM-6	**Low Moderate and High Impact**	
			Conduct ongoing security status monitoring of external service provider activity on the manufacturing system.	CA-7
			Detect defined cybersecurity events and indicators of potential cybersecurity events from external service providers.	SI-4
			Monitor compliance of external providers with personnel security policies and procedures, and contract security requirements.	PS-7, SA-4, SA-9, MA-5
		DE.CM-7	**Low Impact**	
			Conduct ongoing security status monitoring on the manufacturing system for unauthorized personnel, connections, devices, access points, and software.	CA-7
			Monitor for system inventory discrepancies.	CM-8
			Moderate and High Impact	
			Deploy monitoring devices strategically within the manufacturing system to collect essential information to detect specific events of interest.	SI-4
			Monitor for unauthorized configuration changes to the manufacturing system.	CM-3

Function	Category	Subcategory	Manufacturing Profile Guidance	Reference
DETECT	**Security Continuous Monitoring (DE.CM)**	**DE.CM-8**	**Low, Moderate and High Impact** Conduct vulnerability scans on the manufacturing system where safe and feasible. Include analysis, remediation, and information sharing in the vulnerability scanning process. Implement control system-specific vulnerability scanning tools and techniques where safe and feasible. Active vulnerability scanning, which introduces network traffic, is used with care on manufacturing systems to ensure that system functions are not adversely impacted by the scanning process.	ISA/IEC 62443-2-1:2009 4.2.3.1 RA-5
	Detection Processes (DE.DP)	**DE.DP-1**	**Low, Moderate and High Impact** Define roles and responsibilities for detection activities on the manufacturing system and ensure accountability.	ISA/IEC 62443-2-1:2009 4.4.3.1 CA-2, CA-7, PM-14
		DE.DP-2	**Low, Moderate and High Impact** Conduct detection activities in accordance with applicable federal and state laws, industry regulations and standards, policies, and other applicable requirements.	ISA/IEC 62443-2-1:2009 4.4.3.2 CA-2
		DE.DP-3	**Low, Moderate and High Impact** Validate that event detection processes are operating as intended.	ISA/IEC 62443-2-1:2009 4.4.3.2 ISA/IEC 62443-3-3:2013 SR 3.3 PM-14
		DE.DP-4	**Low Impact** Communicate event detection information to defined personnel. Event detection information includes for example, alerts on atypical account usage, unauthorized remote access, wireless connectivity, mobile device connection, altered configuration settings, contrasting system component inventory, use of maintenance tools and nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of mobile code, use of Voice over Internet Protocol (VoIP), and malware disclosure. **Moderate and High Impact** Implement automated mechanisms and system generated alerts to support event detection communication.	ISA/IEC 62443-2-1:2009 4.3.4.5.9 ISA/IEC 62443-3-3:2013 SR 6.1 AU-6 SI-4 AU-6(1) SI-4(5)

Function	Category	Subcategory	Manufacturing Profile Guidance	Reference
DETECT	**Detection Processes (DE.DP)**	**DE.DP-5**	**Low Impact**	ISA/IEC 62443-2-1:2009 4.4.3.4
			Incorporate improvements derived from the monitoring, measurements, assessments, and lessons learned into detection process revisions.	CA-2, CA-7, SI-4
			Ensure the security plan for the manufacturing system provides for the review, testing, and continual improvement of the security detection processes.	
			Moderate Impact	
			Implement independent teams to assess the detection process.	PL-2, PM-14
			High Impact	CA-2(1), CA-7(1)
			Conduct specialized assessments including in-depth monitoring, vulnerability scanning, malicious user testing, insider threat assessment, performance/load testing, and verification and validation testing on the manufacturing system.	CA-2(7)
RESPOND	**Response Planning (RS.RP)**	**RS.RP-1**	**Low, Moderate and High Impact**	ISA/IEC 62443-2-1:2009 4.3.4.5.1
			Execute the response plan during or after a cybersecurity event on the manufacturing system.	IR-8, IR-4
	Communications (RS.CO)	**RS.CO-1**	**Low, Moderate and High Impact**	ISA/IEC 62443-2-1:2009 4.3.4.5.2
			Ensure personnel understand objectives, restoration priorities, task sequences and assignment responsibilities for event response.	CP-2, CP-3, IR-8
		RS.CO-2	**Low Impact**	ISA/IEC 62443-2-1:2009 4.3.4.5.5
			Implement prompt reporting to appropriate stakeholders for cybersecurity events on the manufacturing system.	IR-6
			Ensure that cybersecurity events on the manufacturing system are reported consistent with the response plan.	AU-6
			Moderate and High Impact	
			Implement automated mechanisms to assist in the reporting of cybersecurity events.	IR-6(1)
		RS.CO-3	**Low, Moderate and High Impact**	ISA/IEC 62443-2-1:2009 4.3.4.5.2
			Share cybersecurity incident information with relevant stakeholders per the response plan.	CA-2, CA-7, CP-2f
		RS.CO-4	**Low Impact**	ISA/IEC 62443-2-1:2009 4.3.4.5.5
			Coordinate cybersecurity incident response actions with all relevant stakeholders.	CP-2, CP-2(1), IR-4
			Stakeholders for incident response include for example, mission/business owners, manufacturing system owners, integrators, vendors, human resources offices, physical and personnel security offices, legal departments, operations personnel, and procurement offices.	
			Moderate and High Impact	IR-4(1)
			Implement automated mechanisms to support stakeholder coordination.	

Function	Category	Subcategory	Manufacturing Profile Guidance	Reference
RESPOND	Communications (RS.CO)	RS.CO-5	**Low, Moderate and High Impact**	PM-15, SI-5
			Share cybersecurity event information voluntarily, as appropriate, with industry security groups to achieve broader cybersecurity situational awareness. For example, the DHS National Cybersecurity & Communications Integration Center (NCCIC) [6] serves as a centralized location where operational elements involved in cybersecurity and communications reliance are coordinated and integrated. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) [7] collaborates with international and private sector Computer Emergency Readiness Teams (CERTs) to share control systems-related cybersecurity incidents and mitigation measures.	
	Analysis (RS.AN)	RS.AN-1	**Low Impact**	ISA/IEC 62443-2-1:2009 4.3.4.5.6 ISA/IEC 62443-3-3:2013 SR 6.1 IR-4, CA-7, AU-6 IR-5(1), SI-4(2)
			Investigate cybersecurity-related notifications generated from detection systems.	
			Moderate and High Impact	
			Implement automated mechanisms to assist in the investigation and analysis of cybersecurity-related notifications.	
		RS.AN-2	**Low Impact**	ISA/IEC 62443-2-1:2009 4.3.4.5.6 IR-4(4)
			Understand the full implication of the cybersecurity incident based on thorough investigation and analysis results. Correlate detected event information and incident responses with risk assessment outcomes to achieve perspective on incident impact across the organization.	
			Moderate and High Impact	
			Implement automated mechanisms to support incident impact analysis.	IR-4(1), SI-4(2)
		RS.AN-3	**Low Impact**	ISA/IEC 62443-3-3:SR 2.8, 2.9, 2.10 IR-4
			Conduct forensic analysis on collected cybersecurity event information to determine root cause.	
			Moderate and High Impact	
			Provide on-demand audit review, analysis, and reporting for after-the-fact investigations of cybersecurity incidents.	AU-7(1)
		RS.AN-4	**Low, Moderate and High Impact**	62443-2-1:2009 4.3.4.5.6 RA-3, PM-9, IR-4
			Categorize cybersecurity incidents according to level of severity and impact consistent with the response plan.	

Function	Category	Subcategory	Manufacturing Profile Guidance	Reference
RESPOND	Analysis (RS.AN)	RS.AN-5	**Low and Moderate Impact** Implement vulnerability management processes and procedures to incorporate processing, analyzing, and remediating vulnerabilities identified from internal and external sources	SI-5, PM-15
			High Impact Implement automated mechanisms to disseminate and track remediation efforts for vulnerability information captured from internal and external sources to key stakeholders	SI-5(1)
	Mitigation (RS.MI)	RS.MI-1	**Low, Moderate and High Impact** Contain cybersecurity incidents to minimize impact on the manufacturing system.	ISA/IEC 62443-2-1:2009 4.3.4.5.6 62443-3-3:2013 SR 5.1, SR IR-4, IR-4(1)
		RS.MI-2	**Low Impact** Mitigate cybersecurity incidents occurring on the manufacturing system.	ISA/IEC 62443-2-1:2009 4.3.4.5.6, IR-4
			Moderate and High Impact Implement automated mechanisms to support the cybersecurity incident mitigation process.	IR-4(1)
		RS.MI-3	**Low, Moderate and High Impact** Ensure that vulnerabilities identified while responding to a cybersecurity incident are mitigated or documented as accepted risks.	RA-5, RA-3
	Improvements (RS.IM)	RS.IM-1	**Low, Moderate and High Impact** Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly.	ISA/IEC 62443-2-1:2009 4.3.4.5.10 IR-4
		RS.IM-2	**Low, Moderate and High Impact** Update the response plans to address changes to the organization, manufacturing system, attack vectors, or environment of operation and problems encountered during plan implementation, execution, or testing. Updates may include, for example, responses to disruptions or failures, and predetermined procedures. Enable a process for the response plan to evolve to reflect new threats, improved technology, and lessons learned.	CP-2

Function	Category	Subcategory	Manufacturing Profile Guidance	Reference

RECOVER	Recovery Planning (RC.RP)	RC.RP-1	**Low and Moderate Impact**
			Execute the recovery plan during or after a cybersecurity incident on the manufacturing system.
			Restore the manufacturing system within a predefined time-period from configuration-controlled and integrity-protected information representing a known, operational state for the components.
			High Impact
			Continue essential manufacturing functions and services with little or no loss of operational continuity and sustain continuity until full system restoration.
				IR-8, CP-10
				CP-10(4)
				CP-2(5)

	Improvements (RC.IM)	RC.IM-1	**Low, Moderate and High Impact** Incorporate lessons learned from ongoing recovery activities into system recovery procedures, training, and testing, and implement the resulting changes accordingly.	ISA/IEC 62443-2-1 4.4.3.4 IR-4
		RC.IM-2	**Low, Moderate and High Impact** Update the recovery plan to address changes to the organization, manufacturing system, or environment of operation and problems encountered during plan implementation, execution, or testing. Ensure that updates are integrated into the recovery plans.	CP-2, IR-8
	Communications (RC.CO)	RC.CO-1	**Low Impact** Centralize and coordinate information distribution, and manage the public facing representation of the organization. Public relations management may include, for example, managing media interactions, coordinating and logging all requests for interviews, handling and 'triaging' phone calls and e-mail requests, matching media requests with appropriate and available internal experts who are ready to be interviewed, screening all of information provided to the media, ensuring personnel are familiar with public relations and privacy policies. **Moderate Impact** Assign a Public Relations Officer. **High Impact** Pre-define media contacts. Implement external assets to manage public relations.	COBIT 5 EDM03.02
		RC.CO-2	**Low, Moderate and High Impact** Implement a crisis response strategy to protect against negative impact and repair organizational reputation. Crisis response strategies include, for example, actions to shape attributions of the crisis, change perceptions of the organization in crisis, and reduce the negative effect generated by the crisis.	COBIT 5 EDM03.02
		RC.CO-3	**Low, Moderate and High Impact** Communicate recovery activities to all relevant stakeholders, and executive and management teams.	CP-2 IR-4

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] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018

[3] Stouffer KA, Lightman S, Pillitteri VY, Abrams M, Hahn A (2015) Guide to Industrial Control Systems (ICS) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-82, Rev. 2. https://doi.org/10.6028/NIST.SP.800-82r2

[4] Joint Task Force Transformation Initiative (2013) 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. 4, Includes updates as of January 22, 2015. https://doi.org/10.6028/NIST.SP.800-53r4

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

[6] Cybersecurity and Infrastructure Security Agency (2020) *National Cybersecurity and Communications Integration Center (NCCIC)*. Available at https://www.cisa.gov/national-cybersecurity-communications-integration-center

[7] Cybersecurity and Infrastructure Security Agency (2020) *Industrial Control Systems*. Available at https://www.us-cert.gov/ics [Formerly the site for the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).]

[8] National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 199. https://doi.org/10.6028/NIST.FIPS.199

Appendix A - Acronyms and Abbreviations

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

CAN	Controller Area Network
CSF	Cybersecurity Framework
DCS	Distributed Control System
FIPS	Federal Information Processing Standards
HMI	Human Machine Interface
ICS	Industrial Control System
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IEC	International Electrotechnical Commission
ISA	The International Society of Automation
IT	Information Technology
LAN	Local Area Network
NCCIC	National Cybersecurity & Communications Integration Center
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OT	Operational Technology
PLC	Programmable Logic Controller
RF	Radio Frequency
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
US-CERT	United States Computer Emergency Readiness Team
VPN	Virtual Private Network

Appendix B - Glossary

Selected terms used in the Manufacturing Profile are defined below.

Actuator - A device for moving or controlling a mechanism or system. It is operated by a source of energy, typically electric current, hydraulic fluid pressure, or pneumatic pressure, and converts that energy into motion. An actuator is the mechanism by which a control system acts upon an environment. The control system can be simple (a fixed mechanical or electronic system), software-based (e.g. a printer driver, robot control system), or a human or other agent. [800-82]

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 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.

Network Access - any access across a network connection 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.