



MANUFACTURING
PROFILE

NIST Cybersecurity Framework

A Manufacturing-Sector tailored approach to protecting against cyber risk
April 2016

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

CSF Profile for Manufacturing

Executive Summary	2
1. Introduction	3
1.1 Purpose & Scope	3
1.2 Audience.....	4
1.3 Document Structure	4
2. Overview of Manufacturing Systems	5
3. Overview of the Cybersecurity Framework	6
3.1 Framework Core	6
4. Manufacturing Profile Development Approach	8
4.1 The Framework Profile.....	8
5. Manufacturing Business/Mission Objectives	9
5.1 Alignment of Subcategories to Meet Mission Objectives	9
6. Risk Management.....	14
6.1 Risk Management and the Cybersecurity Framework	14
6.2 Manufacturing System Categorization	14
6.3 Profile Categorization Supporting Structure	16
7. Manufacturing Profile Subcategory Guidance	17
Appendix A - Acronyms and Abbreviations	44
Appendix B - Glossary.....	45
Appendix C - References.....	46

Executive Summary

This document presents the Cybersecurity Framework implementation details developed for the manufacturing environment. The “Manufacturing Profile” of the NIST Cybersecurity Framework addresses the next level of detail in undertakings necessary to meet the recommended Cyber Security Framework core security controls.

The Profile gives manufacturers:

- A simple method to indicate the types of controls they have in place to protect their manufacturing system resources and the operational data
- 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 NIST Cybersecurity Framework which enumerate the most basic functions of cybersecurity activities. The five primary functional areas are: Identify, Protect, Detect, Respond, and Recover. There are 98 distinct security objectives within the primary functional areas. These 98 objectives 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.

The Manufacturing Profile provides a prioritization of the Functions, Categories, and Subcategories of the NIST Cybersecurity Framework, identifying a subset of relevant and actionable security practices that can be implemented to support key business/mission goals.

1. Introduction

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

The Cybersecurity Framework is a voluntary risk-based, assemblage of industry standards and best practices designed to help organizations manage cybersecurity risks. 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 placing additional regulatory requirements on businesses.

The 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 sector-specific approach to cybersecurity from standards, guidelines, and practices that are working effectively in industry.

1.1 Purpose & Scope

This document represents a ‘Target Profile’ that focuses on the desired cybersecurity outcomes and provides a roadmap to the ‘to-be’ state of cybersecurity posture of the manufacturing system. It can be used to identify opportunities for improving cybersecurity posture by comparing the “as is” state (Current) with the “to be” state (Target). The Target Profile can also be used for comparison with the ‘as-is’ state to influence process improvement priorities for the organization. The organization’s ‘Current Profile’ represents the outcomes from the Framework Core that are currently being achieved.

Comparison of Profiles (e.g., the Current Profile and Target Profile) may reveal gaps to be addressed to meet cybersecurity risk management objectives. An action plan to address these gaps can contribute to the roadmap. 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 defined in this document 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 its 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 Categories and Subcategories.

- A critical infrastructure sector may establish a Target Profile that can be used among its constituents as sector-specific starting point from which to build their tailored Target Profiles.

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 apply a manufacturing systems cybersecurity program to help mitigate impacts to business functionality.
- Researchers 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 mission objectives.
- Section 6 discusses cyber Risk Management and the risk categorization of the manufacturing system.
- Section 7 presents the manufacturing profile security practice implementations.

The guide also contains several appendices with supporting material, as follows:

- Appendix A— provides a list of acronyms and abbreviations used in this document.
- Appendix B— provides a glossary of terms used in this document.
- Appendix C— provides a list of references used in the development of this document.

2. Overview of Manufacturing Systems

Manufacturing presents a large and diverse industrial sector with many different processes, which can be categorized into *process-based* and *discrete-based* manufacturing.

The *process-based* manufacturing industries typically utilize two main processes:

- **Continuous Manufacturing Processes.** These processes run continuously, often with transitions 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 step to a batch process with the possibility of brief steady state operations during intermediate steps. Typical batch manufacturing processes include food manufacturing.

The *discrete-based* manufacturing industries typically conduct a series of steps on a single device to create the 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 the same types of control systems, sensors, and networks. Some facilities are a hybrid of discrete and process-based manufacturing.

Manufacturing industries are usually located within a confined factory or plant-centric area. Communications in manufacturing industries are usually performed using local area network (LAN) technologies that are typically reliable and high speed. Wireless/RF (radio frequency) technologies are gaining in use by manufacturing industries.

The Manufacturing sector of the critical infrastructure community includes public and private owners and operators, and other entities with a role in the manufacturing domain. Members of the distinct critical infrastructure sector perform functions that are supported by industrial control systems (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 operations.

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 tools and methods used to achieve the outcomes described by the Profile will vary.

The Manufacturing Profile is meant to enhance but not replace current cybersecurity standards and industry guidelines that the manufacturer is 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.

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. 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 lifecycle of an 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.

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
PR	Protect	PR.AC	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
RC	Recover	RC.IM	Improvements
		RC.RP	Recovery Planning
		RC.CO	Communications

The five “functions” of the Framework Core are:

- A. Identify – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- B. Protect – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- C. Detect – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- D. Respond – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- E. 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.

DRAFT

4. Manufacturing Profile Development Approach

This manufacturing profile was developed using an approach emphasizing the Framework Core informative references to the NIST SP 800-53 (Rev. 4) security controls. Specifically, for each security control referenced, the approach took into account the information pertaining to that control in NIST SP 800-53 Appendix F (Security Control Catalog). The approach also considered any additional guidance from NIST SP 800-82 (Rev. 2) pertaining to the control: both in section 6.2 (Guidance on the Application of Security Controls to ICS) and in Appendix G (ICS Overlay). 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.

4.1 The Framework Profile

The Manufacturing Profile for the Cybersecurity Framework ("Profile") represents 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. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a practical implementation scenario.

This Profile represents 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.

The Profile expresses domain-specific values for cybersecurity controls, tailored to the manufacturing system environment. The developers of the Profile drew from the referenced standards of the Core Framework to address key cybersecurity needs, relying primarily on the security control language from the NIST 800-53 (Rev. 4) and the 800-82(Rev. 2). ISA 62443 is also a very good informative reference to develop cybersecurity controls tailored to the manufacturing system environment but is not freely available to the public. Utilization of the Profile is intended to provide a roadmap of cybersecurity practices that are aligned with organizational and infrastructure sector goals, coverage of legal and regulatory requirements, incorporation of industry best practices, and administer management's security priorities and risk tolerance decisions.

5. Manufacturing Business/Mission Objectives

The development of the Manufacturing Profile included the identification of critical subcategories to address common business/mission objectives to the manufacturing sector. These business/mission objectives provide the necessary context for identifying and managing cybersecurity risk. Four common business/mission objectives for the manufacturing sector were initially identified: *Maintain Personnel Safety*, *Maintain Environmental Safety*, *Maintain Quality of Product*, and *Maintain Production Goals*. Other business/mission objectives were identified but not included in this initial profile. Key cybersecurity practices from the subcategories of the Profile are identified for the goal of supporting each objective, allowing users to better prioritize actions and resources according to each user's defined needs.

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

Maintain Personnel Safety

Reduce cybersecurity risks that could potentially impact personnel safety. Cybersecurity implementations on the manufacturing system could potentially adversely affect personnel safety. Understand and train personnel on cybersecurity and personnel safety interdependencies.

Maintain Environmental Safety

Reduce cybersecurity risks that could adversely affect the environment, including both accidental and deliberate damage. Cybersecurity implementations on the manufacturing system could potentially adversely affect environmental safety. Understand and train personnel on cybersecurity and environmental safety interdependencies.

Maintain Quality of Product

Reduce cybersecurity risks that could adversely affect the quality of product. Protect against compromise of integrity and confidentiality of product data.

Maintain Production Goals

Reduce cybersecurity risks that could adversely affect production goals. Cybersecurity implementations on the manufacturing system could potentially adversely affect production goals. Understand and train personnel on cybersecurity and production goal interdependencies.

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 that are common to the manufacturing sector. This allows the manufacturer to focus on implementing those cybersecurity protections against threats that could severely compromise their ability to perform their essential mission.

For each business mission objective, the most critical subcategories to support the objective are highlighted in the tables under each Function.

***Identify** - This Function guides the manufacturer in the development of the foundation for cybersecurity management, and in the understanding of cyber risk to systems, assets, data, and capabilities.*

The activities in Asset Management, Business Environment, Risk Assessments and Risk Management Strategies are the primary security areas that address protections for the four mission objectives.

		Maintain Personnel Safety	Maintain Environmental Safety	Maintain Quality of Product	Maintain Production Goals
Category		Subcategories			
Identify	Asset Management	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-3	ID.AM-3	ID.AM-3	ID.AM-3
		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-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-2	ID.BE-2	ID.BE-2	ID.BE-2
		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-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-2	ID.GV-2	ID.GV-2	ID.GV-2
		ID.GV-3	ID.GV-3	ID.GV-3	ID.GV-3
		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-2	ID.RA-2	ID.RA-2	ID.RA-2
		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-5	ID.RA-5	ID.RA-5	ID.RA-5
		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-2	ID.RM-2	ID.RM-2	ID.RM-2
		ID.RM-3	ID.RM-3	ID.RM-3	ID.RM-3

Protect – The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Access Control, Awareness and Training, Information Protection Processes, Maintenance, and Protective Technology are the priority security focus areas. Access Control identifies and regulates personnel ingress and egress. Awareness and Training and the Protection Processes prepare the workforce to achieve cyber security. Protective technology implements security decisions.

		Maintain Personnel Safety	Maintain Environmental Safety	Maintain Quality of Product	Maintain Production Goals
Category		Subcategories			
Protect	Access Control	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-3	PR.AC-3	PR.AC-3	PR.AC-3
		PR.AC-4	PR.AC-4	PR.AC-4	PR.AC-4
		PR.AC-5	PR.AC-5	PR.AC-5	PR.AC-5
	Awareness and Training	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-3	PR.AT-3	PR.AT-3	PR.AT-3
		PR.AT-4	PR.AT-4	PR.AT-4	PR.AT-4
		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-2	PR.DS-2	PR.DS-2	PR.DS-2
		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-5	PR.DS-5	PR.DS-5	PR.DS-5
		PR.DS-6	PR.DS-6	PR.DS-6	PR.DS-6
		PR.DS-7	PR.DS-7	PR.DS-7	PR.DS-7
	Information Protection Processes and Procedures	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-3	PR.IP-3	PR.IP-3	PR.IP-3
		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-6	PR.IP-6	PR.IP-6	PR.IP-6
		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-9	PR.IP-9	PR.IP-9	PR.IP-9
		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-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-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-2	PR.PT-2	PR.PT-2	PR.PT-2
		PR.PT-3	PR.PT-3	PR.PT-3	PR.PT-3
		PR.PT-4	PR.PT-4	PR.PT-4	PR.PT-4

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.

		Maintain Personnel Safety	Maintain Environmental Safety	Maintain Quality of Product	Maintain Production Goals
Category		Subcategories			
Detect	Anomalies and Events	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-3	DE.AE-3	DE.AE-3	DE.AE-3
		DE.AE-4	DE.AE-4	DE.AE-4	DE.AE-4
		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-2	DE.CM-2	DE.CM-2	DE.CM-2
		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-5	DE.CM-5	DE.CM-5	DE.CM-5
		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-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-2	DE.DP-2	DE.DP-2	DE.DP-2
		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-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. Rapid and effective response and communication to cyber incidents is critical in protecting personnel and environmental safety. Situational awareness to the event unfolding is needed to properly address it.

		Maintain Personnel Safety	Maintain Environmental Safety	Maintain Quality of Product	Maintain Production Goals
Category		Subcategories			
Respond	Response Planning	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-2	RS.CO-2	RS.CO-2	RS.CO-2
		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-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-2	RS.AN-2	RS.AN-2	RS.AN-2
		RS.AN-3	RS.AN-3	RS.AN-3	RS.AN-3
		RS.AN-4	RS.AN-4	RS.AN-4	RS.AN-4
	Mitigation	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-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-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.

		Maintain Personnel Safety	Maintain Environmental Safety	Maintain Quality of Product	Maintain Production Goals
Category		Subcategories			
Recover	Recovery Planning	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-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-2	RC.CO-2	RC.CO-2	RC.CO-2
		RC.CO-3	RC.CO-3	RC.CO-3	RC.CO-3

6. Risk Management

6.1 Risk Management and the Cybersecurity Framework

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.

Risk management is the ongoing process of identifying, assessing, and responding to the extent to which an entity is threatened by a potential circumstance or event. To manage risk, manufacturers should understand the likelihood that an event will occur and the resulting impact. With this information, manufacturers can determine the acceptable level of risk for delivery of products and services and can express this as their risk tolerance.

With an understanding of risk tolerance, manufacturers can prioritize cybersecurity activities, enabling them to make informed decisions about cybersecurity expenditures. Implementation of risk management programs offers manufacturers the ability to quantify and communicate adjustments to their cybersecurity programs. Manufacturers may choose to handle risk in different ways, including mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk, depending on the potential impact to the delivery of critical services.

6.2 Manufacturing System Categorization

A categorization of the manufacturing system's risk level designation is the starting point for applying the Profile to the system. The categorization is based on the potential impact if a security breach jeopardizes the manufacturing system or components, operational assets, individuals, or the organization. Security categorizations are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization. FIPS 199, for example, defines three levels of potential impact on systems should there be a breach of security (i.e., a loss of integrity, availability, or confidentiality). The application of these definitions must take place within the context of the organization, facility, and manufacturing system.

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, assets, or individuals.
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, assets, or individuals
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, assets, or individuals.

A limited adverse effect means that, for example, the loss of integrity, availability, or confidentiality might: (i) cause a degradation in mission capability to an extent and duration that the system is able to perform its primary functions, but the effectiveness of the functions is

noticeably reduced; (ii) result in minor damage to operational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

A serious adverse effect means that, for example, the loss of integrity, availability, or confidentiality might: (i) cause a significant degradation in mission capability to an extent and duration that the system is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to operational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that 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: (i) 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; (ii) result in major damage to operational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

The security categorization process influences the level of effort expended when implementing the Profile. Manufacturing systems supporting the most critical and/or sensitive operations and assets demand the greatest level of attention and effort to ensure that appropriate operational security and risk mitigation are achieved.

The tables below provide examples of mission-based rationale for selecting the security categorization of the manufacturing system. *Examples are taken from the NIST SP 800-82(Rev. 2)*

Possible Definitions for Manufacturing System Impact Levels Based on ISA99

Impact Category	Low-Impact	Moderate-Impact	High-Impact
Injury	Cuts, bruises requiring first aid	Requires hospitalization	Loss of life or limb
Financial Loss	\$1,000	\$100,000	Millions
Environmental Release	Temporary damage	Lasting damage	Permanent damage, off-site damage
Interruption of Production	Minutes	Days	Weeks
Public Image	Temporary damage	Lasting damage	Permanent damage

Possible Definitions for Manufacturing System Impact Levels Based on Product Produced and Industry Concerns

Category	Low-Impact	Moderate-Impact	High-Impact
Product Produced	Non-hazardous materials or products Non-ingested consumer products	Some hazardous products or steps during production High amount of proprietary information	Critical infrastructure (e.g., electricity) Hazardous materials Ingested products
Industry Examples	Plastic injection molding Warehouse applications	Automotive metal industries Pulp and paper Semiconductors	Utilities Petrochemical Food and beverage Pharmaceutical

6.3 Profile Categorization Supporting Structure

The LOW, MODERATE, and HIGH impacts identify security capability, functionality, and specificity for a defined risk level. The Manufacturing Profile defines LOW, MODERATE, and HIGH security levels. A manufacturer or industry sector applies the Profile to a manufacturing system by selecting an initial security level for the manufacturing system based on their security categorization as determined using the guidance in 6.2. The higher security levels are used in manufacturing systems and environments of operation requiring greater protection due to the potential adverse impacts for the higher categorized systems, or when manufacturers seek additions to the base control functionality due to specific organizational assessments of risk.

Each security level is positioned as the platform to support the next higher security level implementation. The security level implementation starts with Low and increases in rigor through the Moderate and High security level implementations. The Low security level represents the starting guidance for low risk manufacturing systems. The Moderate security level will implement the Low security level language as well as the Moderate language. The High security level will implement all of the Low and Moderate language as well as the High language.

7. Manufacturing Profile Subcategory Guidance

Function	Category	Subcategory	Manufacturing Profile
IDENTIFY	ID.AM	ID.AM-1	Low
			Document an inventory of manufacturing system components that reflects the current system. Manufacturing system components include for example PLCs, sensors, actuators, robots, machine tools, firmware, network switches, routers, power supplies, and other networked components or devices. System component inventory is reviewed and updated as defined by the organization.
			Information deemed necessary for effective accountability of information 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.
			Moderate
			Employ automated mechanisms where feasible to detect the presence of unauthorized hardware and firmware components within the system.
		High	
		Identify individuals who are both responsible and accountable for administering manufacturing system components.	
		ID.AM-2	Low
			Document an inventory of manufacturing system software components that reflects the current system. Manufacturing system software components include for example software license information, software version numbers, HMI and other ICS component applications, software, operating systems. System software inventory is reviewed and updated as defined by the organization.
			Moderate
Update the inventory of manufacturing system software as an integral part of component installations, removals, and system updates. Employ automated mechanisms where feasible to detect the presence of unauthorized software within the system.			
High			
Identify individuals who are both responsible and accountable for administering manufacturing system software.			

Function	Category	Subcategory	Manufacturing Profile
IDENTIFY		ID.AM-3	Low
			<p>Document all connections within the manufacturing system, and between the manufacturing system and other systems. All connections are documented, authorized, and reviewed.</p> <p>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.</p>
			Moderate and High
		ID.AM-4	Low
			<p>Identify and document all external connections for the manufacturing system. Examples of external systems include engineering design services, and those that are controlled under separate authority, personal devices, and other hosted services.</p>
		Moderate and High	
		<p>Require external providers to identify the functions, ports, protocols, and other services required for the use with the manufacturing system.</p>	
		ID.AM-5	Low, Moderate and High
			<p>Identify and prioritize manufacturing system components and functions based on their classification, criticality, and business value.</p> <p>Identify the types of information in possession, custody, or control for which security safeguards are needed (Sensitive and Protected Information). Address the security of Protected Information in its third-party relationships.</p>
		ID.AM-6	Low, Moderate and High
			<p>Establish and maintain personnel cyber security roles and responsibilities for the manufacturing system. Include security roles and responsibilities for third-party providers.</p> <p>Third-party providers are required to notify the organization of any personnel transition (including transfers or terminations) involving personnel with physical or logical access to the manufacturing system components.</p> <p>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.</p>

Function	Category	Subcategory	Manufacturing Profile
IDENTIFY	ID.BE	ID.BE-1	Low and Moderate Define and communicate the layers of the supply chain. Document and communicate the cycle of the input of materials to products delivered. Identify the upstream and downstream supply channels that are outside of the organization's operations. Identify the overall mission supported by the manufacturing system.
			High Protect against supply chain threats to the manufacturing system, system component, or system service by employing security safeguards as part of a comprehensive, defense-in-breadth security strategy.
		ID.BE-2	Low, Moderate and High Define and communicate the manufacturer's place in critical infrastructure and its industry sector. Protection strategies for the manufacturing system are based on the prioritization of critical assets and resources. Security issues are addressed in the development, documentation, and updating of a critical infrastructure and key resources protection plan.
		ID.BE-3	Low, Moderate and High Establish and communicate priorities for manufacturing mission, objectives, and activities. Identify critical manufacturing system components and functions by performing a criticality analysis.
		ID.BE-4	Low Identify supporting services for critical manufacturing system components and functions. Provide a short-term uninterruptible power supply to facilitate the transition of the manufacturing system to long-term alternate power in the event of a primary power source loss.
			Moderate and High Identify alternate and redundant supporting services for its critical manufacturing processes and components.

Function	Category	Subcategory	Manufacturing Profile
IDENTIFY		ID.BE-5	Low
			Resilience requirements for the manufacturing system to support delivery of critical services are established. Critical services utilized in the manufacturing process are identified and prioritized.
			Moderate
			Define a time period for the resumption of essential manufacturing functions. Identify critical manufacturing system assets supporting essential missions and business functions.
			High
			Conduct capacity planning so that necessary capacity for manufacturing system processing, telecommunications, and environmental support exists during contingency operations. Plan 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.
IDENTIFY	ID.GV	ID.GV-1	Low, Moderate and High
			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.
		Ensure that 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
			Develop and disseminate manufacturing security program plan that includes, for example, the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance. This includes security requirements and security roles and responsibilities for third-party providers.

Function	Category	Subcategory	Manufacturing Profile
IDENTIFY		ID.GV-3	<p style="text-align: center;">Low, Moderate and High</p> <p>Ensure that legal and regulatory requirements affecting the manufacturing operations regarding cybersecurity are understood and managed.</p>
		ID.GV-4	<p style="text-align: center;">Low, Moderate and High</p> <p>Develop a comprehensive strategy to manage risk to manufacturing operations. Cybersecurity considerations are included in the risk management strategy.</p>
	ID.RA	ID.RA-1	<p style="text-align: center;">Low and Moderate</p> <p>Develop a plan to identify, document, and report vulnerabilities that exist on the manufacturing system. Include the use of vulnerability scanning where feasible on the manufacturing system, its components, or a representative system. Develop a plan for continuous monitoring of the security posture of the manufacturing system to facilitate ongoing awareness of vulnerabilities. Conduct risk assessments on the manufacturing system that take into account vulnerabilities and potential impact to manufacturing operations and assets.</p>
			<p style="text-align: center;">High</p> <p>Conduct performance/load testing and penetration testing on the manufacturing system with care to ensure that manufacturing operations are not adversely impacted by the testing process. Identify where manufacturing system vulnerabilities may be exposed to adversaries. Production systems may need to be taken 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.</p>

Function	Category	Subcategory	Manufacturing Profile
IDENTIFY		ID.RA-2	Low and Moderate
			<p>Establish and maintain ongoing contact with security groups and associations, and 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.</p> <p>Collaborate and share information about potential vulnerabilities and incidents on a timely basis. The DHS National Cybersecurity & Communications Integration Center (NCCIC), http://www.dhs.gov/about-national-cybersecurity-communications-integration-center 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) http://ics-cert.us-cert.gov/ics-cert/ collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures.</p>
		High	
		<p>Employ automated mechanisms where technically feasible to make security alert and advisory information available throughout the organization.</p>	
		ID.RA-3	Low, Moderate and High
ID.RA-4	Low, Moderate and High		
ID.RA-5	Low, Moderate and High		
<p>Conduct risk assessments of the manufacturing system, including threats, vulnerabilities, likelihood, and impact to organizational operations, assets, and individuals, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the manufacturing system.</p>			

Function	Category	Subcategory	Manufacturing Profile
IDENTIFY		ID.RA-6	<p>Low, Moderate and High</p> <p>Develop and implement a comprehensive strategy to manage risk to the manufacturing system. Implement a process for ensuring that risk responses are developed and maintained to adequately respond to risk.</p>
	ID.RM	ID.RM-1	<p>Low, Moderate and High</p> <p>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.</p>
		ID.RM-2	<p>Low, Moderate and High</p> <p>Develop a risk management strategy that includes an unambiguous expression of the risk tolerance for the manufacturing system, acceptable risk assessment methodologies, risk mitigation strategies, a process for consistently evaluating risk to manufacturing systems across the organization with respect to risk tolerance, and approaches for monitoring risk over time.</p>
		ID.RM-3	<p>Low, Moderate and High</p> <p>Ensure the risk tolerance for the manufacturing system is informed by the organization's role in critical infrastructure and sector-specific risk analysis.</p>
PROTECT	PR.AC	PR.AC-1	<p>Low</p> <p>Establish and manage identification mechanisms and credentials for users and devices of the manufacturing system.</p> <p>Moderate</p> <p>Employ automated mechanisms where feasible to support the management and auditing of information system credentials.</p> <p>High</p> <p>Deactivate system credentials after a specified time period of inactivity. Monitor the manufacturing system for atypical use of system credentials. Credentials associated with significant risk are disabled.</p>

Function	Category	Subcategory	Manufacturing Profile
PROTECT		PR.AC-2	Low
			<p>Protect physical access to the manufacturing facility. Physical access controls may include, for example, lists of authorized individuals, identity credentials, escort requirements, guards, fences, turnstiles, locks, monitoring of facility access. Determine access requirements during emergency situations.</p>
			Moderate
		<p>Protect power equipment, power cabling, network cabling, and network access interfaces for the manufacturing system from accidental damage, disruption, and physical tampering. Employ redundant and physically separated power cables for critical manufacturing operations.</p>	
		High	
		<p>Control physical access to the manufacturing system in addition to the physical access for the facility.</p>	
		PR.AC-3	Low
<p>Establish usage restrictions, connection requirements, implementation guidance, and authorizations for remote access to the manufacturing system. Remote access methods include, for example, wireless, dial-up, broadband, VPN connections, mobile device connections, and communications through external networks.</p>			
Moderate and High			
<p>Allow remote access only through approved and managed access points. Monitor remote access to the manufacturing system, and employ 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.</p>			
PR.AC-4	Low		
<p>Define and manage access permissions for users of the manufacturing system.</p>			

Function	Category	Subcategory	Manufacturing Profile
PROTECT			Moderate
			<p>Employ automated mechanisms where feasible to support the management of manufacturing system user accounts, including the disabling, auditing, notifications, and removal of user accounts. Create separation for duties of users on the manufacturing system. Limit and explicitly authorize privileged user access to the manufacturing system. Audit the execution of privileged functions on the manufacturing system.</p> <p>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.</p>
			High
		PR.AC-5	Low
			<p>Protect network integrity of the manufacturing system, incorporating network 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. Employ boundary protection devices. Boundary protection mechanisms include, for example, routers, gateways, data diodes, and firewalls separating system components into logically separate networks or subnetworks.</p>
			Moderate
<p>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.</p>			
High			
<p>Employ, where feasible, authenticated proxy servers for defined communications traffic between the manufacturing system and external networks.</p> <p>Isolate manufacturing system components performing different missions.</p>			

Function	Category	Subcategory	Manufacturing Profile
PROTECT	PR.AT	PR.AT-1	Low Provide security awareness training for all manufacturing system users and managers. The content can include, for example, a basic understanding of the protections and user actions needed to maintain security of the system, responding to suspected security incidents, and awareness of operational security.
			Moderate and High Include recognizing and reporting potential indicators of insider threat into security training.
		PR.AT-2	Low, Moderate and High 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.
			PR.AT-3
		Moderate and High Require providers of external connected systems to identify the functions, ports, protocols, and services necessary for the connection services.	
		PR.AT-4	Low, Moderate and High Ensure that senior executives understand the requirements for the security and protection of the manufacturing system, and their responsibilities for achieving them.
		PR.AT-5	Low, Moderate and High Ensure that personnel responsible for the physical protection and security of the manufacturing system and facility understand their responsibilities. Establish standards for measuring, building, and validating individual qualifications for physical security personnel.

Function	Category	Subcategory	Manufacturing Profile		
PROTECT	PR.DS	PR.DS-1	Low		
			None		
			Moderate and High		
					Protect while at rest manufacturing system information determined to be critical.
		PR.DS-2	Low		
			None		
			Moderate and High		
					Protect manufacturing system information when in transit. Implement cryptographic mechanisms where determined necessary to prevent unauthorized access, distortion, or modification of system data.
		PR.DS-3	Low		
				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.	
			Moderate		
				Update the inventory of manufacturing system components as an integral part of component installations, removals, and system updates.	
High					
			Employ automated mechanisms where feasible to maintain an up-to-date, complete, accurate, and readily available inventory of manufacturing system components. Ensure that disposal actions are approved, tracked, documented, and verified.		
PR.DS-4	Low Moderate and High				
		Conduct capacity planning so that adequate resources are maintained for manufacturing information processing, telecommunications, and data storage. Protect the manufacturing system against, or limits the effects of, denial of service attacks. Off-load audit records from the manufacturing system for processing to an alternate system.			

Function	Category	Subcategory	Manufacturing Profile
PROTECT		PR.DS-5	<p style="text-align: center;">Low</p> <p>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. Heighten system monitoring activity whenever there is an indication of increased risk to manufacturing operations and assets. Develop and document access agreements for all users of the manufacturing system.</p>
			<p style="text-align: center;">Moderate and High</p> <p>Regulate the information flow within the manufacturing system and to outside systems. Enforce controls restricting connections to only authorized interfaces. Protect the system from information leakage due to electromagnetic signals emanations.</p>
		PR.DS-6	<p style="text-align: center;">Low</p> <p>None</p>
	<p style="text-align: center;">Moderate</p> <p>Employ Software, firmware, and information integrity checks to detect unauthorized changes to manufacturing system components during startup and when determined necessary. Incorporate the detection of unauthorized changes to the manufacturing system into the system's incident response capability.</p>		
	<p style="text-align: center;">High</p> <p>Employ automated tools where feasible to provide notification upon discovering discrepancies during integrity verification. Employ automatic response capability with pre-defined security safeguards when integrity violations are discovered.</p>		
		PR.DS-7	<p style="text-align: center;">Low, Moderate and High</p> <p>Employ separate development and testing environments from the production environment.</p>
	PR.IP	PR.IP-1	<p style="text-align: center;">Low</p> <p>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. Configure the manufacturing system to provide only essential capabilities. Review the baseline configuration and disable unnecessary capabilities.</p>

Function	Category	Subcategory	Manufacturing Profile
PROTECT			Moderate
			<p>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. Employ 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. Employ a deny-all, permit-by-exception policy to allow the execution of only authorized software programs.</p>
		High	
		<p>Employ automated mechanisms where feasible to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the manufacturing system Automated system support includes for example, documentation, notification, and management of the change control process on the manufacturing system. Review system changes to determine whether unauthorized changes have occurred.</p>	
		PR.IP-2	Low
			<p>Manage the manufacturing system using a system development life cycle that includes security considerations. Include security requirements into the acquisition process of the manufacturing system and its components.</p>
Moderate and High			
<p>Require the developer of the manufacturing system and system components to provide a description of the functional properties of the security controls, and design implementation material for security-relevant system interfaces. Apply security engineering principles into the specification, design, development, implementation, and modification of the manufacturing system. Employ configuration management and change control during the development of the manufacturing system and its components, and include flaw tracking and resolution, and security testing.</p>			
PR.IP-3	Low		
<p>Employ configuration change control for the manufacturing system and its components. Conduct security impact analyses in connection with change control reviews.</p>			

Function	Category	Subcategory	Manufacturing Profile
PROTECT			Moderate
			<p>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.</p>
			High
			<p>Employ automated mechanisms where feasible to support the change control process. Conduct security impact analysis in a separate test environment before implementation into an operational environment for planned changes to the manufacturing system.</p>
	PR.IP-4	Low	
		<p>Conduct and maintain backups for manufacturing system data. Manufacturing system data includes for example software, configurations and settings, documentation, system configuration data include computer configuration backups, application configuration backups, operational control limits, control bands and set points for pre-incident operation for all ICS programmable equipment.</p>	
Moderate			
<p>Verify the reliability and integrity of backups. Coordinate backup testing with organizational elements responsible for related plans. Establish a separate alternate storage site for system backups and ensure the same security safeguards are employed.</p>			
PR.IP	PR.IP-5	Low	
		<p>Define, implement, and enforce policy and regulations regarding emergency shutoff, emergency lighting, fire protection, temperature and humidity controls, and water damage protection.</p>	
Moderate			
<p>Employ automatic fire suppression capability for the manufacturing system when the facility is not staffed on a continuous basis.</p>			

Function	Category	Subcategory	Manufacturing Profile
PROTECT			<p>High</p> <p>Employ fire detection devices that activate and notify automatically in the event of a fire.</p>
		PR.IP-6	<p>Low and Moderate</p> <p>Ensure that manufacturing system data is destroyed according to policy.</p>
			<p>High</p> <p>Ensure that media sanitization actions are approved, tracked, documented, and verified. Test sanitation equipment and procedures. Apply nondestructive sanitization techniques to portable storage devices connecting to the manufacturing system.</p>
		PR.IP-7	<p>Low</p> <p>Incorporate improvements derived from the monitoring, measurements, assessments, and lessons learned into protection process revisions. Ensure that the security plan for the manufacturing system provides for the review, testing, and continual improvement of the security protection processes.</p>
			<p>Moderate and High</p> <p>Employ independent teams to assess the protection process.</p>
PR.IP-8	<p>Low, Moderate and High</p> <p>Collaborate and share information about manufacturing system related security incidents and mitigation measures with designated sharing partners. Employ automated mechanisms where feasible to assist in information collaboration.</p> <p>Manufacturing systems are often connected to business systems or interconnected. Any single system can be an attack vector for all systems. It is therefore necessary to provide a uniform defense encompassing all baselines.</p>		
PR.IP	PR.IP-9	<p>Low</p> <p>Develop and maintain plans that identify essential functions and associated contingency requirements, as well as providing a roadmap for implementing incident response. Define recovery objectives, restoration priorities, and metrics. Address contingency roles, including individual assignments and contact information. Address maintaining essential functions despite system disruption, and the eventual restoration of the manufacturing system. Define incident types, and the resources and management support needed to effectively maintain and mature the incident response and contingency capabilities.</p>	

Function	Category	Subcategory	Manufacturing Profile
PROTECT			<p>Moderate and High</p> <p>Coordinate contingency plan development with elements responsible for related plans.</p>
		PR.IP-10	<p>Low</p> <p>Test response and recovery plans to determine the effectiveness of the plans, and the readiness to execute the plans.</p>
			<p>Moderate and High</p> <p>Coordinate plan testing with organizational elements responsible for related plans. 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.</p>
		PR.IP-11	<p>Low, Moderate and High</p> <p>Develop and maintain a personnel security program for the manufacturing system that includes policy, position risk designations, personnel screening, terminations and transfers, access agreements, third-party roles and responsibilities, and personnel sanctions.</p>
	PR.IP-12	<p>Low</p> <p>Establish and maintain a process that allows continuous overview of vulnerabilities, and defines the strategy to mitigate them.</p>	
		<p>Moderate</p> <p>Restrict access to privileged vulnerability data.</p>	
		<p>High</p> <p>Identify where the manufacturing system vulnerabilities may be exposed to adversaries.</p>	
	PR.MA	PR.MA-1	<p>Low</p> <p>Ensure that maintenance and repairs conducted on the manufacturing system control and IT components are scheduled, approved, performed, documented, and reviewed. Enforce authorization requirements for removal of system components and media sanitation, prior to removal for offsite maintenance or repairs.</p> <p>Verify impacted security controls following maintenance or repairs.</p> <p>Establish a process for maintenance personnel authorization, and escort non-authorized maintenance personnel.</p>

Function	Category	Subcategory	Manufacturing Profile
PROTECT			Moderate
			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 and hardware/software packet sniffers. Inspect maintenance tools brought into the facility. Check media containing diagnostic and test programs for malicious code before they are used on the manufacturing system.
			High
		Employ automated mechanisms where feasible to support maintenance processes. Prevent the unauthorized removal of maintenance equipment containing manufacturing system information.	
		PR.MA-2	Low and Moderate
	Enforce approval requirements, process restrictions, and monitoring, of remote maintenance activities. Employ strong authenticators, record keeping, and session termination for remote maintenance.		
		High	
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.			
	PR.PT	PR.PT-1	Low
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. Ensure that audit processing failures on the manufacturing system generate alerts and trigger defined responses. Generate time stamps from an internal system clock that is mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).			
		Moderate	
Review and update audit events. Employ automated mechanisms to integrate audit review, analysis, and reporting. Compare and synchronize the internal system clocks to an authoritative time source. Authoritative time sources include for example, an internal NTP server, radio clock, atomic clock, GPS time source.			

Function	Category	Subcategory	Manufacturing Profile
PROTECT			<p style="text-align: center;">High</p> <p>Integrate analysis of audit records with physical access monitoring. Conduct time correlation of audit records. Enable authorized individuals to extend audit capabilities when required by events.</p>
		PR.PT-2	<p style="text-align: center;">Low</p> <p>Employ technical safeguards to restrict the use of portable storage devices.</p> <p style="text-align: center;">Moderate and High</p> <p>Protect and control portable storage devices containing manufacturing system data while in transit and in storage.</p>
		PR.PT-3	<p style="text-align: center;">Low</p> <p>Employ technical safeguards to control access to the manufacturing system and assets.</p> <p style="text-align: center;">Moderate and High</p> <p>Disable defined functions, ports, protocols, and services within the manufacturing system deemed to be unnecessary. Employ technical safeguards to enforce a deny-all, permit-by-exception policy to only allow the execution of authorized software programs.</p>
		PR.PT-4	<p style="text-align: center;">Low</p> <p>Monitor and control communications at the external boundary and at key internal boundaries within the manufacturing system.</p> <p style="text-align: center;">Moderate and High</p> <p>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.</p> <p>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.</p>

Function	Category	Subcategory	Manufacturing Profile
DETECT	DE.AE	DE.AE-1	<p style="text-align: center;">Low, Moderate and High</p> <p>Ensure that a baseline of network operations and expected data flows for the manufacturing system is developed, documented, and maintained to detect events.</p>
		DE.AE-2	<p style="text-align: center;">Low</p> <p>Review and analyze detected events within the manufacturing system to understand attack targets and methods.</p> <p style="text-align: center;">Moderate and High</p> <p>Employ automated mechanisms where feasible to review and analyze detected events within the manufacturing system.</p>
		DE.AE-3	<p style="text-align: center;">Low and Moderate</p> <p>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.</p> <p style="text-align: center;">High</p> <p>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.</p>
		DE.AE-4	<p style="text-align: center;">Low</p> <p>Determine adverse impacts to manufacturing operations, assets, and individuals resulting from detected events. Correlate detected event impacts with risk assessment outcomes.</p> <p style="text-align: center;">Moderate</p> <p>Employ automated mechanisms to support impact analysis.</p> <p style="text-align: center;">High</p> <p>Correlate detected event information and event responses to achieve perspective on event impact across the organization.</p>
		DE.AE-5	<p style="text-align: center;">Low and Moderate</p> <p>Define incident alert thresholds for the manufacturing system.</p>

Function	Category	Subcategory	Manufacturing Profile
DETECT	DE.CM		High Employ automated mechanisms where feasible to assist in the identification of security alert thresholds.
			Low Conduct ongoing security status monitoring of the manufacturing system network to detect attacks and indicators of potential attacks. Detect unauthorized local, network, and remote connections, and identify unauthorized use of the manufacturing system. Generate audit records for defined cybersecurity events. Monitor network communications at the external boundary of the system and at key internal boundaries within the system. Heighten system monitoring activity whenever there is an indication of increased risk.
			Moderate Employ automated mechanisms to support detection of cybersecurity events. Generate system alerts when indications of compromise or potential compromise occur.
			High Monitor for and report atypical usage of the manufacturing system.
			Low Conduct ongoing security status monitoring of the manufacturing system facility to detect physical security incidents.
			Moderate and High Employ independent teams to monitor the security of the physical environment. Monitor physical intrusion alarms and surveillance equipment. Monitor physical access to the manufacturing system and devices in addition to the facility.
			Low, Moderate and High Conduct security status monitoring of personnel activity associated with the manufacturing system. Enforce software usage and installation restrictions.

Function	Category	Subcategory	Manufacturing Profile
DETECT		DE.CM-4	Low
			Deploy malicious code protection mechanisms throughout the manufacturing system where feasible to detect and eradicate malicious code.
			Update malicious code protection mechanisms whenever new releases are available in accordance with the configuration management policy and procedures for the manufacturing system. Manage for false positives during malicious code detection and eradication.
			Moderate and High
			Automatically update malicious code protection mechanisms where feasible.
		DE.CM-5	Low
	None		
	Moderate and High		
			Define acceptable and detect unacceptable mobile code and mobile code technologies. 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
			Conduct ongoing security status monitoring of external service provider activity on the manufacturing system. Detect attacks and indicators of potential attacks from external service providers. Monitor compliance of external providers with personnel security policies and procedures, and contract security requirements.

Function	Category	Subcategory	Manufacturing Profile
DETECT		DE.CM-7	Low
			Conduct ongoing security status monitoring on the manufacturing system for unauthorized personnel, connections, devices, access points, and software. Monitor for system inventory discrepancies.
			Deploy monitoring devices strategically within the manufacturing system to collect essential information to detect specific events of interest.
			Moderate and High
		Monitor for unauthorized configuration changes to the manufacturing system.	
			Low, Moderate and High
	DE.CM-8	Conduct vulnerability scans on the manufacturing system where feasible. Include analysis, remediation, and information sharing in the vulnerability scanning process. Employ control system-specific vulnerability scanning tools and techniques where 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.	
DE.DP	DE.DP-1	Low, Moderate and High	
		Define roles and responsibilities for detection activities on the manufacturing system and ensure accountability.	
DE.DP-2	Low , Moderate and High		
	Conduct detection activities in accordance with applicable federal and state laws, industry regulations and standards, policies, and other applicable requirements.		
DE.DP-3	Low , Moderate and High		
	Monitor and validate that event detection processes are operating as intended.		

Function	Category	Subcategory	Manufacturing Profile
		DE.DP-4	<p style="text-align: center;">Low</p> <p>Communicate event detection information to defined personnel.</p> <p>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 VoIP, and malware disclosure.</p>
			<p style="text-align: center;">Moderate and High</p> <p>Employ automated mechanisms and system generated alerts to support event detection communication.</p>
		DE.DP-5	<p style="text-align: center;">Low</p> <p>Incorporate improvements derived from the monitoring, measurements, assessments, and lessons learned into detection process revisions.</p> <p>Ensure the security plan for the manufacturing system provides for the review, testing, and continual improvement of the security detection processes.</p>
			<p style="text-align: center;">Moderate</p> <p>Employ independent teams to assess the detection process.</p>
RESPOND	RS.RP	RS.RP-1	<p style="text-align: center;">Low, Moderate and High</p> <p>Execute the response plan during or after a cybersecurity event on the manufacturing system.</p>
	RS.CO	RS.CO-1	<p style="text-align: center;">Low, Moderate and High</p> <p>Verify objectives, restoration priorities, task sequences and assignment responsibilities for event response measures.</p>

Function	Category	Subcategory	Manufacturing Profile
RESPOND		RS.CO-2	Low Employ prompt reporting to appropriate recipients for cybersecurity events on the manufacturing system. Ensure that cybersecurity events on the manufacturing system are reported consistent with the response plan.
			Moderate and High Employ automated mechanisms to assist in the reporting of security incidents.
		RS.CO-3	Low, Moderate and High Share cybersecurity event information with defined parties per the response plan.
		RS.CO-4	Low Coordinate cybersecurity event response actions with all relevant stakeholders. Stakeholders for event 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 Employ automated mechanisms to support stakeholder coordination.
	RS.CO-5	Low, Moderate and High 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), http://www.dhs.gov/about-national-cybersecurity-communications-integration-center , 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) http://ics-cert.us-cert.gov/ics-cert/ , collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures.	
	RS.AN	RS.AN-1	Low Investigate security-related notifications generated from detection systems.

Function	Category	Subcategory	Manufacturing Profile
RESPOND			<p>Moderate and High</p> <p>Employ automated mechanisms to assist in the investigation and analysis of notifications.</p>
		RS.AN-2	<p>Low</p> <p>Understand the full implication of the security event based on thorough investigation and analysis results. Correlate detected event information and event responses with risk assessment outcomes to achieve perspective on event impact across the organization.</p>
			<p>Moderate and High</p> <p>Employ automated mechanisms to support impact analysis.</p>
		RS.AN-3	<p>Low</p> <p>Conduct forensic analysis on collected security event information to determine root cause.</p>
	<p>Moderate and High</p> <p>Provide on-demand audit review, analysis, and reporting for after-the-fact investigations of security events.</p>		
	RS.AN-4	<p>Low, Moderate and High</p> <p>Categorize cybersecurity incidents according to level of severity and impact consistent with the response plan.</p>	
	RS.MI	RS.MI-1	<p>Low, Moderate and High</p> <p>Contain security-related incidents to minimize impact on the manufacturing system.</p>
		RS.MI-2	<p>Low</p> <p>Mitigate security incidents occurring on the manufacturing system.</p>
			<p>Moderate and High</p> <p>Employ automated mechanisms to support the security incident mitigation process.</p>
	RS.MI-3	<p>Low, Moderate and High</p> <p>Ensure that vulnerabilities identified while responding to a security incident are mitigated or documented as accepted risks.</p>	

Function	Category	Subcategory	Manufacturing Profile
RESPOND	RS.IM	RS.IM-1	<p>Low, Moderate and High</p> <p>Incorporate lessons learned from ongoing event handling activities into event response procedures, training, and testing, and implement the resulting changes accordingly.</p>
		RS.IM-2	<p>Low, Moderate and High</p> <p>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.</p> <p>Updates may include, for example, responses to disruptions or failures, and predetermined procedures.</p> <p>Enable a process for the response plan to evolve to reflect new threats, improved technology, and lessons learned.</p>
RECOVER	RC.RP	RC.RP-1	<p>Low, Moderate and High</p> <p>Execute the recovery plan during or after a cybersecurity event on the manufacturing system.</p> <p>Restore the manufacturing system within a predefined time-period from configuration-controlled and integrity-protected information representing a known, operational state for the components.</p>
	RC.IM	RC.IM-1	<p>Low, Moderate and High</p> <p>Incorporate lessons learned from ongoing recovery activities into system recovery procedures, training, and testing, and implement the resulting changes accordingly.</p>
		RC.IM-2	<p>Low, Moderate and High</p> <p>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.</p> <p>Validate that updates are worked into the recovery plan as an integral part of the process.</p>

Function	Category	Subcategory	Manufacturing Profile
RECOVER	RC.CO	RC.CO-1	Low
			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
			Assign a Public Relations Officer.
			High
		Pre-establish and groom media contacts. Utilize external assets to manage public relations.	
		RC.CO-2	Low, Moderate and High
			Employ 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.
RC.CO-3	Low, Moderate and High		
	Communicate recovery activities to all relevant stakeholders, and executive and management teams.		

Appendix A - Acronyms and Abbreviations

Appendix A will list and define acronyms and abbreviations used in this publication.

DRAFT

Appendix B - Glossary

Appendix B will provide definitions of key words and phrases used in the publication.

DRAFT

Appendix C - References

- [SP800-53] NIST Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2013 (including updates as of January 15, 2014), 460pp.
<http://dx.doi.org/10.6028/NIST.SP.800-53r4>.

DRAFT