



DoW CONTROL SYSTEMS/ OPERATIONAL TECHNOLOGY SECURITY REQUIREMENTS GUIDE

27 February 2026

Version 2

CLEARED
For Open Publication

Apr 28, 2026

Unclassified

Contents

1 Control Systems/Operational Technology (OT) in the Department of War (DoW).....	1
1.1 Introduction	1
1.2 Scope and Applicability	2
1.3 Terms and Concepts	4
1.4 Security Requirements Guides (SRGs) / Security Technical Implementation Guides (STIGs)	8
1.5 Document Revisions, Comments, Availability Update Cycle.....	8
1.6 Business Mission Objectives for Control Systems/OT	9
Maintain System Availability	10
Maintain System Integrity	10
Maintain Human Safety.....	11
Maintain Environmental Safety.....	11
Maintain Physical Security	12
1.7 System Security Objectives for Control Systems/OT	13
1.8 Control System/OT Security Architecture	13
1.9 Cybersecurity Governance for Control Systems/OT.....	16
1.10 System Authorization of Control Systems/OT	16
1.11 Cyberspace Defense and Incident Response in the Control System/OT Environment	17
2 Cybersecurity Framework (CSF) Control System/OT Profiles.....	18
2.1 CSF Profile Purpose and Scope.....	20
2.2 CSF Profile Priority Matrix	22
2.3 CSF High Priority Rationale.....	70
Mission Objective 1: Maintain System Availability	70
Mission Objective 2: Maintain System Integrity	97
Mission Objective 3: Maintain Human Safety.....	125
Mission Objective 4: Maintain Environmental Safety	140
Mission Objective 5: Maintain Physical Security.....	154
3 System Security Requirements for Control Systems/OT	177
3.1 Minimum Standards for Cybersecurity	177
3.2 Adapted Scope and Intent of Security Control Families	178

3.3 DoW Policy Regarding Security Controls..... 186

3.4 System Security Requirements Mapping Tables 187

Appendix A References 210

Appendix B Glossary..... 212

Appendix C Framework Glossary 217

1 Control Systems/Operational Technology (OT) in the Department of War (DoW)

1.1 Introduction

Control systems/OT underpin the operation of all DoW missions and are key elements in many diverse DoW operating environments. Control systems/OT – which typically consist of controllers and user interfaces that monitor and control equipment – are prevalent and essential to the function of *weapon systems, utilities, facilities, medical systems, manufacturing and the defense industrial base*. This variance in mission functions and disciplines means that these communities of interest have different terminology and accepted norms. However, there are also areas of commonality in terms of system objectives and the cybersecurity activities necessary to protect them as well as types of cybersecurity risks.

Control systems/OT also pose unique risks due to their interaction with the physical world. These cyber to physical interactions can have unintended and disastrous implications. For example, at a NASA research facility: “a security patch caused monitoring equipment in a large engineering oven to stop running, resulting in a fire that destroyed spacecraft hardware inside the oven. The computer reboot caused by the software upgrade also impeded alarm activation, leaving the fire undetected for 3.5 hours before it was discovered.”¹ Though unintended, this cyber to physical incident highlights risks that adversaries could utilize to not just delay or stop critical business functions of the Department, but also to cause environmental and physical harm, including the loss of life.

These risks are increased from the proliferation of cyber physical systems in the National Security environment. The combination of the importance of control systems/OT and relevance to National Security requires specific considerations and guidance to ensure that all risk and threats are managed according to risk management policies. Understanding National Security Systems (NSS) and critical system dependencies on control systems/OT is a priority and those dependencies should be a factor for all system owners when managing risks to their systems.

The Control systems/OT Security Requirements Guide (SRG) seeks to streamline and unify the Department’s risk-based approach to managing control systems/OT cybersecurity. It utilizes and integrates the Cybersecurity Framework (CSF) to aid organizational risk management and the DoW Risk Management Framework (RMF) to enable system risk management.

A traditional SRG focuses on security control implementation in specific systems or technology types. This SRG provides higher-level orientation to inform organizational cybersecurity

¹ Industrial Control System Security Within NASA’S Critical And Supporting Infrastructure:
<https://oig.nasa.gov/docs/IG-17-011.pdf>

activities for all control systems/OT in the DoW in addition to providing guidance on security requirements for control systems/OT, regardless of individual system type or unique operating environment. This broader approach is necessary to enhance planning and overall execution of cybersecurity risk management for control systems/OT as cybersecurity maturity in many of these systems is minimal or technically unfeasible in contrast to traditional systems.

The audience for this SRG includes:

- DoW Components, Program Executive Offices, Program Offices and Mission Owners using, or considering the use of control systems/OT.
- DoW programs that utilize control systems/OT or operate in control system/OT environments.
- DoW Authorizing Officials and their representatives.
- Control systems/OT Operators.

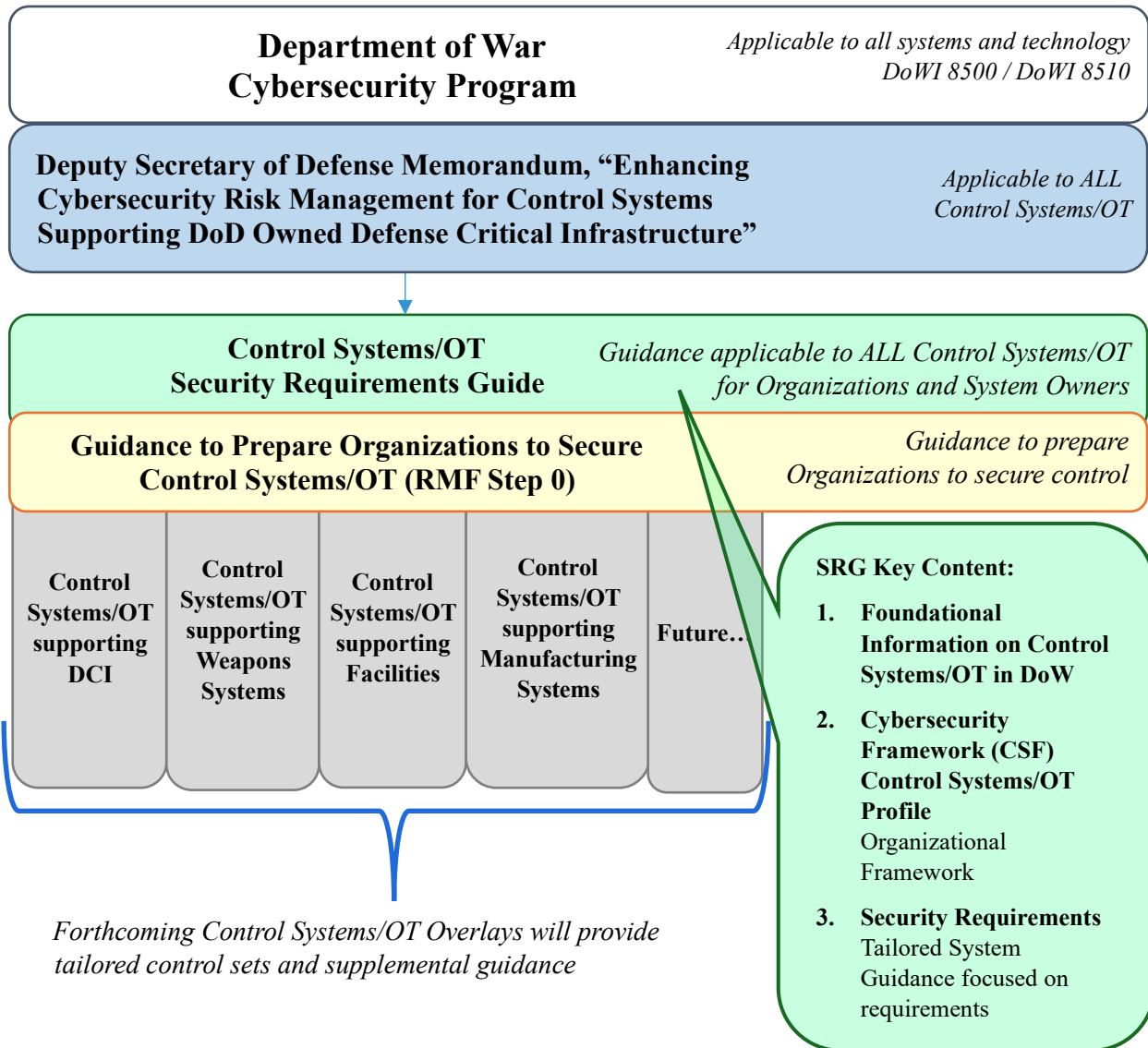
The following document consists of three primary sections. First, foundational material to orient the reader to the scope, applicability, cybersecurity concepts and terminology used in the SRG. Second, a Cybersecurity Framework (CSF) profile, a specific artifact to help organizations and stakeholders with the *prepare* step to organize cybersecurity implementation at an organization level. Third, specific security requirements guidance to aid systems to better shape and describe the spirit and intent of security requirements for control systems/OT.

1.2 Scope and Applicability

This SRG, in support of DoWI 8510.01, establishes the DoW security objectives for all control systems/OT. Personnel may apply this SRG to environments classified as publicly releasable up to and including TOP SECRET General Service (GENSER). Missions including control systems/OT with a Sensitive Compartmented Information (SCI) classification must follow existing DoW and Intelligence Community (IC) policies, as applicable. This SRG does not provide guidance for operation environments with SCI classification levels.

This SRG supports the responsibilities of DoW Component heads, per 44 USC 3534 (a) (1) (ii) Federal Information Security Management Act (FISMA), to provide protections for systems used or operated by an agency, contractor of an agency, or other organization on behalf of an agency.

This DoW SRG applies to all control systems/OT, including weapon systems, operated by or on behalf of the DoW by a contractor or other entity.



Owners or operators can be DoW Components, United States (U.S.) Government agencies, or commercial entities. DoW control systems/OT are likely to support the following:

- Control systems/OT supporting National Security Systems (e.g. weapons systems)
- Control systems/OT supporting Medical Systems
- Control systems/OT supporting Facilities
- Control systems/OT supporting Manufacturing

This DoW SRG complements the existing RMF procedures for cybersecurity programs described in DoWI 8500.01, *Cybersecurity*, by providing consistent requirements based on common strategic objectives for deploying control systems/OT and the cybersecurity activities that are most critical for meeting those objectives. Each DoW organization retains the autonomy to determine its own risk tolerance for Control systems/OT using the policy requirements articulated by the DoWI 8500 series, guidelines found on the Cybersecurity Knowledge Service, and the parameters of organization-specific cybersecurity programs, and can adjust the requirements in this DoW SRG as needed to best support the needs of its specific environment.

1.3 Terms and Concepts

This SRG introduces terminology and concepts unique to specific control system/OT environments while also relying on terms used throughout the cyber domain to better orient cybersecurity practitioners (e.g., Availability Requirements, Cyber-Physical considerations). Still, the intent is to describe security objectives tailored to the unique requirements of control system/OT environments rather than apply traditional information system methods that may not be applicable to control system/OT environments.

Control systems/OT are systems in which deliberate guidance or manipulation is used to achieve a prescribed value for a variable. Control systems/OT include Supervisory Control and Data Acquisition (SCADA), industrial and process controls systems, cyber-physical systems, facilities-related control systems/OT and other types of industrial measurement and control systems/OT. Control systems/OT often consist of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy).

Examples of control system/OT implementation that support DoW include:

- SCADA in a power system
- Air conditioning/ air filtering systems
- Water level controllers
- Chemical filtering systems
- Emergency management systems
- Surveillance systems
- Pharmaceutical applications
- Discrete manufacturing
- A multitude of other industrial fields

A control system/OT consists of several components that segment it from the structure of a standard Information Technology (IT) system. This SRG adheres to NIST definitions to characterize and standardize the discussion of control systems/OT. Essential characteristics of a control system/OT are defined as follows:

Sensors: A sensor is a device, which responds to an input quantity by generating a functionally related output usually in the form of an electrical or optical signal.

Actuators: An actuator is used to directly manipulate the controlled processes of a mechanism or system.

Controllers: The part of the control system/OT used to perform the monitoring and control of the physical process. This includes all control servers, field devices, actuators, sensors, and their supporting communication systems.

Process: The component of the system that deals directly with producing the desired output or performance.

Human Machine Interface (HMI): A hardware or software through which an operator interacts with a controller. An HMI can range from a physical control panel with buttons and indicator lights to an industrial PC with a graphics display running dedicated HMI software.

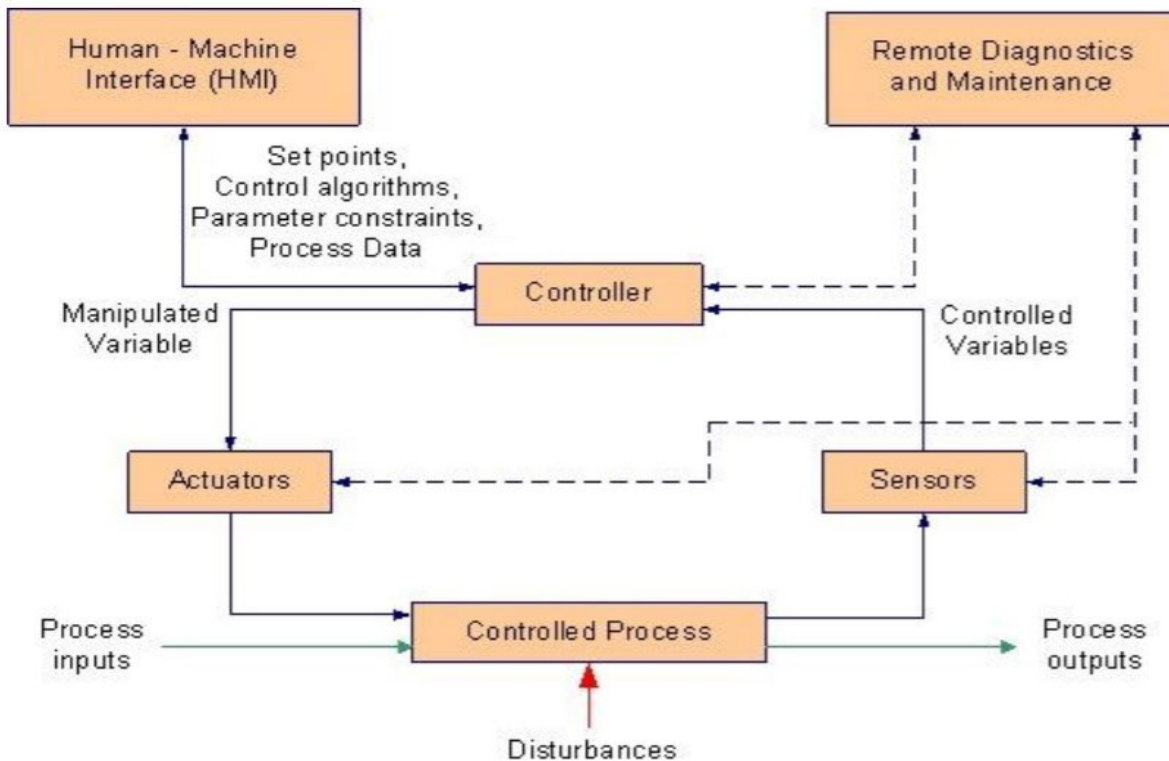


Figure 1: NIST 800-82 (Fig. 2-1 Control System/OT Components)

These key components are what allow control systems/OT to take input from and interact with the environment, making them unique from traditional IT systems and environments. In addition to a control system's essential characteristics, there are three major control system/OT types that can be implemented individually or in concordance with one another. NIST SP 800-82, Rev 2 defines these control system/OT types below:

Supervisory Control and Data Acquisition (SCADA) systems are used to control dispersed assets and rely on centralized data acquisition just as much as control. SCADA systems integrate data acquisition systems with data transmission systems and HMI software to provide a centralized monitoring and control system/OT for numerous process inputs and outputs. SCADA systems are designed to collect field information, transfer it to a central computer facility, and display the information to the operator graphically or textually, thereby allowing the operator to monitor or control an entire system from a centrally remote location in near real time. Use cases for SCADA systems include water distribution and collection systems, mass transit electricity regulation, HVAC systems in large facilities, and many other distribution systems.

Distributed Control Systems (DCS) control production systems within the same geographic location. These systems are usually process control or discrete part control systems/OT. DCS are integrated as a control architecture containing a supervisory level of control overseeing multiple, integrated sub-systems that are responsible for controlling details of a localized process. A DCS uses a centralized supervisory control loop to mediate a group of localized controllers that share the overall tasks of carrying out an entire production process." Use cases for DCS include systems in water treatment plants, pharmaceutical manufacturing, oil refineries, automobile manufacturing, etc.

Programmable Logic Controller (PLC) topologies are used in both SCADA and DCS systems as the control components of an overall hierarchical system to provide local management of processes through feedback control. PLCs also have the capability to be implemented as the primary controller in smaller control system/OT configurations to provide operational control of discrete processes. PLC topologies tend to differ from SCADA and DCS in that they generally lack a central control server and HMI and, therefore, primarily provide closed-loop control without direct human involvement. PLCs can be found in systems from automobile assembly lines to power plant soot blower controls and are very useful for repetitive and easily automated processes.

Control systems/OT are essential for operation of U.S. defense critical infrastructure. Critical infrastructure consists of the physical and cyber systems and assets so vital to the U.S. that their incapacity or destruction would have a debilitating impact on our physical or economic security, on our public health, and on our safety. When designing a control system, additional considerations must be made compared to those required for designing a traditional IT system.

While control systems/OT and traditional IT systems have similarities, they have differing emphases for functionality and security. For example, a traditional IT system may emphasize the

assurance of confidentiality of sensitive data, while a control system/OT that regulates electricity distribution would prioritize availability controls. As a result, NIST SP 800-82, Rev 2, lists the following factors as additional considerations when developing a control system/OT design:

Control timing: Control system/OT processes have a wide range of time-related requirements, including very high speed, consistency, regularity, and synchronization. Humans may not be able to reliably and consistently meet these requirements; automated controllers may be necessary. Some systems may require the computation to be performed as close to the sensor and actuators as possible to reduce communication latency and perform necessary control actions on time.

Geographic distribution: Supervisory control is used to provide a central location that can aggregate data from multiple locations to support control decisions based on the current state of the system.

Hierarchy: Often a hierarchical and centralized control is used to provide human operators with a comprehensive view of the entire system.

Control complexity: Often control functions can be performed by simple controllers and preset algorithms. However, more complex systems (e.g., air traffic control) require human operators to ensure that all control actions are appropriate to meet the larger objectives of the system.

Availability: The system's availability (i.e., reliability) requirements are also an important factor in design. Systems with strong availability/up-time requirements may require more redundancy or alternate implementations across all communication and control.

Impact of failures: The failure of a control function could incur substantially different impacts across domains. Systems with greater impacts often require the ability to continue operations through redundant controls, or the ability to operate in a degraded state. The design needs to address these requirements.

Safety: The system's safety requirements are also an important factor in design. Systems must be able to detect unsafe conditions and trigger actions to reduce unsafe conditions to safe ones. In most safety-critical operations, human oversight and control of a potentially dangerous process is an essential part of the safety system.

DoW Components must understand these additional considerations when integrating control systems/OT into operations to ensure that system's functionality and security.

1.4 Security Requirements Guides (SRGs) / Security Technical Implementation Guides (STIGs)

SRGs provide non-product specific requirements to mitigate sources of security risks commonly encountered across IT systems and applications. While SRGs define the requirements for various technology families and organizations, the Security Technical Implementation Guides (STIGs) provide detailed guidelines for specific products. In other words, STIGs provide product-specific information for validating, attaining, and continuously maintaining compliance with requirements defined in the SRG for that product's technology area.

A single technology related SRG or STIG is not inclusive for a given system. DoW Components must comply with all SRGs and STIGs applicable to a system. This typically results in a system being subject to multiple SRGs and STIGs.

Newly published SRGs and STIGs generally consist of a technology/product overview document and one or more eXtensible Markup Language (XML) (.xml) files in Extensible Configuration Checklist Description Format (XCCDF).

The security requirements contained within SRGs and STIGs, in general, are applicable to all DoW administered systems, all systems connected to DoW networks, and all systems operated or administrated on behalf of the DoW. Mission Owners must meet this requirement for all control systems/OT. The intent is to pursue more specific STIGs for particular control system/OT products following publication of this SRG.

1.5 Document Revisions, Comments, Availability Update Cycle

Under normal circumstances, DISA develops, revises, updates, and publishes SRG and STIG documents on a quarterly maintenance release schedule, as needed. These publications reflect new or changed policies, requirements, threats, or mitigations; reorganized content; corrected errors; and provide additional clarity. Per DoWI 8500.01, DISA performs this role on behalf of DoW under the authority, direction, and control of the DoW CIO.

However, as a matter of exception, this document has been developed by the RMF TAG

Secretariat and not DISA. In keeping with the spirit of the DoWI 8500.01, the RMF TAG Secretariat has developed this document on behalf of DoW under the authority, direction, and control of the DoW CIO.

For this document, the RMF TAG Secretariat coordinates all change requests with relevant DoW organizations before including the change. The RMF TAG Secretariat publishes these changes in a normal publication timeline as previously described. Interested parties can obtain current versions of this document from the DoW Cyber Exchange website. Comments, proposed revisions, and questions for this document, alone, are accepted at any time via email at

osd.pentagon.dod-cio.mbx.rmfm-tag-secretariat@mail.mil. Regarding all other SRG and STIG material published on the Cyber Exchange website DISA remains the primary point of contact.

Whether there is a major version update or minor release update, the requirements in this document become effective immediately upon final publication. However:

- Any new control system/OT assessment, starting after the release of the Control Systems/OT SRG update, will be assessed against the updated requirements.
- Control systems/OT currently in the process of being assessed against the requirements in the previous Control Systems/OT SRG will continue this track but must transition to compliance with the current Control Systems/OT SRG update in coordination with their next DoW annual assessment.
- Control systems/OT currently in continuous monitoring under the previous Control Systems/OT SRG will provide a Plan of Action and Milestones (POA&M) within 30 days for becoming compliant with the current Control Systems/OT SRG requirements as soon as possible, but no later than, their next DoW annual assessment if scheduled six months after the Control Systems/OT SRG update is released, not to exceed one year. i.e., transition is to occur as soon as practicable but no longer than between six months and one year.

The CSF Profiles will be monitored for usefulness, with any gaps identified and recorded. Over time, updates to the Profiles may be adopted based on the information gathered as the Profiles are used and incorporated into the DoW control systems/OT processes and risk management activities.

1.6 Business Mission Objectives for Control Systems/OT

The following Business/Mission Objectives enable DoW to broadly express the business goals and targeted outcomes of DoW organizations utilizing control system/OT environments. These Business/Mission Objectives are a combination of organizational and security goals and are used directly in the development of the CSF Profile tailored to DoW control systems/OT, which appears in Section 2.2 of this DoW SRG. Business/Mission Objectives do not replace any DoW security objectives, nor do they infringe on RMF processes; rather, they articulate high-level business and mission goals that inform the organization's prioritization of cybersecurity activities.

Control systems/OT often require different aspects of confidentiality, integrity, and availability to be prioritized. In a traditional IT system, confidentiality of information may be the most important tenet; however, availability and integrity are more important for control systems/OT. Additionally, operational safety to both personnel and the environment are of great importance to organizations operating control systems/OT given the degree to which control systems/OT

interact with the physical world. As such, the DoW developed the following Business/Mission Objectives for organizations operating control systems/OT:

Maintain System Availability

Description: Preserving the ability to operate the system at the intended level within the desired time frame. Systems function without interruption.

Organizations Should:

- Identify interdependent control systems/OT that pose cybersecurity risks that threaten system availability.
- Initiate risk management procedures related to control system/OT engineering lifecycle and change management procedures.
- Manage vulnerability and risk by applying patches where feasible on systems in a timely manner regardless of service age, proprietary nature, or perceived obsolescence. Patches should address functionality and stability issues within the original code while also enhancing security. Plan for backups and work arounds.
- Deploy continuous monitoring applications to control systems/OT to detect threats to system availability while ensuring system health.
- Engage in business continuity planning to mitigate the risks of maintaining or reestablishing production in the case of an interruption. Specify recovery objectives (Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs)) for the various systems and subsystems involved based on typical business needs.
- Implement redundancy for critical processes and assets.

Maintain System Integrity

Description: Ensuring the ability to execute the correct instructions using the correct data at the correct time to preserve the ability to operate the system in the intended way.

Organizations Should:

- Identify interdependent control systems/OT that pose cybersecurity risks that threaten system integrity.
- Incorporate outcomes of Cybersecurity risk assessments that require an analysis of potential exploitation of vulnerabilities by a malicious actor.
- Incorporate outcomes of Cybersecurity risk assessments that account for adverse impacts on system data that may be the byproduct of system operations.

- Perform data hygiene processes to mitigate risks from duplicative, outdated, incorrect and unused data. Plan for backups and work arounds.
- Incorporate integrity checking mechanisms into operations to verify software, firmware, and information integrity.
- Apply Continuous Monitoring to ensure that data in use, in transit, and at rest is accounted for and checked for deliberate or accidental unauthorized manipulation.
- Mitigate business continuity risk by specifying Recovery Point Objectives (RPO) and backups of system configuration data.

Maintain Human Safety

Description: Recognizing cybersecurity effects on control systems/OT that impact personnel safety. Preventing injury, including loss of life, through Risk Assessment, Awareness and Training, Protective Technology, and Response Planning.

Organizations Should:

- Have a comprehensive process to systematically predict or identify the operational behavior of each safety-critical failure condition, fault condition, or human error that could lead to a hazard and potential human harm.
- Identify and train personnel on interdependence of cybersecurity with operational responsibilities that impact human safety.
- Implement vulnerability management incident responses measures where cybersecurity adversely affects human safety, in the event of a catastrophic failure/incident.

Maintain Environmental Safety

Description: Recognizing cybersecurity effects on control systems/OT that impact environmental safety. Preventing harm to the environment through Governance, Risk Assessment, Awareness and Training, and Response Planning.

Organizations Should:

- Have a comprehensive process to systematically predict or identify the operational behavior of each safety-critical failure condition, fault condition, or human error that could lead to a hazard and potential environmental harm.
- Identify and train personnel on interdependence of cybersecurity with operational responsibilities that impact environmental safety.

- Implement detect, respond, recover measures where cybersecurity adversely affects environmental safety, in the event of a catastrophic failure/incident.

Maintain Physical Security

Description: Recognizing and securing physical controls that impact control systems/OT. Preventing unauthorized access to a control system/OT environment and preventing damage or tampering with physical assets directly related to the control system/OT environment.

Organizations Should:

- Identify physical assets and security controls that directly relate to maintaining continuity of operations of the control system.
- Identify the cybersecurity risks associated with physical assets that could threaten control system/OT functionality.
- Incorporate outcomes of Cybersecurity risk assessments that require an analysis of potential exploitation of vulnerabilities by a malicious actor.
- Incorporate outcomes of Cybersecurity risk assessments that account for adverse impacts on system functionality that may be the byproduct of system operations.
- Reduce the risk of accidental or deliberate loss or damage to plant assets surrounding the control system/OT environment.
- Apply Continuous Monitoring to physical assets associated with the control system/OT security to ensure that there is no deliberate or accidental unauthorized manipulation or tampering of the physical environment.
- Ensure that physical security personnel understand the relative risks and physical security countermeasures associated with the control system/OT environments they protect.
- Ensure that physical security personnel are aware of which areas of a control system/OT production environment house data acquisition and operate in sensitive spaces.
- Mitigate business continuity risk by specifying immediate response plans in the event that physical safety is jeopardized.

1.7 System Security Objectives for Control Systems/OT

As discussed, traditionally, security objectives consider the potential impact on confidentiality, integrity, and availability of a system should it be compromised.

In accordance with 44 U.S.C., Sec. 3542 and according to Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, confidentiality is “preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information...”

A loss of confidentiality is the unauthorized disclosure of information. FIPS Publication 199 defines integrity as “Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity...”

A loss of integrity is the unauthorized modification or destruction of information. It is important to note that the unauthorized destruction of information will result in the loss of availability of that information...

A loss of availability is the disruption of access to or use of information or an information system. FIPS 199 defines availability as “Ensuring timely and reliable access to and use of information...”

However, many control system/OT processes are continuous in nature. Unexpected outages of systems that control industrial processes are not acceptable. Outages often must be planned and scheduled days or weeks in advance. Also, exhaustive pre-deployment testing is essential to ensure high reliability for the control system. As such, availability is often the primary security objective. Specific availability requirements must be included in the contract or a service level agreement between cooperating parties.

1.8 Control System/OT Security Architecture

The reference architecture below (Figure 2) is the 5-level Control System/OT Architecture, used in UFC 4-010-06, *Cybersecurity of Facility-Related Control Systems*. This architecture is defined as a general architecture suitable for a wide range of control systems/OT. For many Departments control systems/OT the 5L- Control systems/OT reference architecture is a key tool for understanding the layering aspect of control system/OT security architecture and IP/non-IP delineation; however, this architecture may not be a useful representation for all control system/OT environments. Given the diversity of control systems/OT in their complexity and capabilities, this architecture will not apply to all DoW control systems/OT. Rather, the architecture can be used to understand key security architecture concepts that may benefit system owners when securing their control system/OT environments.

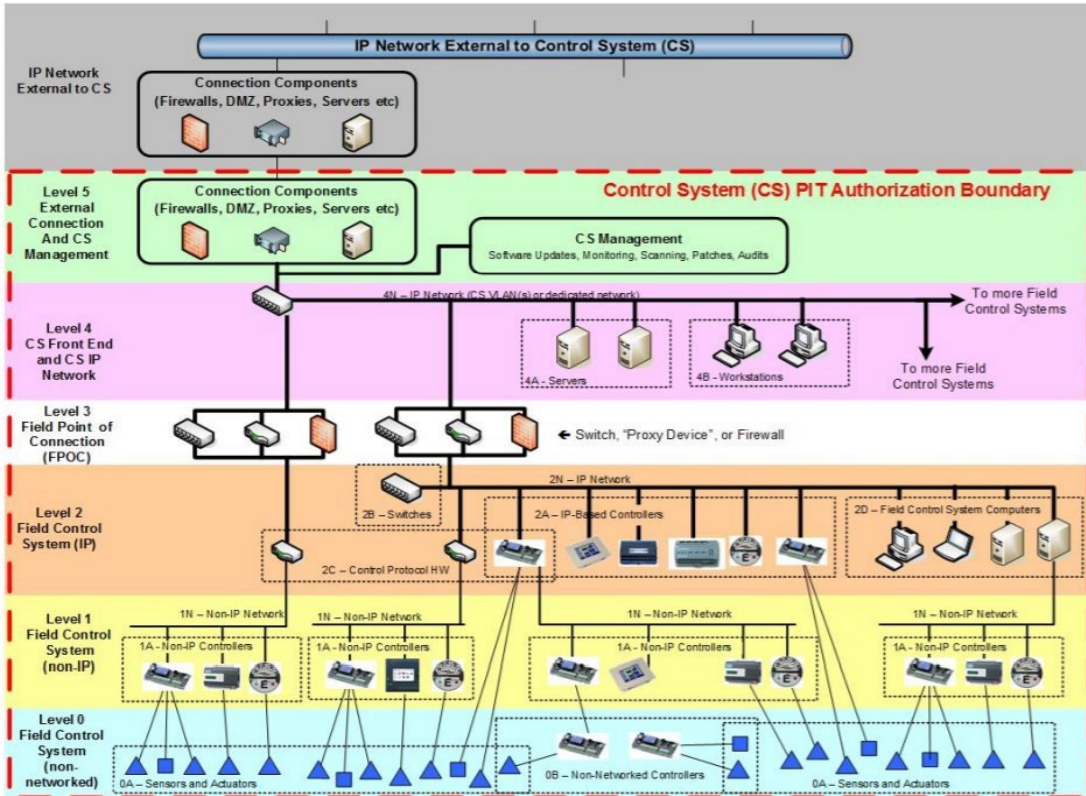


Figure 2: UFC-4-101-06 (5-Level Control System/OT Architecture)

In designing and implementing secure control system/OT security architectures, DoW organizations must use a “Defense in Depth” approach to protecting all assets, while taking into consideration the interconnections and dependencies of a system along with an organization’s available resources to provide effective layers of monitoring and protection based on the business’ exposure to cybersecurity risks.

DoW organizations must understand the relationship of threats and vulnerabilities to the controls and countermeasures put in place to protect the operations, personnel, and technologies that make up the control system/OT environment. Control systems/OT differ from traditional IT in their common attack vectors and the security needs to avoid exploitation. A list of common control system/OT exploits is listed below:

- Backdoors and holes in network perimeter
- Vulnerabilities on common and insecure protocols
- Attacks on field devices
- Database attacks
- Communications hijacking MITM attacks

- Spoofing attacks
- Attacks on privileged/shared accounts

The term control system/OT encompasses a multitude of systems with varying degrees of complexity, connectivity, and security needs. Control systems/OT are utilized across business mission functions ranging from weapons systems to medical and facilities purposes. While control systems/OT operate across a broad spectrum of environments, the following design principles should be incorporated where applicable across all control system/OT environments to implement secure architectures:

Network Segmentation and Segregation: Partitioning the network into smaller networks (logically, physically, etc.). For any network connected control system, partitioning the network based on management authority, level of trust, functional criticality, and data/communication flow is one of the most effective architectural concepts an organization can implement to protect the control system. Segmentation establishes security domains, which allows for emphasis on protection to various control system/OT components that are more sensitive than others. Overall, the purpose of network segmentation and segregation is to minimize access to sensitive information by unauthorized parties while ensuring effective system operation.

Boundary Protection: Controls the flow of information between interconnected security domains to protect the control system/OT environment against malicious users or human error. Separating system components with boundary protection mechanisms provides the capability for increased protection to individual system components and a more effective control of information between components. Boundary protection controls include gateways, routers, firewalls, guards, virtualization systems, intrusion detection systems, encrypted tunnels, managed interfaces, unidirectional gateways, and other controls designed to limit and control communication between interconnected control systems/OT.

Firewalls: Control the flow of network traffic between networks employing differing security postures. This is critical for any control system/OT environment where data flows to and from a control system/OT and amongst systems with differing security needs. Firewalls can restrict control system/OT communications between functional security subnets and devices where applicable. As such, organizations can prevent unauthorized access to systems and resources that are more sensitive.

Logically Separated Control Network: At minimum, a control system/OT must be logically separated from the corporate network (e.g., a separate VLAN) and it must be connected to a separate physical network device (e.g., gateway). A control system/OT environment may operate in an air gapped configuration where its security controls differ greatly from a traditional IT network. Therefore, it is critical for the control system/OT network to be entirely separated from the corporate network. If communication between the control system/OT network and

corporate network are necessary, additional security measures (e.g., an intermediate DMZ network) should be put in place.

At minimum, implementing the above architectural principles when designing a control system/OT environment is critical in creating a secure control system/OT architecture.

1.9 Cybersecurity Governance for Control Systems/OT

In the context of this SRG, a DoW organization's mission refers to the functions that organizations aim to accomplish via the use of control systems/OT. This may be the direct use of a control system/OT as the critical system for performing an enabled business mission, or the use of a control system/OT as a component of a larger system supporting the mission.

The Information Security Risk Management Committee (ISRMC) is a DoW entity that performs the DoW Risk Executive Function. The panel provides strategic guidance to Tiers 2 (Mission/Business Processes) and 3 (Systems) of the DoW RMF and assesses Tier 1 (Organizational) risk. The ISRMC also authorizes information exchanges and connections for enterprise information systems, cross security domain connections, and mission partner connections.

The Defense Security/Cybersecurity Authorization Working Group (DSAWG) works in support of the DoW ISRMC. DSAWG serves as the community forum for reviewing and resolving authorization issues related to the sharing of community risk. The DSAWG develops and provides guidance to Authorizing Officials (AOs) for system connections to the DoW Information Enterprise.

1.10 System Authorization of Control Systems/OT

Systems must have Authorization to Operate (ATOs), and ATOs are based on the boundary of the system. Consider this control system/OT exemplar:

1. Control System/OT (at Boundary)
 - a. In this case all internal connections and field control systems/OT are system components within the control system/OT Authorization Boundary requiring an ATO
2. Control System/OT Components (of a Larger System Boundary)
 - a. In this case the control systems/OT components may leverage the Assess Only approach
(Reference:
<https://cybersecurityks.osd.mil/dodcs/RMFImplementation/AssessOnly/Pages/AssessOnlyOverview.aspx>)

As with any system, control system/OT ATO decisions are expressed as an ATO, an ATO with conditions, an interim authorization to test (IATT), or a denial of ATO (DATO). Mission risk will continue to be assessed and authorized by the Mission Owner's AO through the issuance of an ATO. The Mission Owner's system must be issued an ATO by their Component's AO or other component authorized subordinate AO directly responsible for risk acceptance for the Mission Owner's system. This is applicable at all system criticality levels.

Organizations, System Owners, and Authorizing Officials should consider the system boundary and how systems will be employed. Control systems/OT often have identical instantiations across multiple sites. Type authorization is a form of reciprocity that is used to authorize multiple identical instances of a major application or general support system for operation at approved locations with the same type of computing environment. To protect its facilities and infrastructure, DoW needs to know the type, quantity and purpose of control system/OT it owns and uses. Type authorization for DoW control systems/OT signifies that the Mission Owner has acknowledged, mitigated, and accepted any risk associated with a system's implementation based on an evaluation of the system in a DoW environment. The system is then authorized for operation after ensuring that the system only poses acceptable risk to the organization's mission, business continuity, agency assets and individuals working with the control system. (Reference: <https://cybersecurityks.osd.mil/dodcs/PolicyandGovernance/Reciprocity/Pages/TypeAuthorization.aspx>)

The benefit of leveraging reciprocal use of an authorized control system/OT is that much of the security controls assessment work is already accomplished. Mission Owners and their AOs must still review RMF cybersecurity, mission assurance and related DoW artifacts to understand the risks that the mission will inherit when using the selected control system/OT for the mission system. Mission owners must also consider the prioritization of mission objectives to determine which are most relevant to guide their cybersecurity activities. Mission owners may need to implement compensating controls for any risk deemed unacceptable prior to obtaining an ATO. Additional compensating controls must be reflected in the documentation of the deploying and receiving organizations.

1.11 Cyberspace Defense and Incident Response in the Control System/OT Environment

Cyberspace Defense addresses the defense and protection of networks and systems, detection of threats, and response to incidents. Cyber situational awareness improves the quality and timeliness of collaborative decision-making regarding the employment, protection, and defense of DoW systems and data. DoW cyberspace defense actions provide the means to react to threats and incidents to defend the DoW Information Network (DOWIN). This section addresses critical cyberspace defense actions; roles and responsibilities; incident reporting and response; and other cybersecurity processes relevant to control systems/OT.

DoW operates a cybersecurity structure as defined in DoWI 8530.01, “Cybersecurity Activities Support to DoW Information Network Operations”. The structure establishes United States Cyber Command (USCYBERCOM) and DoW Cyber Defense Command, which was previously known as Joint Forces Headquarters DoDIN (JFHQ-DoDIN)) with directive oversight of a network of Cybersecurity Service Providers (CSSPs), accredited by USCYBERCOM, IAW DoW policy. Each DoW system is operated/managed by a Mission Owner which must be aligned with an accredited CSSP which monitors and protects the information, systems, and associated assets. The Mission Owner is responsible for the implementation and maintenance of the security posture of their system(s) in accordance with SRGs/STIGs, and DoW policy in coordination with, and/or with the assistance of their aligned CSSP. CSSPs report information to USCYBERCOM which maintains Cyber situational awareness over all DoW networks and systems. USCYBERCOM also provides threat information collected from various sources and threat mitigation orders to the CSSPs and Mission Owners.

* An example of maintaining the security posture of a Mission Owner’s system is the application of patches/upgrades and Information Assurance Vulnerability Management (IAVM) compliance. This is a Mission Owner-level activity or responsibility. While some DoW Components relieve their Mission Owners of some, or all, security posture maintenance activities by transferring their performance to the system’s CSSP, they remain Mission Owner-level activities and responsibilities. As such, the CSSP is responsible for performing the transferred Mission Owner level functions along with their CSSP-level functions.

2 Cybersecurity Framework (CSF) Control System/OT Profiles

This section includes strategy and implementation guidance for applying principles from the NIST Cybersecurity Framework, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* (the CSF). Per Executive Order 13800, all Agencies are now required to incorporate the CSF into their risk management processes.

The CSF does not replace any processes or procedures established in DoW RMF; rather, it is used in concert with the RMF to approach risk management from an organizational perspective. The CSF focuses on business drivers to guide cybersecurity activities. Essentially, the CSF assists an organization in aligning and prioritizing its cybersecurity activities with its business-mission requirements, risk tolerances, and resources. The RMF and CSF are complementary and essential pieces to implementing organizational cybersecurity and risk management. The RMF manages the lifecycle cybersecurity risk to DoW IT and the CSF aims to align business/mission objectives with cybersecurity activities.

Specifically, implementing CSF provides a mechanism for an organization to:

- Assess and describe its current and targeted cybersecurity posture.
- Identify gaps in its current programs and processes.
- Identify and prioritize opportunities for improvement using a continuous and repeatable process.
- Assess progress toward reaching its target security posture.
- Communicate cybersecurity posture in a common, recognized language to internal and external stakeholders.

The CSF *Core* (Identify, Protect, Detect, Respond, Recover) is a set of cybersecurity activities, outcomes, and informative references that can help DoW organizations to better organize the risks they have accepted and the risk they are working to remediate across all systems. The CSF Core enables shaping of these business and mission goals using the reporting structure that aligns to SP 800-53 and enables agencies to reconcile mission objectives with the structure of the Core and RMF. The methodology used in this SRG incorporates the NIST CSF profiles which, like RMF, is used to formulate a methodized approach to reducing cybersecurity risk for control systems/OT. However, the CSF provides an opportunity to provide a link between cybersecurity activities and DoW organizational mission/businesses objectives. When used in support of the RMF process, the CSF profiles help to maintain a comprehensive understanding of cybersecurity risk, report cyber security risks, and to inform the tailoring process.

The CSF *Profiles* support a better-organized RMF process by helping mission owners understand their accepted risks, and the risks they are working to remediate, across all systems (at the organization-level). In combination, the CSF Profiles enables DoW organizations to reconcile mission objectives with accepted risks and implemented controls resulting from the RMF process.

The following sections illustrate how an organization can use the CSF methodology to develop a CSF Profile for control system/OT environments.

As discussed, the CSF Core consists of five concurrent and continuous functions. These functions encompass the full spectrum of cybersecurity activities and provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk. The CSF Core then identifies underlying key Categories and Subcategories for each Function, and matches them with informative references, guidelines, and practices. These Functions, summarized below, are incorporated into the risk management process to improve organizational security and resilience.

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.

Protect – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event.

Detect – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events.

Respond – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident.

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 Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident.

2.1 CSF Profile Purpose and Scope

Sections 2.2 and 2.3 of the CS SRG provides a methodology for applying the CSF to DoW control systems/OT. Section 2.2 CSF Profile Priority Matrix examines the policies, procedures, and technical solutions required to meet the language specified in each Category and Subcategory and lists potential solutions that fulfil the requirements, given the criticality of the control system/OT of interest (LOW, MODERATE, or HIGH). The priority levels associated with each subcategory were derived as an example of how an organization can set prioritize cybersecurity activities to ensure Mission Objectives are achieved and maintained. The Profile Priority Matrix supports system owners in areas an organization may add or remove resources specifically for their business environment and leverage the matrix to assist organizations in the development of POA&Ms to maintain a robust cybersecurity posture.

The matrix overview provides five different areas as outlined below to provide familiarity and content in the areas of Function, Category, Criticality, Subcategory, and Mission Objectives and identified impact levels under each mission objective:

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low Priority / Other Implemented Subcategories					
				Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security	
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	<ul style="list-style-type: none"> ● Low: Have awareness of physical devices, software platforms, external information systems, and data flows in priority of business purpose. Establish an organizational structure that assigns cybersecurity roles and responsibilities and trains personnel. ●● Moderate: Employ data flow mapping techniques, Enterprise Resource Planning software. Evaluate personnel that have cybersecurity roles and responsibilities. Identify individuals who are both responsible and accountable for administering control systems/OT. 	ID.AM-1: Physical devices and systems within the organization are inventoried	●●●	●●●	●●	●●	●●●	DoWI 8530.01, DoWI 8320.03, DoWI 5000.64
			ID.AM-2: Software platforms and applications within the organization are inventoried	●●●	●●●	●	●	●	DoWI 8530.01
			ID.AM-3: Organizational communication and data flows are mapped	●●●	●●●	●●●	●	●	DoWI 8530.01
			ID.AM-4: External information systems are catalogued	●●●	●●●	●	●	●●●	DoWI 5000,64

The Profile Categories subdivides the aforementioned Functions into groups of particular cybersecurity activities or programmatic needs. The Subcategories divide the Categories further into specific outcomes of technical and management activities, expressed as results. The Subcategories were also cross-referenced with each DoW Mission Objective mentioned earlier in the document. Each Subcategory was given a prioritization value based on how relevant it was to each respective Mission Objective.

For example, in the Protect (PR) Function of the table at *PR.AC-1: Identities and credentials are managed for authorized devices and users*, the Subcategory was given HIGH priority for Maintaining System Integrity whereas it was given a LOW priority for Maintaining Environmental Safety.

Section 2.3 represents the Cybersecurity Framework High Priority Rationales table demonstrates how an organization can take “**High Priority Subcategories**” from Section 2.2 and further “**Rationalize**” why a particular Subcategory is applicable to one of the given DoW Mission Objectives as annotated in the table providing more clarity into prioritizing the appropriate cybersecurity activities ensuring business continuity and mission success.

2.2 CSF Profile Priority Matrix

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low Priority / Other Implemented Subcategories					
				Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security	
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	<ul style="list-style-type: none"> ● Low: Have awareness of physical devices, software platforms, external information systems, and data flows in priority of business purpose. Establish an organizational structure that assigns cybersecurity roles and responsibilities and trains personnel. ●● Moderate: Employ data flow mapping techniques, Enterprise Resource Planning software. Evaluate personnel that have cybersecurity roles and responsibilities. Identify individuals who 	ID.AM-1: Physical devices and systems within the organization are inventoried	●●●	●●●	●●	●●	●●●	DoWI 8530.01, DoWI 8320.03, DoWI 5000.64
			ID.AM-2: Software platforms and applications within the organization are inventoried	●●●	●●●	●	●	●	DoWI 8530.01
			ID.AM-3: Organizational communication and data flows are mapped	●●●	●●●	●●●	●	●	DoWI 8530.01

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
		are both responsible and accountable for administering control systems/OT. ●●● High: Employ automated mechanisms where safe and feasible to detect unauthorized uses of physical devices, software platforms, external information systems, and data flows that serve a necessary and sufficient business purpose.	ID.AM-4: External information systems are catalogued	●●●	●●●	●	●	●●●	DoWI 5000.64
			ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	●●●	●●●	●●●	●●●	●●●	DoWI 8530.01
			ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	●●	●●	●	●	●●	DoWD 8140.01

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
	<p>Business Environment (ID.BE): The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.</p>	<p>● Low: Understand the organization’s role in mission assurance, supply chain, and critical infrastructure sectors. Prioritize organizational missions, objectives and activities. Establish and communicate priorities for DoW control system/OT missions, objectives, and activities with consideration for security. Have awareness of critical business functions and their dependencies.</p> <p>●● Moderate: Understand typical failures that occur to control systems/OT and dependencies. Establish recovery metrics to inform reliance efforts by specifying recovery objectives (Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs)) for the control system/OT environment and component control</p>	<p>ID.BE-1: The organization’s role in the supply chain is identified and communicated</p>	●●	●●	●	●	●	DoWI 5200.44
			<p>ID.BE-2: The organization’s place in critical infrastructure and its industry sector is identified and communicated</p>	●●●	●●	●	●●	●●	DoWI 3020.45

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
		<p>systems/OT involved based on typical business needs.</p> <p>Identify critical control system components and functions by performing a criticality analysis.</p> <p>●●● High: Protect against threats to the control system/OT environment by employing security safeguards as part of a comprehensive, defense-in-depth security strategy. Conduct contingency planning for the continuance of essential control system/OT functions and services with little or no loss of operational continuity that sustains until full system restoration.</p>	<p>ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated</p>	●●	●●	●●●	●●	●●	<p>Prioritized at the Component or organization level</p>
			<p>ID.BE-4: Dependencies and critical functions for delivery of critical services are established</p>	●●●	●●●	●	●	●●	<p>DoWI 8530.01, DoWI 8500.01, DoW O-8530.01-M</p>

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	<ul style="list-style-type: none"> ● Low: Apply DoW-level and Component cybersecurity policy and local risk governance processes. Address risk from a system perspective that is guided by risk decisions at Tiers 1 and 2 in accordance with DOWI 8500.01. Assure the policy is approved by necessary entities or senior officials with responsibility and accountability for the risk incurred by control system/OT operations. ●● Moderate: Apply mission owner and business mission community risk governance processes. Address risk from a mission and business process perspective that is guided by risk decisions at Tier one and is informed and influenced by risk decisions made in Tier 3 in 	ID.GV-1: Organizational information security policy is established	●●●	●●●	●	●	●●	DoWI 8500.01
			ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	●●	●●	●	●	●●	DoWI 8500.01
			ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	●●	●●	●●	●	●●	DoWI 5144.02

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
		accordance with DOWI 8500.01. ●●● High: Address risk from an organizational perspective that is informed and influenced by risk decisions made in Tiers 2 and 3, in accordance with DOWI 8500.01.	ID.GV-4: Governance and risk management processes address cybersecurity risks	●●●	●●●	●	●	●●●	DoWI 8510.01
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals	● Low , ●● Moderate , ●●● High: Establish and maintain ongoing contact with DoW and USG cybersecurity communities and receive security alerts and advisories. Organizations should consider having both an unclassified and classified information sharing capability. Conduct criticality reviews of control systems/OT informed by their impact to operations, assets, and individuals. Establish risk	ID.RA-1: Asset vulnerabilities are identified and documented	●●	●●	●●	●●	●●	DoWI 3020.01, DoWI 8510.01
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	●●	●●	●●	●●	●●	DoWI 8500.01, DoWI 8530.01	
		ID.RA-3: Threats, both internal and external, are identified and documented	●●●	●●●	●●●	●●●	●●●	DoWI 8500.01, DoWI 8530.01	

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
		tolerances to mitigate with a comprehensive strategy that prioritizes risk responses. Employ automated mechanisms, where technically feasible, to make security alert and advisory information available and prioritized throughout the organization.	ID.RA-4: Potential business impacts and likelihoods are identified	●●●	●●	●	●	●●	DoWI 8500.01, DoWI 8510.01
			ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	●●●	●●●	●●●	●●●	●●●	DoWI 8500.01, DoWI 8510.01
			ID.RA-6: Risk responses are identified and prioritized	●●●	●●●	●●●	●●●	●●●	DoWI 8500.01, DoWI 8510.01

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	●Low, ●● Moderate, ●●●High: Establish and maintain ongoing contact with DoW and USG cybersecurity communities and receive security alerts and advisories. Organizations should consider having both an unclassified and classified information sharing capability. Conduct criticality reviews of control systems/OT informed by their impact to operations, assets, and individuals. Establish risk tolerances to mitigate with a comprehensive strategy that prioritizes risk responses. Employ automated mechanisms, where technically feasible, to make security alert and advisory information available and prioritized throughout the organization.	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	●●	●●	●●	●	●●	DoWI 8500.01, DoWI 8510.01
			ID.RM-2: Organizational risk tolerance is determined and clearly expressed	●●	●●	●●	●●	●●	DoWI 8500.01, DoWI 8510.01
			ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	●●	●●	●	●	●●	DoWI 8500.01, DoWI 8510.01

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
PROTECT (PR)	<p>Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions</p>	<p>● Low: Establish and manage identification mechanisms and credentials for users of assets and facilities of control systems/OT. Define and manage access permissions for users of the control systems/OT including emergency situations. Protect physical access to control system/OT assets or facilities. Maintain and review visitor access records to control system/OT related facilities.</p> <p>Establish usage restrictions, connection requirements,</p>	<p>PR.AC-1: Identities and credentials are managed for authorized devices and users</p>	●●	●●●	●	●	●●●	<p>DoWI 8520.03, DoWI 8500.01 DoWD 8521.01</p>

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
		implementation guidance, and authorizations for remote access to control systems/OT. Use secure protocols for any remote access activity where feasible. Protect network integrity of the control system/OT and incorporate network segmentation where appropriate.	PR.AC-2: Physical access to assets is managed and protected	●●●	●●●	●●●	●●●	●●●	DoWI 8520.03, DoWD 8521.01, DoWI 8500.01

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
		<p>●● Moderate: Deactivate system credentials after a specified period of inactivity. Employ automated mechanisms where feasible to support the management and auditing of authorized credentials (e.g., automating password expiration). Only allow remote access through approved and managed devices or access points while employing</p>	<p>PR.AC-3: Remote access is managed</p>	●●●	●●●	●	●	●●	<p>JIE Enterprise Remote Access STIG,v1 and Release Memo, DoWI 8500.01, DoWD 8521.01</p>

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
		multifactor authentication for authorized personnel where feasible. Limit and monitor connections to the control system/OT while allowing only connections necessary to system functionality and only allowing connections to approved management interfaces (HMI). Audit the execution of privileged functions on the control system/OT environment.	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	●●●	●●●	●	●	●●●	DoWI 8520.03, DoWI 8500.01, DoWD 8521.01
		●●● High: Monitor control systems/OT for atypical use of credentials. Enforce account usage rules to specific time periods where feasible (e.g., certain days of the week, time of day, or specific durations of time). Employ strict access controls to control	PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	●●●	●●●	●	●	●●	DoWI 8520.03, DoWI 8500.01, DoWD 8521.01

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
		systems/OT to enhance the physical protection of the control system/OT facility. Maintain logs of all remote access activity and only allow the use of privileged functions for control systems/OT via authorized remote access. Protect all components of a DoW control system/OT from accidental damage, disruption, and physical tampering. Employ redundant and physically separated power supplies for control systems/OT essential to business operations. Airgap the control system/OT environment where feasible to limit external connections to only those both necessary for system functionality and beneficial to operational continuity	PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions						
			PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)						

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
	<p>Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.</p>	<p>● Low: Train all users on cybersecurity incorporating insider threat recognition and reporting. Enforce security requirements for third-party providers and users. Ensure that personnel responsible for security of, and privileged users with access to, control systems are trained and understand their responsibilities. Ensure that senior level leadership understands their requirements for the security and protection of the control system environment.</p> <p>●● Moderate: Require service providers to identify the functions, ports, protocols, and services necessary for connection services.</p> <p>●●● High: Perform personnel and service provider testing and exercises.</p>	<p>PR.AT-1: All users are informed and trained</p>	●●●	●●●	●●●	●●●	●●●	DoWI 8500.01
			<p>PR.AT-2: Privileged users understand roles & responsibilities</p>	●●	●●	●●	●●	●●	DoWI 8500.01, DoW 8570.01-M, DoWD 8140.01
			<p>PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities</p>	●●	●●	●●	●●	●●	DoWD 8570.01-M
			<p>PR.AT-4: Senior executives understand roles & responsibilities</p>	●●	●●	●●	●●	●●	DoWD 8140.01, DoW 8570.01-M
			<p>PR.AT-5: Physical and information security personnel understand roles & responsibilities</p>	●●●	●●	●●	●●	●●●	DoWD 8140.01, DoW 8570.01-M

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				••• = High Priority, •• = Moderate Priority, • = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	<ul style="list-style-type: none"> • Low: Enforce accountability for all control system/OT components throughout the system lifecycle, including removal, transfers, and disposal. Protect any information at rest critical to business operations. Ensure the control system/OT environment has adequate resources available to accommodate business functionality (e.g., information processing, networking, and data storage if necessary). Protect the control system/OT from data leakage by developing and 	PR.DS-1: Data-at-rest is protected	•	•••	•	•	•	DoWD 8100.02, DoWI 8420.01
			PR.DS-2: Data-in-transit is protected	••	•••	•	•	•	DoWD 8100.02, DoWI 8420.01

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
		documenting access agreements for all users of control systems/OT. When implementing any major change to a control system/OT configuration in an off-line setting where the changes are tested prior to integration into the control system/ OT environment.	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	●●	●●●	●	●	●●	DoWI 8500.01
		●● Moderate: Protect control systems/OT data when in transit. Implement cryptographic mechanisms where determined necessary to prevent unauthorized access, distortion, or modification of system data and audit records. Update the inventory of control	PR.DS-4: Adequate capacity to ensure availability is maintained	●●●	●	●	●	●●	DoWI 8500.01

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
		system/OT components as an integral part of the component installations, removals, and system updates. Ensure availability is maintained by protecting the control system/OT against denial of service (DoS) attacks.	PR.DS-5: Protections against data leaks are implemented	●	●●	●	●	●●	DoWI 8500.01
		Enforce controls restricting connections to only authorized interfaces, where feasible. Utilize an off-line development and testing system for implementing and testing changes to the control system/OT environment.	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	●●	●●●	●	●	●	DoWI 8500.01
		●●● High: Employ automated tools, where feasible, to provide notification upon							

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
		discovering discrepancies during integrity verification. Employ automated response capability with pre-defined security safeguards when integrity violations are discovered.	PR.DS-7: The development and testing environment(s) are separate from the production environment	●●●	●●●	●●	●●	●●	DODI 5000.02
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage	● Low: Develop, document, and maintain a baseline configuration for control systems/OT. Manage control systems /OT using a system development life cycle provided by guidance from the control system/OT vendor that includes security considerations (PR.IP-2). Employ configuration change control and security impact analyses for control systems/OT and its components. Conduct and maintain backups for	PR.IP-1: A baseline configuration of information technology/industrial control systems/OT is created and maintained	●●●	●●●	●	●	●	DoW 8310.01

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
	protection of information systems and assets.	<p>control system/OT data. Ensure safe handling of system data including the destruction of data according to policy (PR.IP3).</p> <p>Require the developer of the control system/OT and system components to provide a description of the functional properties of security controls well as design and implementation information for security-relevant system interfaces. Apply security engineering principles into the specification, design, development, implementation, and modification of control systems/OT.</p> <p>Employ configuration management and change control during the development of the control system/OT environment and its components the</p>	<p>PR.IP-2: A System Development Life Cycle to manage systems is implemented</p>	●●	●●	●	●	●●	DoWI 8580.01, DoWI 5000.02, DoWI 5200.44
			<p>PR.IP-3: Configuration change control processes are in place</p>	●●●	●●●	●	●	●●●	DoWI 5200.44

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
		includes flaw tracking and resolution and security testing, where feasible (PR.IP-2).	<p>PR.IP-4: Backups of information are conducted, maintained, and tested periodically</p>	●●●	●●●	●	●	●	DoWI 3020.26
		Develop, maintain, and execute response and recovery plans that identify essential functions and associated contingency requirements, as well as provides a roadmap for implementing incident response. Plans should incorporate recovery objectives, restoration priorities, metrics, contingency roles, personnel assignments and contact information (PR.IP9). Review response and recovery plans to determine the effectiveness of, and the readiness to execute the plans (PR.IP-10).		<p>PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met</p>	●●●	●●	●●●	●●●	
Define, implement, and enforce policy and regulations regarding									

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
		emergency and safety systems, fire protection systems, and environment controls for control systems/OT. Fire suppression mechanisms should take the control system/OT environment into account (e.g., water sprinkler systems could be hazardous in specific environments) (PR.IP-5)	PR.IP-6: Data is destroyed according to policy	●●	●●	●	●	●	DoWI 8500.01
		Incorporate improvements derived from the monitoring, measurements, assessments, and lessons learned into protection process revisions. Ensure that the security plan for the control system/OT environment facilitates reviewing, testing, and the continual improvement of the security protection processes (PR.IP-7). Develop and maintain a personnel security program	PR.IP-7: Protection processes are continuously improved	●●	●●	●●	●●	●●	DoWI 8500.01

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
		for control system/OT environments (PR.IP-11). Establish and maintain a process that continuously reviews vulnerabilities and their exposure to adversaries, and defines strategies to mitigate them (PR.IP-12). ●● Moderate: Review and update the baseline configurations of the control systems/OT as an integral part of system	PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	●	●	●	●	●	DoWI 8500.01

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
		<p>component installations and upgrades Retain previous versions of the baseline configurations to allow for rollback. Develop configuration management plans for control system/OT environments to include, for example, configuration processes, roles, lifecycle definition, configuration items, and control methods. Define configuration parameters, capabilities, and fail-to-known state procedures ensuring a system fails to a predetermined state of operation. Employ a deny-all, permit-by-exception policy to allow the execution of only authorized software programs (PR.IP-1).</p> <p>Test, validate, and document changes to the control system/OT environment before</p>	<p>PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed</p>	●●●	●●●	●●●	●●●	●●●	●●●

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
		implementing the changes on the component control system. Review and authorize proposed configuration-controlled changes prior to implementing them on the control system/OT environment (PR.IP-3). Verify the reliability and integrity of backups. Establish a separate alternate storage site for system backups and ensure the same security safeguards are employed (PR.IP-4). Employ teams independent of operational responsibility to assess the protection process (PR.IP-7). Coordinate contingency and response and recovery plan development, testing and execution with stakeholders responsible for related plans (PR.IP-9).	PR.IP-10: Response and recovery plans are tested	●●	●●	●●	●●	●●	DoWI 8500.01

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
		<p>Personnel security programs should include policy, position risk designations, personnel screening, terminations and transfers, access agreements, third-party roles and responsibilities, and personnel sanctions (PR.IP-11). Restrict access to privileged vulnerability data (PR.IP-12).</p> <p>●●● High: Conduct security impact analysis in a separate test environment before implementation into an operational environment for planned changes to control systems/OT.</p> <p>Employ automated mechanisms where feasible to maintain an up-to-date, complete, accurate, and readily available baseline configuration of control systems/OT. Automated</p>	<p>PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)</p>	●●	●●	●●	●●	●●	<p>DoWI 8500.01, DoWD 8140, DoWI 5000.02 Encl. 13, DoW 8570.01-M</p>

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
		<p>system support includes for example, documentation, notification, and management of the change control process on control systems/OT (PR.IP-3).</p> <p>Review system changes to determine whether unauthorized changes have occurred (PR.IP-1). Include restorations from backup data into contingency plan testing (PR.IP-4).</p> <p>Ensure that data sanitization actions are approved, tracked, documented, and verified. Test sanitization equipment and procedures. Apply data sanitization techniques to portable storage devices connecting to the control system/OT environment, when feasible (PR.IP-6).</p>	<p>PR.IP-12: A vulnerability management plan is developed and implemented</p>	●●●	●●●	●●	●●	●●●	<p>DoWI 8500.01, DoWI 8530.02, DoW 8570.01-M</p>

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
	<p>Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.</p>	<p>● Low: Establish a process for maintenance personnel authorization and escort nonauthorized maintenance personnel. Verify impacted component security controls following maintenance or repairs. Enforce approval requirements, control, and monitoring, of remote maintenance activities. Employ strong authenticators, record keeping, and session termination for remote maintenance.</p> <p>●● Moderate: Schedule, perform, document and review records of maintenance and repairs to control system/OT components. Enforce approval requirements, control, and monitoring of maintenance tools for use on control systems/OT,</p>	<p>PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools</p>	●●	●●	●●●	●●●	●●●	DoWI 8500.01

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
		<p>where feasible. Maintenance tools can include, for example, hardware/software diagnostic test equipment, hardware/software packet sniffers and laptops. Perform preventative maintenance at defined intervals. Inspect maintenance tools brought into the facility. Scan maintenance tools and portable storage devices for malicious code before they are used on control systems/OT.</p> <p>●●● High: Employ automated mechanisms where feasible to schedule, conduct, and document maintenance and repairs; and to produce records of maintenance activity. Prevent the unauthorized removal of maintenance equipment containing control system/OT</p>	<p>PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access</p>	●●●	●●●	●●	●●	●●	DoDI 8500.01

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
		information. 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 control system/OT.							
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	<ul style="list-style-type: none"> ● Low: Audit and log records are determined and documented. Employ safeguards to restrict the use of portable storage devices. Limit external connections to control systems/OT. ●● Moderate: Audit logs are reviewed and updated after cybersecurity related 	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	●●●	●●●	●	●	●	DoWI 8500.01

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
		events. Disable defined functions, ports, protocols, and services within the control systems/OT 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.	PR.PT-2: Removable media is protected and its use restricted according to policy	●●	●●●	●	●	●●	DoWI 8540.01, Removable Storage and External Connections STIG, DoW 5200.01, v3
		Control the flow of information within control systems/OT and between interconnected systems. ●●● High: Integrate audit logs with physical access monitoring. Employ automated mechanisms to integrate audit review, analysis, and reporting. Scan all portable storage devices for malicious code before use on control systems/OT. Limit external connections to	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	●●●	●●	●●	●●	●●●	DoWI 8500.01

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
		the control system/OT to those necessary for critical functionality. 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.	PR.PT-4: Communications and control networks are protected	●●●	●●●	●●	●●	●●	DoWI 8550.01

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
DETECT (DE)	<p>Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.</p>	<p>● Low: Ensure that a baseline awareness of network operations and expected data flows for control systems/OT is developed and maintained to detect events. Review and analyze detected events within the control system/OT environment to understand attack targets and methods.</p> <p>Define incident alert thresholds for control systems/OT and determine negative impacts to DoW operations, assets, and</p>	<p>DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed</p>	●●●	●●	●	●	●	DoWI 8320.02, DoWI 8330.01, DoW 8530.01
			<p>DE.AE-2: Detected events are analyzed to understand attack targets and methods</p>	●●	●●	●●	●●	●●	DoWI 8530.01, DoWI S-5240.23, CJCSM 6510.01B

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
		individuals resulting from detected events. ●● Moderate: Ensure that event data is compiled and correlated across the control system/OT environment using various sources such as event reports, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	●●	●●	●●	●●	●●	DoWI 8530.01, CJCSM 6510.01B
		●●● High: Integrate analysis of events and vulnerability scanning information, performance data, control system/OT monitoring and other monitoring systems to enhance the ability to identify unusual activity.	DE.AE-4: Impact of events is determined	●●●	●●●	●●●	●●●	●●●	DoWI 8560.01, CJCSM 6510.01B, DoWI 8530.01

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
		Collate detected event information and responses to achieve perspective on event impact across the organization. Employ automated mechanisms to assist in the identification of security alert thresholds and to support impact analysis, where feasible.	DE.AE-5: Incident alert thresholds are established	●	●	●●	●●	●●	DoWI 8510.01, DoWI 8530.01
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	● Low: Where feasible, conduct ongoing security status monitoring of DoW control system/OT environment to detect defined cybersecurity events. Detect unauthorized local, network, and remote connections to the control system/OT environment	DE.CM-1: The network is monitored to detect potential cybersecurity events	●●●	●●●	●	●	●	DoWI 8560.01, DoWI 8530.01, DoWI 8551.01

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
		Employ proper personnel to monitor the security of the physical environment. Conduct ongoing security status monitoring of the control system/OT facility to detect physical security incidents. Monitor for unauthorized personnel, connections, devices, access points, and software. Monitor for and report atypical usage of the control system. Conduct ongoing security status monitoring of service provider activity on control systems/OT. Monitor compliance of external providers with personnel security policies and procedures, and contract security requirements. ●● Moderate: Generate audit records if defined security events occur and generate system alerts	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	●●●	●●●	●●	●●	●●●	DoW 5220.22-M, DoW 5200.08-R
			DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	●●●	●●●	●●●	●●	●●●	DoWI 8500.01
			DE.CM-4: Malicious code is detected	●●●	●●●	●	●	●	DoWI 8510.01, CJCSM 6510.01B, DoWI 8530.01

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
		when indications of compromise or potential compromise occur. Deploy monitoring devices strategically within the control system/OT environment to collect essential information. Employ control system/OT specific vulnerability scanning tools and techniques where safe and feasible.	DE.CM-5: Unauthorized mobile code is detected	●●	●●	●	●	●	DoWI 8510.01, DoWI 8530.01, CJCSM 6510.01B
		●●● High: Continually monitor for unauthorized configuration changes to control systems/OT. Define and detect acceptable and unacceptable mobile code and mobile code technologies. Automatically update malicious code protection mechanisms. Actively incorporate vulnerability scanning of	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	●●	●●●	●	●	●●	DoWI 8510.01
			DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	●●●	●●●	●●●	●●	●●●	DoWI 8530.01, DoWI 8530.03, DoWI 8500.01

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
		network traffic and of critical control systems/OT into the monitoring process to ensure that system functions are not adversely impacted by any threat actors.	DE.CM-8: Vulnerability scans are performed	●●●	●●●	●	●	●	DoWI 8510.01, DoWI 8530.01, DoWI 8500.01
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	● Low: Define the roles and responsibilities for detection activities on control systems/OT and ensure accountability. Conduct detection activities in accordance with applicable federal and state laws, industry regulations, standards,	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	●●	●●	●●	●●	●●	DoWI 8500.01, DoWI 8530.01, CJCSM 6510.01B

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
		<p>policies, and other applicable requirements.</p> <p>Communicate event detection information to defined personnel and ensure the security plans in place for control systems/OT provide for the review, testing, and continual improvement of security detection processes.</p> <p>●● Moderate: Employ proper personnel to assess the detection process and validate that event detection processes are operating as intended.</p>	<p>DE.DP-2: Detection activities comply with all applicable requirements</p>	●	●	●	●	●	DoWI 8530.01, CJCSM 6510.01B
			<p>DE.DP-3: Detection processes are tested</p>	●●	●●	●	●	●●	DoWI 8500.01

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
		<p>●●● High: Conduct specialized assessments including in-depth monitoring, vulnerability scanning safe for the control system/OT (where feasible), malicious user testing, insider threat assessment, and performance/load testing on the control system/OT environment.</p> <p>Employ automated mechanisms and system-generated alerts to support event detection communication, where feasible.</p>	<p>DE.DP-4: Event detection information is communicated to appropriate parties</p>	●●	●●	●●	●●	●●	<p>CJCSM 6510.01B, DTM 17-007, DoWI 5205.13, DoWI 8110.01, Presidential Policy Directive (PPD)-41, United States Cyber Incident Coordination</p>
			<p>DE.DP-5: Detection processes are continuously improved</p>	●●	●●	●●	●●	●●	<p>DoWI 8530.01</p>

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	●Low, ●●Moderate, ●●●High: Execute the response plan during or after a cybersecurity event in the control system/OT environment	RS.RP-1: Response plan is executed during or after an event	●●●	●●●	●●●	●●●	●●●	DoWI 8510.01
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	●Low: Ensure personnel understand objectives, restoration priorities, task sequences and assignment responsibilities for event response. Employ prompt reporting to appropriate stakeholders for cybersecurity events on a DoW control system. Ensure that these reporting procedures are consistent with the response plan and follow any and all DoW Cybersecurity incident handling polices.	RS.CO-1: Personnel know their roles and order of operations when a response is needed	●●	●●	●●●	●	●●	DoWD 8140.01, DoWI 8510.01
			RS.CO-2: Events are reported consistent with established criteria	●	●	●	●	●	DoWI 8510.01

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
		Share cybersecurity event information voluntarily, as appropriate, with DoW cybersecurity communities and USG partners to achieve broader cybersecurity situational awareness	RS.CO-3: Information is shared consistent with response plans	●●	●●	●●	●●	●●	DoWI 8110.01
		●● Moderate: Employ automated mechanisms to support communication amongst relevant stakeholders, where feasible. Ensure that reporting procedures follow any additional DoW Component or organizational requirements	RS.CO-4: Coordination with stakeholders occurs consistent with response plans	●●	●●	●	●	●	DoWI 8510.01
		●●● High: Employ automated mechanisms to assist in the reporting of cybersecurity events and support stakeholder coordination, where feasible	RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	●●	●●	●	●	●	DoWI 5205.13

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	<p>●Low: Understand the full implication of a 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.</p> <p>Categorize cybersecurity incidents according to level of severity and impact consistent with the response plan.</p> <p>●●Moderate: Investigate cybersecurity-related notifications generated</p>	<p>RS.AN-1: Notifications from detection systems are investigated</p>	●●	●●	●●	●	●●	DoWI 8510.01
			<p>RS.AN-2: The impact of the incident is understood</p>	●●●	●●●	●●●	●●●	●●●	DoWI 8510.01

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
		from detection systems. Provide on-demand audit review, analysis, and reporting of cybersecurity incidents. Conduct forensic analysis on collected cybersecurity event information to determine root cause. ●●●High: Employ automated mechanisms to assist in the investigation of a cybersecurity related notification and support incident impact analysis, where feasible	RS.AN-3: Forensics are performed	●●	●●	●	●	●●	DoWI 8510.01
			RS.AN-4: Incidents are categorized consistent with response plans	●●	●●	●●	●●	●●	DoWI 8510.01

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	<p>●Low: , ●●Moderate: Contain and mitigate cybersecurity incidents to minimize impact on the control system/OT environment and business objectives. Ensure that vulnerabilities identified while responding to a cybersecurity incident are also mitigated or documented as accepted risks.</p> <p>●●●High: Employ automated mechanisms to support the cybersecurity incident mitigation process, where feasible. If necessary, incorporate manual mitigation by properly trained personnel to thwart a threat within the control system/OT environment.</p>	RS.MI-1: Incidents are contained	●●●	●●●	●●●	●●●	●●●	CJSCM 6510.01B
			RS.MI-2: Incidents are mitigated	●●●	●●●	●●●	●●●	●●●	CJSCM 6510.01B
			RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	●●●	●●●	●●●	●●●	●●●	CJSCM 6510.01B

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
	<p>Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.</p>	<p>●Low, ●●Moderate, ●●●High: Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly.</p> <p>Update response plans to address changes to the organization, control system, attack vectors, or environment of operation and problems encountered during plan implementation, execution, or testing.</p> <p>Enable a process for the response plan to evolve to reflect new threats, improved technology, and lessons learned.</p>	<p>RS.IM-1: Response plans incorporate lessons learned</p>	●●	●●	●●	●●	●●	DoWI 8500.01, DoWI 8510.01
			<p>RS.IM-2: Response strategies are updated</p>	●●	●●	●●	●●	●●	DoWI 8500.01, DoWI 8510.01

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
RECOVER (RC)	<p>Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.</p>	<p>●Low: Execute recovery plans during or after a cybersecurity incident on the control system/OT environment. Restore control systems/OT to a secure operational state.</p> <p>●●Moderate: Execute periodic recovery testing to ensure personnel are prepared for any necessary recovery procedure.</p> <p>●●●High: Ensure that necessary system backups are in place and in accordance with the recovery plan to maintain the control system/OT environment's functionality with little or no loss of operational continuity until the control systems/OT are restored. Ensure that critical devices/systems are identified and that necessary organizational procedures are in place to maintain operational continuity in the event of a system failure.</p>	<p>RC.RP-1: Recovery plan is executed during or after an event</p>	●●●	●●●	●●●	●●●	●●●	DoWI 8500.01, CJCSM 6510.01B

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
	<p>Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.</p>	<p>●Low, ●●Moderate, ●●●High: Incorporate lessons learned from ongoing recovery activities into system recovery procedures, training, and testing. Implement the resulting changes accordingly.</p> <p>Update the recovery plan to address changes to the organization, to the control systems/OT, or to the operational environment. Document all problems encountered during plan implementation, execution, and testing.</p>	<p>RC.IM-1: Recovery plans incorporate lessons learned</p>	●●	●●	●●	●●	●●	DoWI 8500.01, CJCSM 6510.01B
			<p>RC.IM-2: Recovery strategies are updated</p>	●●	●●	●●	●●	●●	DoWI 8500.01, CJCSM 6510.01B

Function	Category	Criticality	Subcategory	Mission Objectives					Informative References
				●●● = High Priority, ●● = Moderate Priority, ● = Low					
				Priority / Other Implemented Subcategories					
Maintain System Availability	Maintain System Integrity	Maintain Human Safety	Maintain Environmental Safety	Maintain Physical Security					
	<p>Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.</p>	<p>●Low, ●●Moderate, ●●●High: Manage the public-facing representation of the organization or of the DoW Component through a coordinated effort. Ensure information is distributed to in a manner that is beneficial to the reputation of the organization according to DoW policies and procedures.</p> <p>Communicate recovery activities to all relevant stakeholders, and executive management teams within DoW and any external participating parties.</p> <p>Assign a Public Affairs Officer and coordinate with DoW PAO.</p>	<p>RC.CO-1: Public relations are managed</p>	●	●	●●	●	●	DoWI 8500.01, CJCSM 6510.01B
			<p>RC.CO-2: Reputation after an event is repaired</p>	●●	●	●●	●	●	DoWI 8500.01, CJCSM 6510.01B
			<p>RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams</p>	●●	●●	●●	●●	●●	DoWI 8500.01, CJCSM 6510.01B

2.3 CSF High Priority Rationale

This section includes a Mission Objective summary, a table with the High and Moderate Priority Subcategories, and a detailed table of High Priority Subcategories for each Mission Objective. This includes context to describe the reasoning behind designating certain Subcategories as High Priority as they relate to business continuity and mission success. Such information can help organizations and mission owners understand and prioritize limited resources within the control system/OT environment.

Mission Objective 1: Maintain System Availability

Description: Preserving the ability to operate the system at the intended level within the desired time frame. Systems function without interruption.

Organizations Should:

- Identify interdependent control systems/OT that pose cybersecurity risks that threaten system availability.
- Initiate risk management procedures related to control systems/OT' engineering lifecycle and change management procedures.
- Manage vulnerability and risk by applying patches on systems in a timely manner regardless of service age, proprietary nature, or perceived obsolescence. Patches should address functionality and stability issues within the original code while also enhancing security. Plan for backups and work arounds.
- Deploy continuous monitoring applications to control systems/OT to detect threats to system availability while ensuring system health.
- Engage in business continuity planning to mitigate the risks of maintaining or reestablishing production in the case of an interruption. Specify recovery objectives (Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs)) for the various systems and subsystems involved based on typical business needs.
- Implement redundancy for critical processes and assets

Identify

In order to maintain system availability, it is essential to identify and understand the security environment of control system/OT assets and their place in the organization's business objectives; each organization's risk management and strategy informs its approach to the Cybersecurity Framework Core.

	High Priority Subcategories	Moderate Priority Subcategories
Asset Management	ID.AM-1, ID.AM-2, ID.AM-3, ID.AM-4, ID.AM-5	ID.AM-6
Business Environment	ID.BE-2, ID.BE-4, ID.BE-5	ID.BE-1, ID.BE-3
Governance	ID.GV-1, ID.GV-4	ID.GV-2, ID.GV-3
Risk Assessment	ID.RA-3, ID.RA-4, ID.RA-5, ID.RA-6	ID.RA-1, ID.RA-2
Risk Management Strategy		ID.RM-1, ID.RM-2, ID.RM-3

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Asset Management	ID.AM-1: Physical devices and systems within the organization are inventoried	Keeping track of the equipment, its physical location, and the software/firmware installed on the hardware is important for normal operations as well as defense and recovery with respect to cyber incidents. If proper inventory is not established and maintained, there could be significant detrimental effects to maintaining availability in the control system/OT environment.
	ID.AM-2: Software platforms and applications within the organization are inventoried	As stated above, keeping track of the equipment, its physical location, and the software/firmware installed on the hardware is important for normal operations as well as defense and recovery with respect to cyber incidents. If proper inventory is not established and maintained, there could be significant detrimental effects to maintaining availability in the control system/OT environment.
	ID.AM-3: Organizational communication and data flows are mapped	Data pathways are becoming increasingly complex and increasingly vulnerable to loss of availability. To mitigate the additional risks to the system environment that comes with additional complexity, it is a high priority to map the organization's data flows. It is essential to do this mapping to identify if a data pathway is at risk of a cyber incident to data-in-transit (e.g., man-in-the-middle attack).

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	ID.AM-4: External information systems are catalogued	It is essential for organizations to comply with DoWI 8510.01's external IT service requirements that external information systems are catalogued. DoW organizations that use external IT services provided by a commercial or other non-federal government entity must ensure the security protections of the system delivering the service is appropriate to the availability needs of the DoW organization's information and mission.
	ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	Prioritizing resources (e.g., hardware, devices, data, and software) based on their classification, criticality, and business value is an essential step in identifying risks and vulnerabilities to the availability of the organization's control system/OT environment.
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	<i>Rationale only provided for High Priority Subcategories</i>
Business Environment	ID.BE-1: The organization's role in the supply chain is identified and communicated	<i>Rationale only provided for High Priority Subcategories</i>
	ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	Control systems/OT are vital to the operation of the DoW and of the U.S. critical infrastructures that are often highly interconnected and mutually dependent systems.
	ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	<i>Rationale only provided for High Priority Subcategories</i>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	ID.BE-4: Dependencies and critical functions for delivery of critical services are established	Identifying dependencies and critical functions for the delivery of critical missions/business functions must be done to understand the threat landscape of the control system/OT environment. This is a high priority due to the continuous nature of control system's processes. A lack of understanding of dependencies and critical functions in relation to control systems/OT will lead to unacceptable and unexpected outages of process that will lead to critical missions/business function failure.
	ID.BE-5: Resilience requirements to support delivery of critical services are established	Due to the potential costs and impact to control system/OT availability of not restoring communication links and processing capabilities, it is necessary to establish resilience requirements of critical services. Without the resilience requirements, organizations run the risk of unacceptable gaps in system availability.

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Governance	ID.GV-1: Organizational information security policy is established	It is DoW policy that: the DoW will establish and use an integrated enterprise-wide decision structure for cybersecurity risk management (the RMF) that includes and integrates DoW mission areas (MAs) pursuant to DoWD 8115.01. Without an organizational information security policy, organizations run the unacceptable risk of having either no protection of control systems/OT or an ad-hoc, disparate policy that is not aligned with overall availability requirements of the control system/OT environment.
	ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	<i>Rationale only provided for High Priority Subcategories</i>
	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberty obligations, are understood and managed	<i>Rationale only provided for High Priority Subcategories</i>
	ID.GV-4: Governance and risk management processes address cybersecurity risks	It is DoW policy that: the DoW will establish and use an integrated enterprise-wide decision structure for cybersecurity risk management (the RMF) that includes and integrates DoW mission areas (MAs) pursuant to DoWD 8115.01. Without a governance and risk management process that address cybersecurity risks, organizations run the unacceptable risk of having either no protection of control systems/OT or an ad-hoc, disparate policy that is not aligned with overall availability requirements of the control system/OT environment.

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Risk Assessment	ID.RA-1: Asset vulnerabilities are identified and documented	<i>Rationale only provided for High Priority Subcategories</i>
	ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	<i>Rationale only provided for High Priority Subcategories</i>
	ID.RA-3: Threats, both internal and external, are identified and documented	Identifying and documenting internal and external threats is an imperative step to securing control systems/OT and mitigating cybersecurity risks. Organizations must identify these threats to control system/OT security throughout the lifecycle of the control systems/OT from architecture to procurement to installation to maintenance to decommissioning. Due to the rapidly evolving nature of control systems/OT, it is important to identify and review new control system/OT capabilities and their associated emerging threats, particularly to system availability. The identification process should leverage organizations that identify emerging threats such as the ICSCERT.

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	ID.RA-4: Potential business impacts and likelihoods are identified	Due to the assumption that cybersecurity events in the control system/OT environment are likely inevitable, organizations must identify potential business impacts of these events, preferably, where applicable, in financial terms. This essential step in identifying risk utilizes a combination of business impact and likelihood to assess risks and utilizes resources efficiently to mitigate those risks. Without identifying business impacts, organizations run the risk of establishing inappropriate, compliance-based IT security programs that are wasteful and non-resilient. This is a particularly high priority due to the continuous nature of control systems/OT processes and their strong availability requirements.
	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	It is a high priority that the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation that would result from a failure in control system/OT availability is determined by considering threats, vulnerabilities, and potential impacts as well as existing and planned risk mitigation. If threats, vulnerabilities, likelihoods, and impacts are not used to determine risk, organizations will expose its control system/OT environment to multiple, unacceptable risks to system availability.

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	ID.RA-6: Risk responses are identified and prioritized	Risk responses differ from incident responses in that actions taken by an organization in responding to incidents are pre-determined and are derived from the information contained in risk responses. Risk responses take into consideration the organization's risk tolerance after identifying a risk considers the best alternatives for the organization (e.g., acceptance, avoidance, mitigation, sharing or transfer). If risk responses are not identified and prioritized, organizations will accept inappropriate risks to system availability.
Risk Management Strategy	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	<i>Rationale only provided for High Priority Subcategories</i>
	ID.RM-2: Organizational risk tolerance is determined and clearly expressed	<i>Rationale only provided for High Priority Subcategories</i>
	ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	<i>Rationale only provided for High Priority Subcategories</i>

Protect

For control systems/OT, system availability (i.e., reliability) requirements are an essential factor in design. This stringent availability requirement differs from typical IT systems and results in different strategies to mitigate vulnerabilities and risks (e.g., rebooting a component may not be acceptable for control systems/OT because of the adverse effects on availability). These strategies to protect from and mitigate risks include maintaining strong access control measures; protecting data in-transit and at-rest; employing comprehensive information protection processes and procedures; ensuring maintenance and repairs are performed consistent with policies and procedures; and deploying technical security solutions to maintain the security and availability of the control system /OT environment.

	High Priority Subcategories	Moderate Priority Subcategories
Access Control	PR.AC-2, PR.AC-3, PR.AC-4, PR.AC5	PR.AC-1
Awareness and Training	PR.AT-1, PR.AT-5	PR.AT-2, PR.AT-3, PR.AT-4
Data Security	PR.DS-4, PR.DS-7	PR.DS-2, PR.DS-3, PR.DS-6
Information Protection Process and Procedures	PR.IP-1, PR.IP-3, PR.IP-4, PR.IP-5, PR.IP-9, PR.IP-12	PR.IP-2, PR.IP-6, PR.IP-7, PR.IP-10, PR.IP-11
Maintenance	PR.MA-2	PR.MA-1
Protective Technology	PR.PT-1, PR.PT-3, PR.PT-4	PR.PT-2

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Access Control	PR.AC-1: Identities and credentials are managed for unauthorized devices and users	<i>Rationale only provided for High Priority Subcategories</i>
	PR.AC-2: Physical access to assets is managed and protected	Unauthorized physical access to the control system/OT environment could cause serious disruption to the control system's functionality and could result in a loss of availability of the system. It is important for organizations to limit physical access to control system/OT environments to prevent physical modification, manipulation, or destruction of existing system infrastructure. Any malicious tampering with the control system/OT environment could result in system failure or interruption of business operations. As such, physical access to assets must be managed to ensure that system availability is maintained.

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	PR.AC-3: Remote access is managed	<p>There are many reasons why a control system may need to be remotely accessed, including vendors and system integrators performing system maintenance functions, and control system/OT engineers accessing geographically remote system components. Remote access capabilities must be adequately controlled to prevent unauthorized individuals from gaining access to the control system. Unauthorized access from a remote location can have the same catastrophic effect on a control system/OT environment as malicious physical access. As such, remote access must be carefully managed to maintain system availability.</p>
	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	<p>Incorporating least privilege is only allowing authorized accesses for users which are necessary to accomplish the assigned tasks in accordance with organizational missions and business functions. Separation of duties is requiring more than one person to complete a task to prevent fraud and human error. These role-based measures are particularly helpful in a control system/OT environment to prevent any accidental or intentional tampering that could lead to system failure and hinder system availability.</p>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	Network integrity refers to the complete organizational network with network discoverable resources matching those that would be listed in an organization's inventory. As such, it is essential to preserve network integrity by only allowing secure connections between nodes in a network and minimizing connections to only those needed for necessary business functions. Particularly in a control system/OT environment, it is beneficial to separate the control system/OT network from the organization's internal network with a firewall, DMZ, or by air gapping (at minimum), because the two often have differing security requirements. Any compromise to network integrity by hardware failure, software failure, or network intrusion, will impede system availability causing an unexpected stop in critical mission/business objectives.
Awareness and Training	PR.AT-1: All users are informed and trained	A key measure in maintaining a control system/OT environment's availability is ensuring that all users are informed of the dangers, risks and responsibilities associated with their roles. Proper training is one of the greatest forms of protection when creating a safe control system/OT environment. Human error is a common cause of vulnerability exploitation, security breaches and accidental cyber incidents that can lead to potential loss of system availability. Therefore, all users interacting with the control system/OT environment must receive proper training to maintain a safe control system/OT environment.

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	PR.AT-2: Privileged users understand roles & responsibilities	<i>Rationale only provided for High Priority Subcategories</i>
	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	<i>Rationale only provided for High Priority Subcategories</i>
	PR.AT-4: Senior executives understand roles & responsibilities	<i>Rationale only provided for High Priority Subcategories</i>
	PR.AT-5: Physical and information security personnel understand roles & responsibilities	A key measure in maintaining system availability is ensuring that all physical and information security personnel understand their roles and responsibilities in the control system/OT environment and are aware of the risks of and threats to the control system/OT environment. Particularly with control systems/OT, attack vectors exist at the physical level as well as the system level that can lead to an unplanned loss of availability. Therefore, physical and information security personnel must have a clear understanding of their responsibility to protect control systems/OT.
Data Security	PR.DS-2: Data-in-transit is protected	<i>Rationale only provided for High Priority Subcategories</i>
	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	<i>Rationale only provided for High Priority Subcategories</i>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	<p>PR.DS-4: Adequate capacity to ensure availability is maintained</p>	<p>Maintaining adequate capacity (including but not limited to computing power, networking capability, storage space, etc.) ensures that essential mission and business functions continue running efficiently. If an organization does not provide adequate capacity within a control system/OT environment, the system could be susceptible to a denial of service attack or another incident that could lead to catastrophic system failure and a gap in system availability. Supplying a control system/OT environment with adequate capacity (computing power, networking capability, storage space, etc.) is essential to maintain system availability.</p>
	<p>PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity</p>	<p><i>Rationale only provided for High Priority Subcategories</i></p>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	<p>PR.DS-7: The development and testing environment(s) are separate from the production environment</p>	<p>It is important to have separation between the development/testing and production environment, particularly in maintaining system availability. The development and testing environments are used to implement patches, configuration changes, adjust control system/OT components, and make other changes to the control system/OT environment. Often, it is during the change process that vulnerabilities arise. As such, it is essential to implement these changes in a testing environment prior to pushing the changes to the production environment. If changes were incorporated into the production environment prior to any testing, the changes could result in a vulnerability that would cause system failure and ultimately impede system availability.</p>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Information Protection Process and Procedures	PR.IP-1: A baseline configuration of control systems/OT is created and maintained	Validated and tested baseline configurations promote consistency when configuring new systems to provide a reliable operating state. Baselines also support response and recovery efforts in returning to a reliable operating state after an incident. Lastly, baseline configurations establish a minimum standard of security that is required in the control system/OT environment. Each of these factors contribute to supporting system availability and business continuity. Without a baseline configuration for the control system/OT environment, it would be more challenging for organizations to return to a reliable operating state, which would impede system availability.
	PR.IP-2: A System Development Life Cycle to manage systems is implemented	<i>Rationale only provided for High Priority Subcategories</i>
	PR.IP-3: Configuration change control processes are in place	A lack of configuration change management procedures can lead to security oversights, exposures, and risks that can harm system availability. Vulnerabilities typically arise when the configuration of a system or environment changes. As such, any alteration to a control system/OT environment, network, component, or software must be documented and tested. Neglecting configuration change control processes could lead to the exploitation of a vulnerability that results in catastrophic system failure, inhibiting system availability.

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	PR.IP-4: Backups of information are conducted, maintained, and tested periodically	Having information backups directly correlates to maintaining system availability. Incidents within a control system/OT environment are an inevitability, and they can often lead to system failure or data loss. Ensuring that backups of mission critical information are in place and tested provides redundancy and supports system availability and overall business continuity.
	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	High availability control system/OT components must be placed in controlled environments to ensure their continued operation. Computing equipment is highly sensitive to temperature, humidity, and dust. Therefore, it is essential that organizations satisfy policy and regulations to ensure that availability within the control system/OT environment is maintained.
	PR.IP-6: Data is destroyed according to policy	<i>Rationale only provided for High Priority Subcategories</i>
	PR.IP-7: Protection processes are continuously improved	<i>Rationale only provided for High Priority Subcategories</i>
	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	Response plans and recovery plans are fundamental in any organization's security posture to limit the consequences of incidents and maintain or reestablish operations (and system availability) in the case of an interruption. Establishing a plan of action for rapid response to, and effective recovery from an incident or disaster is paramount in maintaining system availability.
	PR.IP-10: Response and recovery plans are tested	<i>Rationale only provided for High Priority Subcategories</i>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	<p>PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)</p>	<p><i>Rationale only provided for High Priority Subcategories</i></p>
	<p>PR.IP-12: A vulnerability management plan is developed and implemented</p>	<p>Incorporating a vulnerability management plan into the control system/OT environment is vital in protecting control system/OT assets. Organizations need a systematic method for documenting vulnerabilities, developing a standard remediation timeline and defining periodic and proactive activities for vulnerability detection. Patch management allows for controlled and secure updates that can be tailored for the needs of the control system/OT environment. Ensuring that vulnerabilities are managed minimizes the potential for system exploits, supporting the mission objective of maintaining system availability.</p>
Maintenance	<p>PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools</p>	<p><i>Rationale only provided for High Priority Subcategories</i></p>
	<p>PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access</p>	<p>Remote maintenance must be monitored. Like unauthorized physical access, unauthorized remote access to a control system/OT environment for maintenance could result in serious disruption to control system/OT functionality. Any malicious tampering with the control system/OT environment could result in system failure or interruption of business operations. As such, remote access to assets must be managed to ensure that system availability is maintained.</p>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Protective Technology	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	<p>The security architecture of a control system/OT must incorporate mechanisms to monitor, log, and audit activities occurring within the control system/OT environment and on control system/OT networks. Auditing and logging activities are imperative to understanding the current state of the control system, validating that the system is operating as intended, and that no policy violations or cyber incidents have hindered the operation of the system. Auditing and logging can help provide indication of a compromised system and can assist in forensic analysis after an incident occurs. As such, these activities are crucial in maintaining system availability.</p>
	PR.PT-2: Removable media is protected and its use restricted according to policy	<i>Rationale only provided for High Priority Subcategories</i>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	<p>PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality</p>	<p>The principle of least functionality provides that a system is configured to execute only essential capabilities and to prohibit the use of non-essential functions that are not integral to the operation of the system. Incorporating the principle of least functionality on top of protective measures against unauthorized physical or remote access to systems and assets further aids in protecting a control system/OT environment. As aforementioned, unauthorized access to a control system/OT environment can lead to catastrophic system failure, which inhibits system availability. Incorporating the principle of least functionality aids in minimizing the damage that an attacker can cause to a control system/OT environment by limiting the capabilities of the system itself.</p>
	<p>PR.PT-4: Communications and control networks are protected</p>	<p>Network security is critical in any control system/OT environment. At minimum, the control system/OT network should be logically separated from the corporate network on physically separate network devices (ideally with a DMZ as an intermediary between the two networks). Communications and control networks both have avenues through which an adversary could impact the availability of a control system/OT and hinder business operations. Therefore, it is critical to implement protective technologies (e.g., network and host firewalls) to ensure networks are protected from external sources and only explicitly authorized communication and activity occurs.</p>

Detect	Implementing detection measures for continuous monitoring of control system/OT environments and data is a critical way to ensure system availability. Detection for anomalous events and continuous monitoring allows for rapid detection of inappropriate or malicious activity that can lead to rapid response and ensure constant functionality.	
	High Priority Subcategories	Moderate Priority Subcategories
Anomalies and Events	DE.AE-1, DE.AE-4	DE.AE-2, DE.AE-3
Security Continuous Monitoring	DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-4, DE.CM-7, DE.CM-8	DE.CM-5, DE.CM-6
Detection Processes		DE.DP-1, DE.DP-3, DE.DP-4, DE.DP-5

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Anomalies and Events	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	Understanding the baseline of network operations and expected data flows during operations supports operational security by providing a means of comparing current activities against expectations to identify anomalies or other events that may require analysis and response.
	DE.AE-2: Detected Events are analyzed to understand attack targets and methods	<i>Rationale only provided for High Priority Subcategories</i>
	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	<i>Rationale only provided for High Priority Subcategories</i>
	DE.AE-4: Impact of events is determined	Knowing the impact of events is essential for organizations to prevent events from becoming incidents; to understand the way forward to maintain and recover system availability; and to mitigate the effects of an incident.
Security Continuous Monitoring	DE.CM-1: The network is monitored to detect potential cybersecurity events	Detecting potential cybersecurity events using appropriate continuous monitoring processes can help defenders break the attack chain before attackers attain their objectives, maintaining system availability.

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	Monitoring the physical environment for potential cybersecurity events can help defenders break the attack chain before attackers attain their objectives, maintaining system availability. Due to the nature of control systems/OT interaction with the physical world, physical monitoring is essential.
	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	Monitoring personnel activity is of high priority to reduce the possibility and risk of human error, theft, and fraud and their impacts on system availability by detecting intentional or unintentional misuse of control systems/OT and other informational assets.
	DE.CM-4: Malicious code is detected	Detecting malicious code rapidly before the code can negatively affect a control system/OT is critical for maintaining system availability. Implementing antivirus tools into a control system/OT environment is essential for malicious code detection. Antivirus tools function effectively when configured against a known state of attack methods and payloads.
	DE.CM-5: Unauthorized mobile code is detected	<i>Rationale only provided for High Priority Subcategories</i>
	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	<i>Rationale only provided for High Priority Subcategories</i>
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	Monitoring for unauthorized personnel, connections, devices and software is necessary to validate that the control system/OT environment is operating as intended and that no policy or cyber incidents have hindered system availability.

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	DE.CM-8: Vulnerability scans are performed	Where applicable, vulnerability scans are a high priority for identifying any weaknesses that can contribute to system availability risks and mitigation approaches to reduce those risks. Not all systems within a control system/OT environment (e.g., legacy control systems/OT) benefit from traditional vulnerability scans. It is essential that the risks of vulnerability scanning on particular systems is understood and that alternative scanning methods (passive or manual vulnerability analysis) are used when needed.
Detection Processes	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	<i>Rationale only provided for High Priority Subcategories</i>
	DE.DP-3: Detection processes are tested	<i>Rationale only provided for High Priority Subcategories</i>
	DE.DP-4: Event detection information is communicated to appropriate parties	<i>Rationale only provided for High Priority Subcategories</i>
	DE.DP-5: Detection processes are continuously improved	<i>Rationale only provided for High Priority Subcategories</i>

Respond Response plan development and execution is critical to maintaining system availability. Organizations must be prepared contain, mitigate, and understand the impact of incidents as they are an inevitability.

	High Priority Subcategories	Moderate Priority Subcategories
Response Planning	RS.RP-1	
Communications		RS.CO-1, RS.CO-3, RS.CO-4, RS.CO-5
Analysis	RS.AN-2	RS.AN-1, RS.AN-3, RS.AN-4
Mitigation	RS.MI-1, RS.MI-2, RS.MI-3	
Information Protection Process and Procedures		RS.IM-1, RS.IM-2

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Response Planning	RS.RP-1: Response plan is executed during or after an event	An incident response plan is essential documentation consisting of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of incidents against an organization's information systems' availability. Responding appropriately to incidents can help protect the organization's resources including those that may impact system availability.
Communications	RS.CO-1: Personnel know their roles and order of operations when a response is needed	<i>Rationale only provided for High Priority Subcategories</i>
	RS.CO-3: Information is shared consistent with response plans	<i>Rationale only provided for High Priority Subcategories</i>
	RS.CO-4: Coordination with stakeholders occurs consistent with response plans	<i>Rationale only provided for High Priority Subcategories</i>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	<i>Rationale only provided for High Priority Subcategories</i>
Analysis	RS.AN-1: Notifications from detection systems are investigated	<i>Rationale only provided for High Priority Subcategories</i>
	RS.AN-2: The impact of the incident is understood	Knowing the impact of incidents is essential for organizations to mitigate the incident's effect on system availability; to understand the way forward to maintain system availability; to provide a means to compare current state with expected state in a response timeline; and to allow an organization to apply lessons learned in responding to a future incident. This is critical in control system/OT environments as an organization must understand the immediate and long-term effects an incident can have on system availability.
	RS.AN-3: Forensics are performed	<i>Rationale only provided for High Priority Subcategories</i>
	RS.AN-4: Incidents are categorized consistent with response plans	<i>Rationale only provided for High Priority Subcategories</i>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Mitigation	RS.MI-1: The incidents are contained	In any incident response situation, the primary action after detecting a cyber incident is to contain the incident so it cannot spread throughout the organization or to other systems. Effectively contained events and incidents isolate control systems/OT to minimize any damage or impact to DoW information networks, control system/OT components, data, and services by preventing any further contamination, intrusion, or malicious activity. As such, containment is key in ensuring business continuity and maintaining system availability.
	RS.MI-2: The incidents are mitigated	It is essential in responding to an incident to follow an appropriate course of action that executes a response plan identifying if eradication is necessary, or should be performed in recovery, to properly mitigate an incident that is adversely affecting system availability. Any mitigation measures must be carefully considered to ensure that they do not add additional adverse effects to those caused by the incident. If proper mitigation measures are not incorporated into an organization's incident response, the harmful impact an incident could have on system availability would be indefinite.

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	A newly identified vulnerability that can result in unauthorized access, use, disclosure, disruption, modification, or destruction of a control system/OT and data is as threatening to an organization or system environment must be mitigated or documented as acceptable risk. Zero-day vulnerabilities are a common cause of security breaches and can be exploited by adversaries to affect system availability until they are mitigated. Once a vulnerability of any kind is discovered, it must be resolved or documented as an accepted risk based on the priorities and risk tolerance of the organization; otherwise, the vulnerability could result in an exploit that could cause catastrophic system failure and hinder system availability.
Improvements	RS.IM-1: Response plans incorporate lessons learned	<i>Rationale only provided for High Priority Subcategories</i>
	RS.IM-2: Response strategies are updated	<i>Rationale only provided for High Priority Subcategories</i>

Recover Effective recovery measures are critical to maintaining system availability. After an incident occurs, organizations must be able to return to full functionality quickly and they must be able to make improvements based on lessons learned.

	High Priority Subcategories	Moderate Priority Subcategories
Recovery Planning	RC.RP-1	
Improvements		RC.IM-1, RC.IM-2
Communications		RC.CO-2, RC.CO-3

Detailed Specifications

Category	Subcategory	Rationale for High Priority
Recovery Planning	RC.RP-1: Recovery plan is executed during or after an event	Recovery plans help organizations maintain operational continuity after an adverse event or cyber incident has occurred. Ensuring that an organization has pre-defined activities in place that specify recovery objectives (Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs)) for the various systems and subsystems involved, based on typical business need, to restore functionality is essential to maintaining system availability.
Improvements	RC.IM-1: Recovery plans incorporate lessons learned	<i>Rationale only provided for High Priority Subcategories</i>
	RC.IM-2: Recovery strategies are updated	<i>Rationale only provided for High Priority Subcategories</i>
Communications	RC.CO-2: Reputation after an event is repaired	<i>Rationale only provided for High Priority Subcategories</i>
	RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	<i>Rationale only provided for High Priority Subcategories</i>

Mission Objective 2: Maintain System Integrity

Description: Ensuring the ability to execute the correct instructions using the correct data at the correct time to preserve the ability to operate the system in the intended way.

Organizations Should:

- Identify interdependent control systems/OT that pose cybersecurity risks that threaten system integrity.
- Incorporate outcomes of Cybersecurity risk assessments that require an analysis of potential exploitation of vulnerabilities by a malicious actor.
- Incorporate outcomes of Cybersecurity risk assessments that account for adverse impacts on system data that may be the byproduct of system operations.
- Perform data hygiene processes to mitigate risks from duplicative, outdated, incorrect and unused data. Plan for backups and work arounds.
- Incorporate integrity checking mechanisms into operations to verify software, firmware, and information integrity.
- Apply Continuous Monitoring to ensure that data in use, in transit, and at rest is accounted for and checked for deliberate or accidental unauthorized manipulation.
- Mitigate business continuity risk by specifying Recovery Point Objectives (RPO) and backups of system configuration data.

Identify

Risk assessment and asset management are the primary methods for ensuring that system integrity is maintained. It is essential that an organization is aware of the risks associated with a control system/OT environment and that authorized personnel are interacting with the system. Additionally, proper governance and policy is needed to ensure that appropriate security measures are used.

	High Priority Subcategories	Moderate Priority Subcategories
Asset Management	ID.AM-1, ID.AM-2, ID.AM-3, ID.AM-4, ID.AM-5	ID.AM-6
Business Environment	ID.BE-4, ID.BE-5	ID.BE-1, ID.BE-2, ID.BE-3
Governance	ID.GV-1, ID.GV-4	ID.GV-2, ID.GV-3
Risk Assessment	ID.RA-3, ID.RA-5, ID.RA-6	ID.RA-1, ID.RA-2, ID.RA-4
Risk Management Strategy		ID.RM-1, ID.RM-2, ID.RM-3

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Asset Management	ID.AM-1: Physical devices and systems within the organization are inventoried	Keeping track of the equipment, its physical location, and the software/firmware installed on the hardware is important for normal operations as well as defense and recovery with respect to cyber incidents. If proper inventory is not established and maintained, there could be significant detrimental effects to maintaining integrity in the control system/OT environment.
	ID.AM-2: Software platforms and applications within the organization are inventoried	As stated above, keeping track of the equipment, its physical location, and the software/firmware installed on the hardware is important for normal operations as well as defense and recovery with respect to cyber incidents. If proper inventory is not established and maintained, there could be significant detrimental effects to maintaining integrity in the control system/OT environment.

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	ID.AM-3: Organizational communication and data flows are mapped	Data pathways are becoming increasingly complex and increasingly vulnerable to loss of integrity. To mitigate the additional risks to the system environment that comes with additional complexity, it is a high priority to map the organization's data flows. It is essential to do this mapping to identify if a data pathway is at risk of a cyber incident to data-in-transit (e.g., man-in-the-middle attack). Additionally, mapping logical data flows allows an organization to identify anomalous or inappropriate data flow within a control system/OT environment. If data flows to or from a source do not match the mapping established by the organization, this could indicate a compromise to system integrity.
	ID.AM-4: External information systems are catalogued	It is essential for organizations to comply with DoWI 8510.01's external IT service requirements that external information systems are catalogued. DoW organizations that use external IT services provided by a commercial or other non-federal government entity must ensure the security protections of the system delivering the service is appropriate to the integrity needs of the DoW organization's information and mission. Otherwise, the organization opens itself to vulnerabilities from external sources that could negatively impact system integrity.

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	<p>ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value</p>	<p>Prioritizing resources (e.g., hardware, devices, data, and software) based on their classification, criticality, and business value is an essential step in identifying risks and vulnerabilities to the integrity of the organization's control system/OT environment.</p>
	<p>ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established</p>	<p><i>Rationale only provided for High Priority Subcategories</i></p>
Business Environment	<p>ID.BE-1: The organization's role in the supply chain is identified and communicated</p>	<p><i>Rationale only provided for High Priority Subcategories</i></p>
	<p>ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated</p>	<p><i>Rationale only provided for High Priority Subcategories</i></p>
	<p>ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated</p>	<p><i>Rationale only provided for High Priority Subcategories</i></p>
	<p>ID.BE-4: Dependencies and critical functions for delivery of critical services are established</p>	<p>Identifying dependencies and critical functions for the delivery of critical missions/business functions must be done to understand the threat landscape of the control system/OT environment. This is a high priority due to the continuous nature of control system's processes. A lack of understanding of dependencies and critical functions in relation to control systems/OT will lead to unacceptable and unexpected outages of process that will lead to critical missions/business function failure.</p>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	ID.BE-5: Resilience requirements to support delivery of critical services are established	Due to the potential costs and impact to control system/OT integrity of not restoring production or product conditions to a past, successful state, it is necessary to establish resilience requirements of critical services. Without the resilience requirements, organizations run the risk of an intolerable absence of data posing a risk to critical mission/business objectives.
Governance	ID.GV-1: Organizational information security policy is established	It is DoW policy that: the DoW will establish and use an integrated enterprise-wide decision structure for cybersecurity risk management (the RMF) that includes and integrates DoW mission areas (MAs) pursuant to DoWD 8115.01. Without an organizational information security policy, organizations run the unacceptable risk of having either no protection of control systems/OT or an ad-hoc, disparate policy that is not aligned with overall integrity requirements of the control system/OT environment.
	ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	<i>Rationale only provided for High Priority Subcategories</i>
	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberty obligations, are understood and managed	<i>Rationale only provided for High Priority Subcategories</i>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	ID.GV-4: Governance and risk management processes address cybersecurity risks	It is DoW policy that: the DoW will establish and use an integrated enterprise-wide decision structure for cybersecurity risk management (the RMF) that includes and integrates DoW mission areas (MAs) pursuant to DoWD 8115.01. Without a governance and risk management process that address cybersecurity risks, organizations run the unacceptable risk of having either no protection of control systems/OT or an adhoc, disparate policy that is not aligned with overall integrity requirements of the control system/OT environment.
Risk Assessment	ID.RA-1: Asset vulnerabilities are identified and documented	<i>Rationale only provided for High Priority Subcategories</i>
	ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	<i>Rationale only provided for High Priority Subcategories</i>
	ID.RA-3: Threats, both internal and external, are identified and documented	Identifying and documenting internal and external threats is an imperative step to securing control systems/OT and mitigating cybersecurity risks. Organizations must identify these threats to control system/OT security throughout the lifecycle from architecture to procurement to installation to maintenance to decommissioning. Due to the rapidly evolving nature of control systems/OT, it is important to identify and review new control system/OT capabilities and their associated emerging threats, particularly to system integrity. The identification process should leverage organizations that identify emerging threats such as the ICS-CERT.

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	ID.RA-4: Potential business impacts and likelihoods are identified	<i>Rationale only provided for High Priority Subcategories</i>
	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	It is a high priority that the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation that would result from a failure in control system/OT availability is determined by considering threats, vulnerabilities, and potential impacts as well as existing and planned risk mitigation. If threats, vulnerabilities, likelihoods, and impacts are not used to determine risk, organizations will expose its control system/OT environment to multiple, unacceptable risks to system integrity.
	ID.RA-6: Risk responses are identified and prioritized	Risk responses differ from incident responses in that actions taken by an organization in responding to incidents are pre-determined and are derived from the information contained in risk responses. Risk responses take into consideration the organization's risk tolerance after identifying a risk considers the best alternatives for the organization (e.g., acceptance, avoidance, mitigation, sharing or transfer). If risk responses are not identified and prioritized, organizations will accept inappropriate risks to system integrity.
Risk Management Strategy	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	<i>Rationale only provided for High Priority Subcategories</i>
	ID.RM-2: Organizational risk tolerance is determined and clearly expressed	<i>Rationale only provided for High Priority Subcategories</i>

Unclassified

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	<i>Rationale only provided for High Priority Subcategories</i>

Protect

For control systems/OT, security protections must be implemented with a focus on maintaining system integrity due to the high potential impact on the control system/OT environment from a loss of integrity. These protection strategies to mitigate risks include maintaining strong access control measures; protecting data in-transit and at-rest; employing comprehensive information protection processes and procedures; ensuring maintenance and repairs are performed consistent with policies and procedures; and deploying technical security solutions (e.g., strong auditing and log management tools) to maintain the security and integrity of the control system/OT environment.

	High Priority Subcategories	Moderate Priority Subcategories
Access Control	PR.AC-1, PR.AC-2, PR.AC-3, PR.AC4, PR.AC-5	
Awareness and Training	PR.AT-1	PR.AT-2, PR.AT-3, PR.AT-4, PR.AT-5
Data Security	PR.DS-1, PR.DS-2, PR.DS-3, PR.DS-6, PR.DS-7	PR.DS-5
Information Protection Process and Procedures	PR.IP-1, PR.IP-3, PR.IP-4, PR.IP-9, PR.IP-12	PR.IP-2, PR.IP-5, PR.IP-6, PR.IP-7, PR.IP-10, PR.IP11
Maintenance	PR.MA-2	PR.MA-1
Protective Technology	PR.PT-1, PR.PT-2, PR.PT-4	PR.PT-3

Detailed Specifications

Category	Subcategory	Rationale for High Priority
Access Control	PR.AC-1: Identities and credentials are managed for authorized devices and users	Unauthorized access to the control system/OT environment could allow a malicious actor to alter the configuration of a system or manipulate system data. As such, organizations must implement procedures for identifying and authenticating users, processes, and devices for approved business functions. Without identity and access management, the attack surface area for altering data in the control system/OT environment is unacceptable. Ensuring that only authorized users access systems for approved uses is critical in maintaining system integrity.

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	PR.AC-2: Physical access to assets is managed and protected	Unauthorized physical access to the control system/OT environment could cause serious disruption and tampering to the control system's functionality. This could result in a loss of availability of the system. It is important for organizations to limit physical access to control system environments to prevent physical modification, manipulation, or destruction of existing system infrastructure. Any malicious tampering with the control system/OT environment could result in system failure or loss of integrity. As such, physical access to assets must be managed to ensure that system integrity is maintained.
	PR.AC-3: Remote access is managed	There are many reasons why a control system/OT may need to be remotely accessed, including vendors and system integrators performing system maintenance functions, and control system/OT engineers accessing geographically remote system components. Remote access capabilities must be adequately controlled to prevent unauthorized individuals from gaining access to the control system/OT environment. Unauthorized remote access offers an adversary many avenues to manipulate control system/OT data or the control system/OT environment as a whole. As such, remote access must be carefully managed to maintain system integrity.

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	<p>PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties</p>	<p>Incorporating least privilege is only allowing authorized accesses for users which are necessary to accomplish the assigned tasks in accordance with organizational missions and business functions. Separation of duties is requiring more than one person to complete a task to prevent fraud and human error. These role-based measures are particularly helpful in a control system/OT environment to prevent any accidental or intentional tampering that could lead to the alteration of data or system configuration and damage system integrity.</p>
	<p>PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate</p>	<p>Network integrity refers to the complete organizational network with network discoverable resources matching those that would be listed in an organization's inventory. As such, it is essential to preserve network integrity by only allowing secure connections between nodes in a network and minimizing connections to only those needed for necessary business functions. Particularly in a control system/OT environment, it is beneficial to separate the control system/OT network from the organization's internal network with a firewall (at minimum) because the two often have differing security requirements. Loss of network integrity due to hardware failure, software failure, or network intrusion could directly create a design flaw or unauthorized data modification, damaging overall system integrity.</p>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Awareness and Training	PR.AT-1: All users are informed and trained	A key measure in maintaining a control system/OT environment's integrity is ensuring that all users are informed of the dangers, risks and responsibilities associated with their roles. Proper training is one of the greatest forms of protection when creating a safe control system/OT environment. Human error is a common cause of vulnerability exploitation, security breaches and accidental cyber incidents that can lead to potential loss of system integrity. Therefore, all users interacting with the control system/OT environment must receive proper training to maintain a safe control system/OT environment.
	PR.AT-2: Privileged users understand roles & responsibilities	<i>Rationale only provided for High Priority Subcategories</i>
	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	<i>Rationale only provided for High Priority Subcategories</i>
	PR.AT-4: Senior executives understand roles & responsibilities	<i>Rationale only provided for High Priority Subcategories</i>
	PR.AT-5: Physical and information security personnel understand roles & responsibilities	<i>Rationale only provided for High Priority Subcategories</i>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Data Security	PR.DS-1: Data-at-rest is protected	Data security is a critical aspect of maintaining system integrity. Although data-at-rest does not flow across multiple devices or nodes in a network, it is susceptible to theft and unauthorized access that could lead to malicious manipulation of data. Organizations must employ protective measures such as device encryption and limiting user access to control system/OT assets to protect data-at-rest and ultimately maintain system integrity.
	PR.DS-2: Data-in-transit is protected	Protecting data-in-transit is an integral part of maintaining system integrity. Data-in-transit flows from device to device and across networks. As such, it is susceptible to man-in-the-middle attacks and other interception and manipulation methods if not properly secured. In order to maintain system integrity, organizations must implement protective measures such as secure protocols and cryptographic mechanisms in the control system/OT environment to restrict unauthorized modification of data-in-transit.

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	Organizations must establish and maintain tracking and management procedures for systems and assets throughout their lifecycle. Whether an asset is removed, transferred or it is disposed of entirely from the control system/OT environment, the organization must document the changes and execute established change management procedures. Without executing the proper asset management procedures, an attacker could use a mismanaged asset to threaten system integrity. For example, if a device was removed from the control system/OT environment without the change being documented, an attacker could use this device and be perceived as an authorized asset while acting maliciously in the control system/OT environment. Therefore, it is essential for organizations to formally manage all assets in a control system/OT environment throughout removal, transfers, and disposition.
	PR.DS-5: Protections against data leaks are implemented	<i>Rationale only provided for High Priority Subcategories</i>
	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	Integrity checking mechanisms are used to prevent, deter, detect and mitigate malware. It is essential to have monitoring mechanisms in place to know if unauthorized alteration of software, firmware, or data has occurred within the control system/OT environment. If organizations neglect to implement integrity checking mechanisms, it severely limits the organization's ability to determine if system integrity is maintained.

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	<p>PR.DS-7: The development and testing environment(s) are separate from the production environment</p>	<p>It is important to have separation between the development/testing and production environment, particularly for maintaining system integrity. The development and testing environments are used to implement patches, configuration changes, adjust control system/OT components, and make other changes to the control system environment. Often, it is during the change process that vulnerabilities arise. As such, it is essential to implement these changes in an environment separate from the production environment and prior to pushing the changes to the production environment. Without testing overall system environment functionality prior to the production phase, a vulnerability in the production environment could be exploited by an adversary that would ultimately damage system integrity.</p>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Information Protection Process and Procedures	<p>PR.IP-1: A baseline configuration of information technology/ control systems/OT is created and maintained</p>	<p>Validated and tested baseline configurations promote consistency when configuring new systems to provide a reliable operating state. Baseline configurations also establish a minimum standard of security that is required in the control system/OT environment. Without a baseline configuration for the control system/OT environment, it would be very challenging for organizations to securely implement new systems or components into the control system/OT environment. If two of the same devices were incorporated into the control system/OT environment with the same mission function and differing levels of security due to inconsistent configuration, vulnerabilities could arise that would open avenues for intentional or accidental manipulation of a system or data that would impede overall system integrity.</p>
	<p>PR.IP-2: A System Development Life Cycle to manage systems is implemented</p>	<p><i>Rationale only provided for High Priority Subcategories</i></p>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	PR.IP-3: Configuration change control processes are in place	A lack of configuration change management procedures can lead to security oversights, exposures, and risks that pose significant harm, to system integrity. Vulnerabilities typically arise when the configuration of a system or environment changes. As such, any alteration to a control system/OT environment, network, component, or software must be documented and tested. Neglecting configuration change control processes could lead to the exploitation of a vulnerability that results in the alteration of data, damaging system integrity.
	PR.IP-4: Backups of information are conducted, maintained, and tested periodically	Having information backups directly correlates to maintaining system integrity. Incidents within a control system/OT environment are an inevitability, and they can often lead to system failure or data loss. Ensuring that secure backups of system configuration data and production data are in place and tested is essential to maintaining system integrity. Without proper backups of information, there is greater potential for alteration of data or loss of integrity when attempting to restore a control system/OT environment to an operational state after an incident occurs.
	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	<i>Rationale only provided for High Priority Subcategories</i>
	PR.IP-6: Data is destroyed according to policy	<i>Rationale only provided for High Priority Subcategories</i>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	PR.IP-7: Protection processes are continuously improved	<i>Rationale only provided for High Priority Subcategories</i>
	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	Response plans and recovery plans are fundamental in any organization's security posture to limit the consequences of incidents and maintain or reestablish operations (and system integrity) in the case of an interruption. Establishing a plan of action for rapid response to, and effective recovery from an incident or disaster is paramount in maintaining system integrity.
	PR.IP-10: Response and recovery plans are tested	<i>Rationale only provided for High Priority Subcategories</i>
	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	<i>Rationale only provided for High Priority Subcategories</i>
	PR.IP-12: A vulnerability management plan is developed and implemented	Incorporating a vulnerability management plan into the control system/OT environment is vital in protecting control system/OT assets. Organizations need a systematic method for documenting vulnerabilities, developing a standard remediation timeline and defining periodic and proactive activities for vulnerability detection. Patch management allows for controlled and secure updates that can be tailored for the needs of the control system/OT environment. If vulnerabilities are not detected, documented, and mitigated in a timely manner, there is a much higher potential for an attacker to exploit the control system/OT environment and inhibit system availability.

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Maintenance	<p>PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools</p>	<p><i>Rationale only provided for High Priority Subcategories</i></p>
	<p>PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access</p>	<p>Remote maintenance must be monitored. Like unauthorized physical access, unauthorized remote access to a control system/OT environment for maintenance could result in serious disruption to control system/OT functionality. Any malicious tampering with the control system/OT environment could result in the alteration of data or damage to overall system integrity. As such, remote access to assets must be managed to ensure that system integrity is maintained.</p>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Protective Technology	<p>PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy</p>	<p>The security architecture of a control system/OT must incorporate mechanisms to monitor, log, and audit activities occurring within the control system/OT environment and on control system/OT networks. Auditing and logging activities are imperative to understanding the current state of the control system, validating that the system is operating as intended, and that no policy violations or cyber incidents have hindered the operation of the system. Auditing and logging can help provide indication of a compromised system and can assist in forensic analysis after an incident occurs. Auditing and logging can show irregular or inappropriate user activity, anomalous system activity, or irregular input and output from the control system/OT environment that would indicate damage to system integrity. As such, audit and log records are integral to maintaining system integrity.</p>
	<p>PR.PT-2: Removable media is protected and its use restricted according to policy</p>	<p>Organizations must have specific security requirements for transporting, storing, handling, and erasing or destroying removable media. Loss, theft, destruction, and unintentional distribution of removable media could provide an adversary with valuable data for launching an attack in the control system/OT environment. This data could include machine names, IP addresses, access credentials, and other valuable data useful in planning and executing an attack. Therefore, removable media must be protected and its use restricted to maintain system integrity.</p>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	<i>Rationale only provided for High Priority Subcategories</i>
	PR.PT-4: Communications and control networks are protected	Network security is critical in any control system/OT environment. At minimum, the control system/OT network should be logically separated from the corporate network on physically separate network devices (ideally with a DMZ as an intermediary between the two networks). Communications and control networks both have avenues through which an adversary could impact the integrity of a control system/OT and hinder business operations. Therefore, it is critical to implement protective technologies (e.g., network and host firewalls) to ensure networks are protected from external sources and only explicitly authorized communication and activity occurs.

Detect	Implementing detection measures for continuous monitoring and detection measures for anomalous events of control system/OT environments and data is one of the more critical ways to ensure system integrity. Continuous monitoring allows for rapid detection of inappropriate or malicious activity that could alter both data and system integrity.	
	High Priority Subcategories	Moderate Priority Subcategories
Anomalies and Events	DE.AE-4	DE.AE-1, DE.AE-2, DE.AE-3
Security Continuous Monitoring	DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-4, DE.CM-6, DE.CM-7, DE.CM-8	DE.CM-5
Detection Processes		DE.DP-1, DE.DP-3, DE.DP-4, DE.DP-5

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Anomalies and Events	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	<i>Rationale only provided for High Priority Subcategories</i>
	DE.AE-2: Detected Events are analyzed to understand attack targets and methods	<i>Rationale only provided for High Priority Subcategories</i>
	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	<i>Rationale only provided for High Priority Subcategories</i>
	DE.AE-4: Impact of events is determined	Knowing the impact of events is essential for organizations to prevent events from becoming incidents; to understand the way forward to maintain and recover system integrity; and to mitigate the effects of an incident.
Security Continuous Monitoring	DE.CM-1: The network is monitored to detect potential cybersecurity events	Detecting potential cybersecurity events using appropriate continuous monitoring processes can help defenders break the attack chain before attackers attain their objectives, maintaining system integrity.

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	Monitoring the physical environment for potential cybersecurity events can help defenders break the attack chain before attackers attain their objectives, maintaining system integrity. Due to the nature of control systems'/OT's interaction with the physical world, physical monitoring is essential.
	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	Monitoring personnel activity is of high priority to reduce the possibility and risk of human error, theft, and fraud and their impacts on system integrity by detecting intentional or unintentional misuse of control systems/OT and other informational assets.
	DE.CM-4: Malicious code is detected	Detecting malicious code rapidly before the code can negatively affect a control system/OT is critical for maintaining system integrity. Implementing antivirus tools into a control system/OT environment is essential for malicious code detection. Antivirus tools function effectively when configured against a known state of attack methods and payloads.
	DE.CM-5: Unauthorized mobile code is detected	<i>Rationale only provided for High Priority Subcategories</i>
	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	Monitoring external service provider activity is of high priority to reduce the possibility and risk of human error, theft, and fraud. Intentional or unintentional misuse of control systems/OT by external sources can directly and adversely impact system integrity.

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	Monitoring for unauthorized personnel, connections, devices and software is necessary to validate that the control system/OT environment is operating as intended and that no policy or cyber incidents have hindered system integrity.
	DE.CM-8: Vulnerability scans are performed	Vulnerability scans are a high priority for identifying any weaknesses that can contribute to system integrity risks and mitigation approaches to reduce those risks.
Detection Processes	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	<i>Rationale only provided for High Priority Subcategories</i>
	DE.DP-3: Detection processes are tested	<i>Rationale only provided for High Priority Subcategories</i>
	DE.DP-4: Event detection information is communicated to appropriate parties	<i>Rationale only provided for High Priority Subcategories</i>
	DE.DP-5: Detection processes are continuously improved	<i>Rationale only provided for High Priority Subcategories</i>

Respond Response plan development and execution is critical to maintaining system integrity. Organizations must be prepared contain, mitigate, and understand the impact of incidents as they are an inevitability.

	High Priority Subcategories	Moderate Priority Subcategories
Response Planning	RS.RP-1	
Communications		RS.CO-1, RS.CO-3, RS.CO-4, RS.CO-5
Analysis	RS.AN-2	RS.AN-1, RS.AN-3, RS.AN-4
Mitigation	RS.MI-1, RS.MI-2, RS.MI-3	
Information Protection Process and Procedures		RS.IM-1, RS.IM-2

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Response Planning	RS.RP-1: Response plan is executed during or after an event	An incident response plan is essential documentation consisting of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of incidents against an organization's information systems' integrity. Responding appropriately to incidents can help protect the organization's resources including those that may impact system integrity.
Communications	RS.CO-1: Personnel know their roles and order of operations when a response is needed	<i>Rationale only provided for High Priority Subcategories</i>
	RS.CO-3: Information is shared consistent with response plans	<i>Rationale only provided for High Priority Subcategories</i>
	RS.CO-4: Coordination with stakeholders occurs consistent with response plans.	<i>Rationale only provided for High Priority Subcategories</i>
	RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	<i>Rationale only provided for High Priority Subcategories</i>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Analysis	RS.AN-1: Notifications from detection systems are investigated.	<i>Rationale only provided for High Priority Subcategories</i>
	RS.AN-2: The impact of the incident is understood	Knowing the impact of incidents is essential for organizations to mitigate the incident's effect on system integrity; to understand the way forward to maintain system integrity; to provide a means to compare current state with expected state in a response timeline; and to allow an organization to apply lessons learned in responding to a future incident. This is critical in control system/OT environments as an organization must understand the immediate and long term effects an incident can have on system integrity.
	RS.AN-3: Forensics are performed	<i>Rationale only provided for High Priority Subcategories</i>
	RS.AN-4: Incidents are categorized consistent with response plans	<i>Rationale only provided for High Priority Subcategories</i>
Mitigation	RS.MI-1: The incidents are contained	In any incident response situation, the primary action after detecting a cyber incident is to contain the incident so it cannot spread throughout the organization or to other systems. Effectively contained events and incidents isolate control systems/OT to minimize any damage or impact to DoW information networks, control system/OT components, data, and services by preventing any further contamination, intrusion, or malicious activity. As such, containment is key in ensuring system functionality and maintaining system integrity.

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	RS.MI-2: The incidents are mitigated	It is essential in responding to an incident to follow an appropriate course of action that executes a response plan identifying if eradication is necessary, or should be performed in recovery, to properly mitigate an incident that is adversely affecting system integrity. Any mitigation measures must be carefully considered to ensure that they do not add additional adverse effects to those caused by the incident. If proper mitigation measures are not incorporated into an organization's incident response, the harmful impact an incident could have on system integrity would be indefinite.
	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	A newly identified vulnerability that can result in unauthorized access, use, disclosure, disruption, modification, or destruction of a control system/OT and data is as threatening to an organization or system environment must be mitigated or documented as acceptable risk. Zero day vulnerabilities are a common cause of security breaches and can be exploited by adversaries to affect system integrity until they are mitigated. Once a vulnerability of any kind is discovered, it must be resolved or documented as an accepted risk based on the priorities and risk tolerance of the organization; otherwise, the vulnerability could result in an exploit that could cause catastrophic system failure and damage system integrity.
Improvements	RS.IM-1: Response plans incorporate lessons learned	<i>Rationale only provided for High Priority Subcategories</i>
	RS.IM-2: Response strategies are updated	<i>Rationale only provided for High Priority Subcategories</i>

Recover Effective recovery measures are critical to maintaining system integrity. After an incident occurs, organizations must be able to return to full functionality quickly and they must be able to make improvements based on lessons learned.

	High Priority Subcategories	Moderate Priority Subcategories
Recovery Planning	RC.RP-1	
Improvements		RC.IM-1, RC.IM-2
Communications		RC.CO-3

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Recovery Planning	RC.RP-1: Recovery plan is executed during or after an event	Recovery plans help organizations maintain operational continuity after an adverse event or cyber incident has occurred. The timely restoration (specifying recovery objectives (Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs)) for the various systems and subsystems involved) of systems or assets to full functionality can directly contribute to ensuring that control system/OT environments are operating with sustained integrity at both the system and data level.
Improvements	RC.IM-1: Recovery plans incorporate lessons learned	<i>Rationale only provided for High Priority Subcategories</i>
	RC.IM-2: Recovery strategies are updated	<i>Rationale only provided for High Priority Subcategories</i>
Communications	RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	<i>Rationale only provided for High Priority Subcategories</i>

Mission Objective 3: Maintain Human Safety

Description: Recognizing cybersecurity effects on control systems/OT that impact personnel safety. Preventing injury, including loss of life, through Risk Assessment, Awareness and Training, Protective Technology, and Response Planning.

Organizations Should:

- Have a comprehensive process to systematically predict or identify the operational behavior of each safety-critical failure condition, fault condition, or human error that could lead to a hazard and potential human harm.
- Identify and train personnel on interdependence of cybersecurity with operational responsibilities that impact human safety.
- Implement vulnerability management incident responses measures where cybersecurity adversely affects human safety, in the event of a catastrophic failure/incident.

Identify	Risk assessment processes are the primary methods used to identify procedures, technologies, and equipment that may impact the organization’s ability to maintain human safety. Each organization’s approach to implementing the Cybersecurity Framework Core is based on the decisions made because of risk assessments. For control systems/OT, human safety and fault tolerance to prevent loss of life or endangerment of public health or confidence is a primary concern as opposed to typical IT systems.	
	High Priority Subcategories	Moderate Priority Subcategories
Asset Management	ID.AM-3, ID.AM-5	ID.AM-1
Business Environment	ID.BE-3	
Governance		ID.GV-3
Risk Assessment	ID.RA-3, ID.RA-5, ID.RA-6	ID.RA-1, ID.RA-2
Risk Management Strategy		ID.RM-1, ID.RM-2

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Asset Management	ID.AM-1: Physical devices and systems within the organization are inventoried	<i>Rationale only provided for High Priority Subcategories</i>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	ID.AM-3: Organizational communication and data flows are mapped	Data pathways are becoming increasingly complex and increasingly vulnerable to loss of availability. To mitigate the additional risks to the system environment that comes with additional complexity, it is a high priority to map the organization's data flows. It is essential to do this mapping to identify if a data pathway is at risk of a cyber incident to data-in-transit (e.g., man-in-the-middle attack).
	ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	Prioritizing resources (e.g., hardware, devices, data, and software) based on their classification, criticality, and business value is an essential step in identifying risks and vulnerabilities to the human safety of the organization's control system/OT environment.
Business Environment	ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	Organizational awareness is a critical part of control system/OT personnel incident prevention. Establishing priorities for organizational mission, objectives, and activities that are properly communicated is essential to mitigating social engineering threats by helping personnel be less susceptible to manipulation. In addition, by communicating organizational priorities as they relate to control systems/OT, managers can demonstrate their commitment to, and value of, a cybersecurity program that can solicit valuable input from personnel contributing to the overall personnel safety of the control system/OT environment.

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Governance	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberty obligations, are understood and managed	<i>Rationale only provided for High Priority Subcategories</i>
	ID.RA-1: Asset vulnerabilities are identified and documented	<i>Rationale only provided for High Priority Subcategories</i>
Risk Assessment	ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	<i>Rationale only provided for High Priority Subcategories</i>
	ID.RA-3: Threats, both internal and external, are identified and documented	Identifying and documenting internal and external threats is an imperative step to securing control systems/OT, and mitigating cybersecurity risks. Organizations must identify these threats to control system/OT security throughout the lifecycle of the component control systems/OT from architecture to procurement to installation to maintenance to decommissioning. Due to the rapidly evolving nature of control systems/OT, it is important to identify and review new control system/OT capabilities and their associated emerging threats, particularly to human safety. The identification process should leverage organizations that identify emerging threats such as the ICS-CERT.

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	<p>ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk</p>	<p>It is a high priority that the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation that would result from a failure in control system/OT availability is determined by considering threats, vulnerabilities, and potential impacts as well as existing and planned risk mitigation. If threats, vulnerabilities, likelihoods, and impacts are not used to determine risk, organizations will expose its control systems/OT to multiple, unacceptable risks to human safety.</p>
	<p>ID.RA-6: Risk responses are identified and prioritized</p>	<p>Risk responses differ from incident responses in that actions taken by an organization in responding to incidents are pre-determined and are derived from the information contained in risk responses. Risk responses take into consideration the organization's risk tolerance after identifying a risk and considers the best alternatives for the organization (e.g., acceptance, avoidance, mitigation, sharing or transfer). If risk responses are not identified and prioritized, organizations will accept inappropriate risks to human safety.</p>
Risk Management Strategy	<p>ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders</p>	<p><i>Rationale only provided for High Priority Subcategories</i></p>
	<p>ID.RM-2: Organizational risk tolerance is determined and clearly expressed</p>	<p><i>Rationale only provided for High Priority Subcategories</i></p>

Protect Awareness and training, access control, information protection processes and maintenance were identified as the priority activities. Without necessary training, personnel are not prepared to manage a security incident that could cause human harm. Access control measures are required to ensure only authorized personnel interact with the control system/OT environment. These measures minimize the potential for catastrophic human safety failures in the control system/OT environment.

	High Priority Subcategories	Moderate Priority Subcategories
Access Control	PR.AC-2	
Awareness and Training	PR.AT-1	PR.AT-2, PR.AT-3, PR.AT-4, PR.AT-5
Data Security		PR.DS-7
Information Protection Process and Procedures	PR.IP-5, PR.IP-9	PR.IP-7, PR.IP-10, PR.IP-11, PR.IP-12
Maintenance	PR.MA-1	PR.MA-2
Protective Technology		PR.PT-3, PR.PT-4

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Access Control	PR.AC-2: Physical access to assets is managed and protected	Unauthorized physical access to the control system/OT environment could cause serious disruption to the control system's functionality and could result in endangering personnel. It is important for organizations to limit physical access to control system/OT environments to prevent physical modification, manipulation, or destruction of existing system infrastructure. Because control systems/OT have the ability to interact with the physical world, a system failure could directly cause human harm (e.g., unauthorized access to a control system/OT causing system failure resulting in a fire within the control system/OT facility).

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Awareness and Training	PR.AT-1: All users are informed and trained	A key measure in maintaining human safety within a control system/OT environment is ensuring that all users are informed of the dangers, risks and responsibilities associated with their roles. Proper training is one of the greatest forms of protection when creating a safe control system/OT environment. Human error is a common cause of vulnerability exploitation, security breaches and accidental cyber incidents that can lead to potential human harm. Therefore, all users interacting with the control system/OT environment must receive proper training to maintain a safe control system/OT environment.
	PR.AT-2: Privileged users understand roles & responsibilities	<i>Rationale only provided for High Priority Subcategories</i>
	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	<i>Rationale only provided for High Priority Subcategories</i>
	PR.AT-4: Senior executives understand roles & responsibilities	<i>Rationale only provided for High Priority Subcategories</i>
	PR.AT-5: Physical and information security personnel understand roles & responsibilities	<i>Rationale only provided for High Priority Subcategories</i>
Data Security	PR.DS-7: The development and testing environment(s) are separate from the production environment	<i>Rationale only provided for High Priority Subcategories</i>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Information Protection Process and Procedures	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	Neglecting existing policy and regulations for the physical operating environment of control systems/OT could cause a system failure, producing negative physical impacts such as the release of hazardous materials, damaging kinetic forces (e.g., explosions), and exposure to energy sources (e.g., electricity). Meeting the required regulations for control system/OT environments can help protect against catastrophic system failure, which could directly result in human harm.
	PR.IP-7: Protection processes are continuously improved	<i>Rationale only provided for High Priority Subcategories</i>
	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	Response plans and recovery plans are fundamental in any organization's security posture to limit the consequences of incidents and maintain or reestablish operations in the case of an interruption. Establishing a plan of action for rapid response to, and effective recovery from an incident or disaster is paramount in maintaining human safety.
	PR.IP-10: Response and recovery plans are tested	<i>Rationale only provided for High Priority Subcategories</i>
	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	<i>Rationale only provided for High Priority Subcategories</i>
	PR.IP-12: A vulnerability management plan is developed and implemented	<i>Rationale only provided for High Priority Subcategories</i>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Maintenance	PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	It is essential in maintaining human safety to ensure that all physical safeguards are properly maintained and repaired if necessary. Neglecting proper maintenance of physical assets with approved and controlled tools could leave a control system/OT environment exposed to potentially critical exploits. Therefore, ensuring that physical organizational assets are maintained, and the maintenance is documented in a timely manner.
	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	<i>Rationale only provided for High Priority Subcategories.</i>
Protective Technology	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	<i>Rationale only provided for High Priority Subcategories</i>
	PR.PT-4: Communications and control networks are protected	<i>Rationale only provided for High Priority Subcategories</i>

Detect	Implementing detection measures for continuous monitoring of control system/OT environments is critical to ensuring human safety. Continuous monitoring for anomalous events allows for rapid detection of inappropriate or malicious activity from a threat actor that could directly lead to a system failure, resulting in harm to personnel.	
	High Priority Subcategories	Moderate Priority Subcategories
Anomalies and Events	DE.AE-4	DE.AE-2, DE.AE-3, DE.AE-5
Security Continuous Monitoring	DE.CM-3, DE.CM-7	DE.CM-2
Detection Processes		DE.DP-1, DE.DP-4, DE.DP-5

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Anomalies and Events	DE.AE-2: Detected Events are analyzed to understand attack targets and methods	<i>Rationale only provided for High Priority Subcategories</i>
	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	<i>Rationale only provided for High Priority Subcategories</i>
	DE.AE-4: Impact of events is determined	Knowing the impact of events is essential for organizations to prevent events from becoming incidents; to understand the way forward to maintain human safety; and to mitigate the effects of an incident.
	DE.AE-5: Incident alert thresholds are established	<i>Rationale only provided for High Priority Subcategories</i>
Security Continuous Monitoring	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	<i>Rationale only provided for High Priority Subcategories</i>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	Monitoring personnel activity is of high priority to reduce the possibility and risk of human error, theft, and fraud and their impacts on human safety by detecting intentional or unintentional misuse of control systems/OT and other informational assets.
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	Monitoring for unauthorized personnel, connections, devices and software is necessary to validate that the control system/OT environment is operating as intended and that no policy or cyber incidents have occurred to threaten human safety.
Detection Processes	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	<i>Rationale only provided for High Priority Subcategories</i>
	DE.DP-4: Event detection information is communicated to appropriate parties	<i>Rationale only provided for High Priority Subcategories</i>
	DE.DP-5: Detection processes are continuously improved	<i>Rationale only provided for High Priority Subcategories</i>

Respond Response plan development and execution is critical in the response phase of maintaining human safety. Personnel must be prepared to execute response procedures based on various incident scenarios and organizations must be prepared to contain, mitigate, and understand the impact of incidents as they are an inevitability.

	High Priority Subcategories	Moderate Priority Subcategories
Response Planning	RS.RP-1	
Communications	RS.CO-1	RS.CO-3
Analysis	RS.AN-2	RS.AN-1, RS.AN-4
Mitigation	RS.MI-1, RS.MI-2, RS.MI-3	
Information Protection Process and Procedures		RS.IM-1, RS.IM-2

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Response Planning	RS.RP-1: Response plan is executed during or after an event	An incident response plan is essential documentation consisting of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of incidents. Responding appropriately to incidents can help protect the organization's resources including those that may impact human safety.
Communications	RS.CO-1: Personnel know their roles and order of operations when a response is needed	In the event of an incident with life and death consequences, control system/OT personnel need to know their designated roles and the proper response measures. Individuals must know the correct procedures to ensure their own safety before notifying the necessary parties. A lack of awareness of these planned response measures can lead to unnecessary and avoidable harm, highlighting the critical importance of knowing one's role and proper planning to mitigate the incident.
	RS.CO-3: Information is shared consistent with response plans	<i>Rationale only provided for High Priority Subcategories</i>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Analysis	RS.AN-1: Notifications from detection systems are investigated.	<i>Rationale only provided for High Priority Subcategories</i>
	RS.AN-2: The impact of the incident is understood	Knowing the impact of incidents is essential for organizations to mitigate the incident's effect on human safety; to understand the way forward to maintain human safety; to provide a means to compare current state with expected state in a response timeline; and to allow an organization to apply lessons learned in responding to a future incident. This is critical in control system/OT environments as an organization must understand the immediate and long-term effects an incident can have on human safety.
	RS.AN-4: Incidents are categorized consistent with response plans	<i>Rationale only provided for High Priority Subcategories</i>
Mitigation	RS.MI-1: The incidents are contained	In any incident response situation, the primary action upon detecting a cyber incident is to contain the incident so it cannot spread throughout the organization or to other systems. If an incident has the potential to cause harm to personnel (e.g., fire in a control systems/OT facility), it is particularly important to ensure that the incident is rapidly contained.

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	RS.MI-2: The incidents are mitigated	It is essential to mitigate an incident that can cause catastrophic harm to human safety. A properly mitigated incident from a human safety context is absent of unacceptable risk of physical injury or damage to the health of personnel. Appropriate mitigation may include non-cyber, mechanical solutions to a cyber security problem. Many safety-critical systems are designed with redundancy which cybersecurity engineers can leverage in mitigating an incident. Within the control system/OT environment, an incident must be mitigated as quickly as possible to minimize the negative impacts, particularly when the incident causes harm to personnel.
	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	A newly identified vulnerability that can result in unauthorized access, use, disclosure, disruption, modification, or destruction of a control system/OT and data that poses a threat to human safety must be mitigated or documented as acceptable risk. Zero-day vulnerabilities are a common cause of security breaches and can be exploited by adversaries until they are mitigated. Once a vulnerability of any kind is discovered, it must be resolved or documented as an accepted risk based on the priorities and risk tolerance of the organization; otherwise, the vulnerability could result in an exploit that could cause catastrophic system failure and threaten human safety.
Improvements	RS.IM-1: Response plans incorporate lessons learned	<i>Rationale only provided for High Priority Subcategories</i>
	RS.IM-2: Response strategies are updated	<i>Rationale only provided for High Priority Subcategories</i>

Recover		
Effective recovery measures are critical to ensuring human safety in a control system/OT environment. After an incident occurs, organizations must be able to protect their personnel and they must be able to make organizational improvements based on lessons learned.		
	High Priority Subcategories	Moderate Priority Subcategories
Recovery Planning	RC.RP-1	
Improvements		RC.IM-1, RC.IM-2
Communications		RC.CO-1; RC.CO-2, RC.CO-3

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Recovery Planning	RC.RP-1: Recovery plan is executed during or after an event	Recovery plans help organizations maintain operational continuity after an adverse event or cyber incident has occurred. Ensuring that an organization has pre-defined activities in place that specify recovery objectives (Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs)) for the various systems and subsystems involved, based on typical business need, to restore functionality is essential to maintaining personnel safety.
Improvements	RC.IM-1: Recovery plans incorporate lessons learned	<i>Rationale only provided for High Priority Subcategories</i>
	RC.IM-2: Recovery strategies are updated	<i>Rationale only provided for High Priority Subcategories</i>
Communications	RC.CO-1: Public relations are managed	<i>Rationale only provided for High Priority Subcategories</i>
	RC.CO-2: Reputation after an event is repaired	<i>Rationale only provided for High Priority Subcategories.</i>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	<i>Rationale only provided for High Priority Subcategories</i>

Mission Objective 4: Maintain Environmental Safety

Description: Recognizing cybersecurity effects on control systems/OT that impact environmental safety. Preventing harm to the environment through Governance, Risk Assessment, Awareness and Training, and Response Planning.

Organizations Should:

- Have a comprehensive process to systematically predict or identify the operational behavior of each safety-critical failure condition, fault condition, or human error that could lead to a hazard and potential environmental harm.
- Identify and train personnel on interdependence of cybersecurity with operational responsibilities that impact environmental safety.
- Implement detect, respond, recover measures where cybersecurity adversely affects environmental safety, in the event of a catastrophic failure/incident.

Identify

Risk assessment processes are the primary methods used to identify procedures, technologies, and equipment that may impact the organization's ability to maintain environmental safety. Each organization's approach to implementing the Cybersecurity Framework Core is based on the decisions made because of risk assessments. Control systems/OT often have specific environmental requirements (e.g. manufacturing process may require precise temperature), or they may be tied to their physical environment for operations. Such requirements and constraints must be identified so the risks arising from those constraints can be mitigated.

	High Priority Subcategories	Moderate Priority Subcategories
Asset Management	ID.AM-5	ID.AM-1
Business Environment		ID.BE-2, ID.BE-3
Governance		
Risk Assessment	ID.RA-3, ID.RA-5, ID.RA-6	ID.RA-1, ID.RA-2
Risk Management Strategy		ID.RM-2

Detailed Specifications

Category	Subcategory	Rationale for High Priority
Asset Management	ID.AM-1: Physical devices and systems within the organization are inventoried	<i>Rationale only provided for High Priority Subcategories</i>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	Prioritizing resources (e.g., hardware, devices, data, and software) based on their classification, criticality, and business value is an essential step in identifying risks and vulnerabilities to the environmental safety of the organization's control system/OT environment.
Business Environment	ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	<i>Rationale only provided for High Priority Subcategories</i>
	ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	<i>Rationale only provided for High Priority Subcategories</i>
Risk Assessment	ID.RA-1: Asset vulnerabilities are identified and documented	<i>Rationale only provided for High Priority Subcategories</i>
	ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	<i>Rationale only provided for High Priority Subcategories</i>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	ID.RA-3: Threats, both internal and external, are identified and documented	Identifying and documenting internal and external threats is an imperative step to securing control systems/OT and mitigating cybersecurity risks. Organizations must identify these threats to control system/OT security throughout the lifecycle of the control systems/OT from architecture to procurement to installation to maintenance to decommissioning. Due to the rapidly evolving nature of control systems/OT, it is important to identify and review new control system/OT capabilities and their associated emerging threats, particularly to environmental safety. The identification process should leverage organizations that identify emerging threats such as the ICS-CERT.
	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	It is a high priority that the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation that would result from a failure in control system/OT availability is determined by considering threats, vulnerabilities, and potential impacts as well as existing and planned risk mitigation. If threats, vulnerabilities, likelihoods, and impacts are not used to determine risk, organizations will expose its control systems/OT to multiple, unacceptable risks to environmental safety.

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	ID.RA-6: Risk responses are identified and prioritized	Prioritizing risks is high importance for all business/mission requirements. In general, identification and prioritization of risks has a high importance. As such, ensuring that risk responses are identified and prioritized are critical in maintaining environmental safety.
Risk Management Strategy	ID.RM-2: Organizational risk tolerance is determined and clearly expressed	<i>Rationale only provided for High Priority Subcategories</i>

Protect

Awareness and training, access control, information protection processes and maintenance were identified as the priority activities. Without necessary training, personnel are not prepared to manage a personnel security incident. Access control measures are required to ensure only authorized personnel interact with the control system/OT environment. These measures minimize the potential for system failure that could result in harm to the environment.

	High Priority Subcategories	Moderate Priority Subcategories
Access Control	PR.AC-2	
Awareness and Training	PR.AT-1	PR.AT-2, PR.AT-3, PR.AT-4, PR.AT-5
Data Security		PR.DS-7
Information Protection Process and Procedures	PR.IP-5, PR.IP-9	PR.IP-7, PR.IP-10, PR.IP-11, PR.IP-12
Maintenance	PR.MA-1	PR.MA-2
Protective Technology		PR.PT-3, PR.PT-4

Detailed Specifications

Category	Subcategory	Rationale for High Priority
Access Control	PR.AC-2: Physical access to assets is managed and protected	Unauthorized physical access to the control system/OT environment could cause serious disruption to the control system's functionality and could result in damage to the environment. It is important for organizations to limit physical access to control system/OT environments to prevent physical modification, manipulation, or destruction of existing system infrastructure. Because control systems/OT have the ability to interact with the physical world, a system failure could directly cause environmental harm (e.g., unauthorized access to a control system/OT causing system failure resulting in a chemical spill that contaminates a water source).

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Awareness and Training	PR.AT-1: All users are informed and trained	A key measure in maintaining environmental safety within a control system/OT environment is ensuring that all users are informed of the dangers, risks and responsibilities associated with their roles. Proper training is one of the greatest forms of protection when creating a safe control system/OT environment. Human error is a common cause of vulnerability exploitation, security breaches and accidental cyber incidents that can lead to potential environmental harm. Therefore, all users interacting with the control system/OT environment must receive proper training to maintain a safe control system/OT environment.
	PR.AT-2: Privileged users understand roles & responsibilities	<i>Rationale only provided for High Priority Subcategories</i>
	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	<i>Rationale only provided for High Priority Subcategories</i>
	PR.AT-4: Senior executives understand roles & responsibilities	<i>Rationale only provided for High Priority Subcategories</i>
	PR.AT-5: Physical and information security personnel understand roles & responsibilities	<i>Rationale only provided for High Priority Subcategories</i>
Data Security	PR.DS-7: The development and testing environment(s) are separate from the production environment	<i>Rationale only provided for High Priority Subcategories</i>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Information Protection Process and Procedures	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	Neglecting existing policy and regulations for the physical operating environment of control systems/OT could cause a system failure, producing negative physical impacts such as the release of hazardous materials, damaging kinetic forces (e.g., explosions), and exposure to energy sources (e.g., electricity). Meeting the required regulations for control system/OT environments can help protect against catastrophic system failure, which could directly result in damage to the environment.
	PR.IP-7: Protection processes are continuously improved	<i>Rationale only provided for High Priority Subcategories</i>
	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	Response plans and recovery plans are fundamental in any organization's security posture to limit the consequences of incidents and maintain or reestablish operations in the case of an interruption. Establishing a plan of action for rapid response to, and effective recovery from an incident or disaster is paramount in maintaining environmental safety.
	PR.IP-10: Response and recovery plans are tested	<i>Rationale only provided for High Priority Subcategories</i>
	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	<i>Rationale only provided for High Priority Subcategories</i>
	PR.IP-12: A vulnerability management plan is developed and implemented	<i>Rationale only provided for High Priority Subcategories</i>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Maintenance	PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	<i>Rationale only provided for High Priority Subcategories</i>
	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	Remote maintenance must be monitored. Like unauthorized physical access, unauthorized remote access to a control system/OT environment for maintenance could result in serious disruption to control system/OT functionality. Because control systems/OT have the ability to interact with the physical world, malicious tampering could cause harm to the environment. As such, remote interaction with the control system/OT environment must be approved and logged.
Protective Technology	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	<i>Rationale only provided for High Priority Subcategories</i>
	PR.PT-4: Communications and control networks are protected	<i>Rationale only provided for High Priority Subcategories</i>

Detect	Implementing detection measures for anomalies and events of control system/OT environments is critical to ensuring environmental safety. Continuous monitoring allows for rapid detection of inappropriate or malicious activity from a threat actor that could directly lead to a system failure, resulting in harm to the environment.	
	High Priority Subcategories	Moderate Priority Subcategories
Anomalies and Events	DE.AE-4	DE.AE-2, DE.AE-3, DE.AE-5
Security Continuous Monitoring		DE.CM-2, DE.CM-3, DE.CM-7
Detection Processes		DE.DP-1, DE.DP-4, DE.DP-5

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Anomalies and Events	DE.AE-2: Detected Events are analyzed to understand attack targets and methods	<i>Rationale only provided for High Priority Subcategories</i>
	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	<i>Rationale only provided for High Priority Subcategories</i>
	DE.AE-4: Impact of events is determined	Knowing the impact of events is essential for organizations to prevent events from becoming incidents; to understand the way forward to maintain human safety; and to mitigate the effects of an incident.
	DE.AE-5: Incident alert thresholds are established	<i>Rationale only provided for High Priority Subcategories</i>
Security Continuous Monitoring	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	<i>Rationale only provided for High Priority Subcategories</i>
	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	<i>Rationale only provided for High Priority Subcategories</i>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	<i>Rationale only provided for High Priority Subcategories</i>
Detection Processes	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	<i>Rationale only provided for High Priority Subcategories</i>
	DE.DP-4: Event detection information is communicated to appropriate parties	<i>Rationale only provided for High Priority Subcategories</i>
	DE.DP-5: Detection processes are continuously improved	<i>Rationale only provided for High Priority Subcategories</i>

Respond Proper response plan development and execution is critical in the response phase of maintaining environmental safety. Organizations must be prepared to analyze and mitigate any control system/OT environment vulnerability or flaw that could relate to potential environmental harm.

Category	High Priority Subcategories	Moderate Priority Subcategories
Response Planning	RS.RP-1	
Communications		RS.CO-3
Analysis	RS.AN-2	RS.AN-4
Mitigation	RS.MI-1, RS.MI-2, RS.MI-3	
Information Protection Process and Procedures		RS.IM-1, RS.IM-2

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Response Planning	RS.RP-1: Response plan is executed during or after an event	An incident response plan is essential documentation consisting of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of incidents. Responding appropriately to incidents can help protect the organization's resources, including those that may impact environmental safety.
Communications	RS.CO-3: Information is shared consistent with response plans	<i>Rationale only provided for High Priority Subcategories</i>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Analysis	RS.AN-2: The impact of the incident is understood	Knowing the impact of incidents is essential for organizations to mitigate the incident's effect on environmental safety; to understand the way forward to maintain environmental safety; to provide a means to compare current state with expected state in a response timeline; and to allow an organization to apply lessons learned in responding to a future incident. This is critical in control system/OT environments as an organization must understand the immediate and long-term effects an incident can have on environmental safety.
	RS.AN-4: Incidents are categorized consistent with response plans	<i>Rationale only provided for High Priority Subcategories</i>
Mitigation	RS.MI-1: The incidents are contained	In any incident response situation, the primary action upon detecting a cyber incident is to contain the incident so it cannot spread throughout the organization or to other systems. If an incident has the potential to cause harm to the environment (e.g., control system/OT failure that leads to a chemical spill), it is particularly important to ensure that the incident is rapidly contained.

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	RS.MI-2: The incidents are mitigated	It is essential to mitigate an incident that can cause catastrophic harm to environmental safety. A properly mitigated incident from an environmental safety context is absent of unacceptable risk to the environment. Many safety-critical systems are designed with redundancy which cybersecurity engineers can leverage in mitigating an incident. Within the control system/OT environment, an incident must be mitigated as quickly as possible to minimize the negative impacts, particularly when the incident causes harm to the environment.
	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	A newly identified vulnerability that can result in unauthorized access, use, disclosure, disruption, modification, or destruction of a control system/OT must be mitigated or documented as acceptable risk. Zero-day vulnerabilities are a common cause of security breaches and can be exploited by adversaries until they are mitigated. Once a vulnerability of any kind is discovered, it must be resolved or documented as an accepted risk based on the priorities and risk tolerance of the organization; otherwise, the vulnerability could result in an exploit that could cause catastrophic system failure and threaten environmental safety.
Improvements	RS.IM-1: Response plans incorporate lessons learned	<i>Rationale only provided for High Priority Subcategories</i>
	RS.IM-2: Response strategies are updated	<i>Rationale only provided for High Priority Subcategories</i>

Recover

Effective recovery measures are critical to ensuring environmental safety in a control system/OT environment. After an incident occurs, organizations must be able to protect their personnel, and they must be able to make organizational improvements based on lessons learned.

	High Priority Subcategories	Moderate Priority Subcategories
Recovery Planning	RC.RP-1	
Improvements		RC.IM-1, RC.IM-2
Communications		RC.CO-3

Detailed Specifications

Category	Subcategory	Rationale for High Priority
Recovery Planning	RC.RP-1: Recovery plan is executed during or after an event	Recovery plans help organizations maintain operational continuity after an adverse event or cyber incident has occurred. Ensuring that an organization has pre-defined activities in place that specify recovery objectives (Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs)) for the various systems and subsystems involved, based on typical business need, to restore functionality is essential to maintaining environmental safety.
Improvements	RC.IM-1: Recovery plans incorporate lessons learned	<i>Rationale only provided for High Priority Subcategories</i>
	RC.IM-2: Recovery strategies are updated	<i>Rationale only provided for High Priority Subcategories</i>
Communications	RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	<i>Rationale only provided for High Priority Subcategories</i>

Mission Objective 5: Maintain Physical Security

Description: Recognizing and securing physical controls that impact control systems/OT. Preventing unauthorized access to a control system/OT environment and preventing unauthorized damage or tampering with physical assets directly related to the control system/OT environment.

Organizations Should:

- Identify physical assets and security controls that directly relate to maintaining continuity of operations of the control system.
- Identify the cybersecurity risks associated with physical assets that could threaten control system/OT functionality.
- Incorporate outcomes of Cybersecurity risk assessments that require an analysis of potential exploitation of vulnerabilities by a malicious actor.
- Incorporate outcomes of Cybersecurity risk assessments that account for adverse impacts on system functionality that may be the byproduct of system operations.
- Reduce the risk of accidental or deliberate loss or damage to plant assets surrounding the control system/OT environment.
- Apply Continuous Monitoring to physical assets associated with the control system/OT security to ensure that there is no deliberate or accidental unauthorized manipulation or tampering of the physical environment.
- Ensure that physical security personnel understand the relative risks and physical security countermeasures associated with the control system/OT environments they protect.
- Ensure that physical security personnel are aware of which areas of a control system/OT production environment house data acquisition and operate in sensitive spaces.
- Mitigate business continuity risk by specifying immediate response plans in the event that physical safety is jeopardized.

Identify	Risk assessment processes are the primary methods used to identify procedures, technologies, and equipment that may impact the organization's ability to maintain physical safety. Each organization's approach to implementing the Cybersecurity Framework Core is based on the decisions made because of risk assessments. Control systems/OT and control system/OT environments are particularly vulnerable to physical tampering by a malicious actor. As such, access management along with proper governance and policy are crucial in ensuring that physical safety is maintained.	
	High Priority Subcategories	Moderate Priority Subcategories
Asset Management	ID.AM-1, ID.AM-4, ID.AM-5	ID.AM-6
Business Environment	ID.BE-5	ID.BE-2, ID.BE-3, ID.BE-4
Governance	ID.GV-4	ID.GV-1, ID.GV-2, ID.GV-3
Risk Assessment	ID.RA-3, ID.RA-5, ID.RA-6	ID.RA-1, ID.RA-2, ID.RA-4
Risk Management Strategy		ID.RM-1, ID.RM-2, ID.RM-3

Unclassified

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Asset Management	ID.AM-1: Physical devices and systems within the organization are inventoried	It is essential that physical devices are inventoried and accounted for when maintaining physical safety of the control system/OT environment. To properly protect critical IT and control system/OT assets, these assets must first be identified and documented. Otherwise, there could be malicious or accidental tampering with physical assets without the knowledge of those responsible for maintaining physical security.

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	ID.AM-4: External information systems are catalogued	It is essential for organizations to comply with DoWI 8510.01's external IT service requirements that external information systems are catalogued. DoW organizations that use external IT services provided by a commercial or other nonfederal government entity must ensure the security protections of the information system delivering the service is appropriate to the availability needs of the DoW organization's information and mission. Moreover, the physical tampering with or damaging of external assets can also have detrimental effects on the control system/OT environment. Therefore, it is crucial to ensure that all external information systems are catalogued for maintaining physical safety.
	ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	Prioritizing resources (e.g., hardware, devices, data, and software) based on their classification, criticality, and business value is an essential step in identifying physical risks and vulnerabilities to the control system/OT environment.
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	<i>Rationale only provided for High Priority Subcategories</i>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Business Environment	ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	<i>Rationale only provided for High Priority Subcategories</i>
	ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	<i>Rationale only provided for High Priority Subcategories</i>
	ID.BE-4: Dependencies and critical functions for delivery of critical services are established	<i>Rationale only provided for High Priority Subcategories</i>
	ID.BE-5: Resilience requirements to support delivery of critical services are established	Due to the potential costs and impact a physically tampered with or damaged system can have on continuity of operations, restoring production or product conditions to a past, successful state is necessary in maintaining system functionality and business continuity. Without the resilience requirements, organizations run the risk of an intolerable absence of functionality in the control system/OT environment and a risk to critical mission/business objectives.

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Governance	ID.GV-1: Organizational information security policy is established	<i>Rationale only provided for High Priority Subcategories</i>
	ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	<i>Rationale only provided for High Priority Subcategories</i>
	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberty obligations, are understood and managed	<i>Rationale only provided for High Priority Subcategories</i>
	ID.GV-4: Governance and risk management processes address cybersecurity risks	It is DoW policy that: the DoW will establish and use an integrated enterprise-wide decision structure for cybersecurity risk management (the RMF) that includes and integrates DoW mission areas (MAs) pursuant to DoWD 8115.01. Without a governance and risk management process that address cybersecurity risks, organizations run the unacceptable risk of having either no protection of control systems/OT or an ad-hoc, disparate policy that is not aligned with overall physical safety requirements of the control system/OT environment.

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Risk Assessment	ID.RA-1: Asset vulnerabilities are identified and documented	<i>Rationale only provided for High Priority Subcategories</i>
	ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	<i>Rationale only provided for High Priority Subcategories</i>
	ID.RA-3: Threats, both internal and external, are identified and documented	Identifying and documenting internal and external threats is an imperative step to securing control systems/OT and mitigating cybersecurity risks. Organizations must identify these threats to control system/OT security throughout the lifecycle of the control system. Due to the rapidly evolving nature of control systems/OT, it is important to identify and review new control system/OT capabilities and their associated emerging threats. This includes analyzing flaws and vulnerabilities to physical controls as they are critical in securing the control system/OT environment.
	ID.RA-4: Potential business impacts and likelihoods are identified	<i>Rationale only provided for High Priority Subcategories</i>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	<p>ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk</p>	<p>It is a high priority that the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation that would result from a failure in control system/OT availability is determined by considering all physical threats, vulnerabilities, and potential impacts as well as existing and planned risk mitigation. If threats, vulnerabilities, likelihoods, and impacts are not used to determine risk, organizations will expose its control system/OT environment to unacceptable risks. Therefore, analyzing and determining physical safety is critical in ensuring the secure implementation of a control system/OT environment.</p>
	<p>ID.RA-6: Risk responses are identified and prioritized</p>	<p>Risk responses differ from incident responses in that actions taken by an organization in responding to incidents are pre-determined and are derived from the information contained in risk responses. Risk responses take into consideration the organization's risk tolerance after identifying a risk. If risk responses are not identified and prioritized regarding physical controls and safeguards for control system/OT assets, organizations will accept inappropriate risks to business continuity.</p>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Risk Management Strategy	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	<i>Rationale only provided for High Priority Subcategories</i>
	ID.RM-2: Organizational risk tolerance is determined and clearly expressed	<i>Rationale only provided for High Priority Subcategories</i>
	ID.RM-3: The organization’s determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	<i>Rationale only provided for High Priority Subcategories</i>

Protect

For control systems/OT, security protections must be implemented with a focus on maintaining system integrity due to the high potential impact on the control system/OT environment from a loss of integrity. These protection strategies to mitigate risks include maintaining strong access control measures; protecting data in-transit and at-rest; employing comprehensive information protection processes and procedures; ensuring maintenance and repairs are performed consistent with policies and procedures; and deploying technical security solutions (e.g., strong auditing and log management tools) to maintain the security and integrity of the control system/OT environment.

	High Priority Subcategories	Moderate Priority Subcategories
Access Control	PR.AC-1, PR.AC-2, PR.AC-4	PR.AC-3, PR.AC-5
Awareness and Training	PR.AT-1, PR.AT-5	PR.AT-2, PR.AT-3, PR.AT-4,
Data Security		PR.DS-3 PR.DS-4, PR.DS-5, PR.DS-7
Information Protection Process and Procedures	PR.IP-3, PR.IP-5, PR.IP-9, PR.IP-12	PR.IP-2, PR.IP-7, PR.IP-10, PR.IP-11
Maintenance	PR.MA-1	PR.MA-2
Protective Technology	PR.PT-3	PR.PT-2, PR.PT-4

Detailed Specifications

Category	Subcategory	Rationale for High Priority
Access Control	PR.AC-1: Identities and credentials are managed for unauthorized devices and users	Unauthorized access to the control system/OT environment could allow a malicious actor to alter the configuration of a system, manipulate system data, or physically damage the system itself. As such, organizations must implement physical security procedures for identifying and authenticating users, processes, and devices for approved business functions. Without implementing physical access control safeguards, the attack surface area in the control system/OT environment is unacceptable. Ensuring that only authorized users access systems for approved uses is critical in maintaining physical security.

Unclassified

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	PR.AC-2: Physical access to assets is managed and protected	Unauthorized physical access to the control system/OT environment could cause serious disruption to the control system's functionality and could result in a loss of system functionality. It is important for organizations to limit physical access to control system/OT environments to prevent physical modification, manipulation, or destruction of existing system infrastructure. Any malicious tampering with the control system/OT environment could result in system failure or interruption of business operations. As such, physical access to assets must be securely managed.
	PR.AC-3: Remote access is managed	<i>Rationale only provided for High Priority Subcategories</i>
	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	Incorporating least privilege is allowing only authorized accesses for users which are necessary to accomplish the assigned tasks in accordance with organizational missions and business functions. Separation of duties is requiring more than one person to complete a task so as to prevent fraud and human error. These role-based measures are particularly helpful in a control system/OT environment to prevent any accidental or intentional physical tampering of a control system/OT environment could lead to system failure and hinder business continuity.
	PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	<i>Rationale only provided for High Priority Subcategories</i>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Awareness and Training	PR.AT-1: All users are informed and trained	A key measure in maintaining the physical safety of a control system/OT environment is ensuring that all users are informed of the dangers, risks and responsibilities associated with their roles. Proper training is one of the greatest forms of protection when creating a safe control system/OT environment. Human error is a common cause of vulnerability exploitation, security breaches and accidental cyber incidents that can lead to the halting of business operations. Therefore, all users involved in the physical protection of control system-related assets must receive proper training to maintain a secure control system/OT environment.
	PR.AT-2: Privileged users understand roles & responsibilities	<i>Rationale only provided for High Priority Subcategories</i>
	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	<i>Rationale only provided for High Priority Subcategories</i>
	PR.AT-4: Senior executives understand roles & responsibilities	<i>Rationale only provided for High Priority Subcategories</i>
	PR.AT-5: Physical and information security personnel understand roles & responsibilities	Physical security personnel understanding their roles is a high priority for maintaining physical security. If personnel are not informed of the systems they are protecting and what they are doing to protect them, they may not understand what to look for in an adversary attempting to compromise the control system/OT environment.

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Data Security	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	<i>Rationale only provided for High Priority Subcategories</i>
	PR.DS-4: Adequate capacity to ensure availability is maintained	<i>Rationale only provided for High Priority Subcategories</i>
	PR.DS-5: Protections against data leaks are implemented	<i>Rationale only provided for High Priority Subcategories</i>
	PR.DS-7: The development and testing environment(s) are separate from the production environment	<i>Rationale only provided for High Priority Subcategories</i>
Information Protection Process and Procedures	PR.IP-2: A System Development Life Cycle to manage systems is implemented	<i>Rationale only provided for High Priority Subcategories</i>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	PR.IP-3: Configuration change control processes are in place	<p>A lack of configuration change management procedures can lead to security oversights, exposures, and risks that can harm a control system/OT environment. Vulnerabilities typically arise when the configuration of a system or environment changes. Particularly regarding physical controls, any alteration to a control system/OT environment, must be documented and tested.</p> <p>Neglecting configuration change control processes to physical controls could lead to a critical physical access vulnerability, allowing a malicious actor to easily cause physical damage within the control system/OT environment.</p>
	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	<p>Neglecting existing policy and regulations for the physical operating environment of control systems/OT could cause a system failure, producing negative physical impacts such as the release of hazardous materials, damaging kinetic forces (e.g., explosions), and exposure to energy sources (e.g., electricity). Meeting the required regulations for control system/OT environments can help protect against catastrophic system failure, irreparable tampering of physical systems due to lack of physical safeguards, and damage to the environment. As such, it is essential in maintaining physical safety that the proper policies and regulations are met.</p>
	PR.IP-7: Protection processes are continuously improved	<i>Rationale only provided for High Priority Subcategories</i>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	Response plans and recovery plans are fundamental in any organization's security posture to limit the consequences of incidents and maintain or reestablish operations in the case of an interruption. Establishing a plan of action for rapid response to, and effective recovery from an incident or disaster is paramount in maintaining physical safety.
	PR.IP-10: Response and recovery plans are tested	<i>Rationale only provided for High Priority Subcategories</i>
	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	<i>Rationale only provided for High Priority Subcategories</i>
	PR.IP-12: A vulnerability management plan is developed and implemented	Incorporating a vulnerability management plan into the control system/OT environment is vital in protecting control system/OT assets. Organizations need a systematic method for documenting vulnerabilities, developing a standard remediation timeline and defining periodic and proactive activities for vulnerability detection. Particularly regarding physical safeguards, any documented vulnerability needs to be rapidly addressed and mitigated; otherwise, the control system/OT environment could be susceptible to physical damage by a malicious actor. Ensuring that vulnerabilities are managed minimizes the potential for system exploits and supporting the mission objective.

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Maintenance	PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	It is essential in maintaining physical security to ensure that all physical safeguards are properly maintained and repaired if necessary. Neglecting proper maintenance of physical assets with approved and controlled tools could leave a control system environment exposed to potentially critical exploits. Therefore, ensuring that physical organizational assets are maintained, and the maintenance is documented in a timely manner.
	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	<i>Rationale only provided for High Priority Subcategories</i>
Protective Technology	PR.PT-2: Removable media is protected and its use restricted according to policy	<i>Rationale only provided for High Priority Subcategories</i>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	<p>PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality</p>	<p>The principle of least functionality provides that a system is configured to execute only essential capabilities and to prohibit the use of non-essential functions that are not integral to the operation of the system. Incorporating the principle of least functionality on top of protective measures against unauthorized physical access further aids in protecting a control system/OT environment. As aforementioned, unauthorized access to a control system/OT environment can lead to catastrophic system failure, which inhibits system functionality and business continuity. Incorporating the principle of least functionality aids in minimizing the damage that an attacker can cause to a control system/OT environment if they were able to gain unauthorized physical access.</p>
	<p>PR.PT-4: Communications and control networks are protected</p>	<p><i>Rationale only provided for High Priority Subcategories</i></p>

Detect		
Implementing detection measures for anomalous events related to control system/OT environments is critical in ensuring that physical safety is maintained. Continuous monitoring allows for rapid detection of inappropriate or malicious activity from a threat actor to physical equipment and assets in and around a control system/OT facility.		
	High Priority Subcategories	Moderate Priority Subcategories
Anomalies and Events	DE.AE-4	DE.AE-2, DE.AE-3, DE.AE-5
Security Continuous Monitoring	DE.CM-2, DE.CM-3; DE.CM-7	DE.CM-6,
Detection Processes		DE.DP-1, DE.DP-3, DE.DP-4, DE.DP-5

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Anomalies and Events	DE.AE-2: Detected Events are analyzed to understand attack targets and methods	<i>Rationale only provided for High Priority Subcategories</i>
	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	<i>Rationale only provided for High Priority Subcategories</i>
	DE.AE-4: Impact of events is determined	Knowing the impact of events is essential for organizations to prevent events from recurring or escalating in severity; to understand the way forward in maintaining physical safety; and to mitigate the effects of an incident.
	DE.AE-5: Incident alert thresholds are established	<i>Rationale only provided for High Priority Subcategories</i>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Security Continuous Monitoring	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	Monitoring the physical environment is essential in protecting all critical assets of a control system/OT environment. Due to the nature of control systems'/OT's interactions with the physical world, physical monitoring is a vital aspect of maintaining physical safety.
	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	Monitoring personnel activity is of high priority to reduce the possibility and risk of human error, theft, fraud, and malicious tampering or damaging of physical assets directly related to the control system/OT environment. It is essential for maintaining physical safety that proper monitoring mechanisms exist throughout a control system/OT facility to ensure that personnel are only carrying out authorized and appropriate tasks within the control system/OT environment.
	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	<i>Rationale only provided for High Priority Subcategories</i>
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	Monitoring for unauthorized personnel, connections, devices and software is necessary to validate that the control system/OT environment is operating as intended and that no policy or cyber incidents have occurred to threaten physical security.

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Detection Processes	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	<i>Rationale only provided for High Priority Subcategories</i>
	DE.DP-3: Detection processes are tested	<i>Rationale only provided for High Priority Subcategories</i>
	DE.DP-4: Event detection information is communicated to appropriate parties	<i>Rationale only provided for High Priority Subcategories</i>
	DE.DP-5: Detection processes are continuously improved	<i>Rationale only provided for High Priority Subcategories</i>

Respond	Proper response plan development and execution is critical in the response phase of maintaining physical safety. Organizations must be prepared to analyze and mitigate any control system/OT environment vulnerability or flaw that could potentially harm physical assets and impact business continuity.	
	High Priority Subcategories	Moderate Priority Subcategories
Response Planning	RS.RP-1	
Communications		RS.CO-1, RS.CO-3
Analysis	RS.AN-2	RS.AN-1, RS.AN-3, RS.AN-4
Mitigation	RS.MI-1, RS.MI-2, RS.MI-3	
Information Protection Process and Procedures		RS.IM-1, RS.IM-2

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Response Planning	RS.RP-1: Response plan is executed during or after an event	An incident response plan is essential documentation consisting of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of incidents against an organization's physical and IT assets. Responding appropriately to incidents can help protect the physical safety of an organization's resources including those that may impact business continuity.
Communications	RS.CO-1: Personnel know their roles and order of operations when a response is needed	<i>Rationale only provided for High Priority Subcategories</i>
	RS.CO-3: Information is shared consistent with response plans	<i>Rationale only provided for High Priority Subcategories</i>

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Analysis	RS.AN-1: Notifications from detection systems are investigated.	<i>Rationale only provided for High Priority Subcategories</i>
	RS.AN-2: The impact of the incident is understood	Knowing the impact of incidents is essential for organizations to mitigate the incident's effect on an organization's physical assets; to understand the way forward to maintain physical security; to provide a means to compare current state with expected state in a response timeline; and to allow an organization to apply lessons learned in responding to a future incident. This is critical in control system/OT environments as an organization must understand the immediate and long-term effects an incident can have on continuity of operations.
	RS.AN-3: Forensics are performed	<i>Rationale only provided for High Priority Subcategories</i>
	RS.AN-4: Incidents are categorized consistent with response plans	<i>Rationale only provided for High Priority Subcategories</i>
Mitigation	RS.MI-1: The incidents are contained	In any incident response situation, the primary action after detecting a cyber incident is to contain the incident so it cannot spread throughout the organization or to other systems. Effectively contained events and incidents isolate control systems/OT to minimize any damage or impact to DoW IT assets, control system/OT components, data, and services by preventing any further contamination, intrusion, or malicious activity. As such, containment is key in ensuring business continuity and maintaining physical security.

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
	RS.MI-2: The incidents are mitigated	It is essential in responding to an incident to follow an appropriate course of action that executes a response plan identifying if eradication is necessary, or should be performed in recovery, to properly mitigate an incident that is adversely affecting physical safety of the control system/OT environment. Any mitigation measures must be carefully considered to ensure that they do not add additional adverse effects to those caused by the incident. If proper mitigation measures are not incorporated into an organization's incident response, there could be devastating and lasting effects to the control system/OT environment.
	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	A newly identified vulnerability that can result in unauthorized access, use, disclosure, disruption, modification, or destruction of a control system/OT or control system/OT-related asset must be mitigated or documented as acceptable risk. Zero-day vulnerabilities are a common cause of security breaches and can include exploits of established physical security safeguards protecting a control system/OT environment. Once a vulnerability of any kind is discovered, it must be resolved or documented as an accepted risk based on the priorities and risk tolerance of the organization; otherwise, the vulnerability could result in an exploit that could cause irreparable physical damage to the control system/OT environment.
Improvements	RS.IM-1: Response plans incorporate lessons learned	<i>Rationale only provided for High Priority Subcategories</i>
	RS.IM-2: Response strategies are updated	<i>Rationale only provided for High Priority Subcategories</i>

Recover	Effective recovery measures are critical to ensuring physical safety in a control system/OT environment. After an incident occurs, organizations must be able to protect their personnel, and they must be able to make organizational improvements based on lessons learned.	
	High Priority Subcategories	Moderate Priority Subcategories
Recovery Planning	RC.RP-1	
Improvements		RC.IM-1, RC.IM-2
Communications		RC.CO-3

Detailed Specifications		
Category	Subcategory	Rationale for High Priority
Recovery Planning	RC.RP-1: Recovery plan is executed during or after an event	Recovery plans help organizations maintain operational continuity after an adverse event or cyber incident has occurred. Ensuring that an organization has pre-defined activities in place that specify recovery objectives (Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs)) for the various systems and subsystems involved, based on typical business need, to restore functionality is essential to maintaining the physical safety of assets within a control system/OT environment.
Improvements	RC.IM-1: Recovery plans incorporate lessons learned	<i>Rationale only provided for High Priority Subcategories</i>
	RC.IM-2: Recovery strategies are updated	<i>Rationale only provided for High Priority Subcategories</i>
Communications	RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	<i>Rationale only provided for High Priority Subcategories</i>

3 System Security Requirements for Control Systems/OT

The following sections take a system-oriented approach to control system/OT security. Rather than addressing security from an organizational perspective as in the CSF, this section describes tailored implementation guidance for control systems/OT with relation to the security controls established in NIST SP 800-53 and the NIST SP 800-82. Particularly, section 6.2 of NIST SP 800-82, Rev 2, “Guidance on the Application of Security Controls to ICS” gives control system-specific recommendations and guidance to applying the NIST SP 800-53 controls in a control system/OT environment. Section 3.1 begins with the discussion of the minimum system cybersecurity requirements established by the U.S. Government and how they can be applied to DoW control systems/OT. Each control family established in FIPS 200 is explained with supplemental language tailoring the control family’s purpose to its applicability in a control system/OT environment. Finally, Section 3.4 contains tables of each control family mapping the DoW control systems/OT derived security requirements to the appropriate controls established in NIST SP 800-53, providing guidance for secure implementation of control systems/OT cybersecurity.

3.1 Minimum Standards for Cybersecurity

The U.S. Government developed standards that organize U.S. efforts to implement system cybersecurity into a repeatable, verifiable and sustainable effort. These standards are known as Federal Information Processing Standards (FIPS). FIPS 200 establishes security control families that include requirements for security controls used in cybersecurity processes such as the RMF. The security controls used by the U.S. Government under the RMF process are organized into the FIPS 200 security control families.

The requirements laid out in FIPS 200 for these security families establishes the requirements for system cybersecurity. The individual security controls in these families are one possible way to implement these requirements. The FIPS 200 security families enable different parties to coordinate and communicate their security practices while leveraging different practices.

FIPS 200 sets up 16 control families for system cybersecurity. Many control families easily relate to traditional IT or communications security practices. However, a number of these control families include disciplines not traditionally linked to IT or communications security, but as a result of shifts in technology, organizational structure, and even global economics can directly impact system cybersecurity. Additionally, FIPS 200 attempts to be organization agnostic. As such, the use of the term “organization” applies to the organization that owns and maintains responsibility for the security of a specific system.

3.2 Adapted Scope and Intent of Security Control Families

The following paragraphs describe the 16 control families from a control systems/OT perspective to include the applicability of each control family as it relates to control systems/OT and implementing control systems/OT cybersecurity.

Access controls (AC)

Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

Access control is concerned with ensuring that only authorized users and data flows have access to a system and that systems data. A major focus of this security control family is the creation and management of user accounts. However, this family also includes security controls specific to access-related safeguarding considerations such as managing system information flows, enforcing least privilege on system users and administrators as well as remote and wireless access to the system. Due to the gatekeeper nature of these security activities, the AC security control family contains most of the highest impact security requirements.

From a control systems/OT perspective, closely managing remote access through role-based access control (RBAC) tools and centralized VLAN management or eliminating remote access altogether when it is not needed is critical to implementing secure access control measures. Physical access to devices must be limited to authorized users only. Access management should be implemented at all levels of the control system/OT to create defense-in-depth.

Audit and Accountability (AU)

Organizations must:

- (i) Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and
- (ii) Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

Audit and accountability are focused on the ability to recreate events after the fact and linking those events and actions back to a user. The audit of system logs provides critical understanding of what normal operations look like on a given system. This is the first step in the ability to identify anomalous behavior, which may be an indication of compromise. Additionally, auditing plays a critical role in post incident lessons learned. Audit logs provide details on the chain of events leading up to an incident, what happened during the incident, the full impact on the system and what users, or components were affected. This information is critical in identifying

who, what, where, and how of adversarial behavior, but also in identifying areas for improvement or remediation in the system.

Regarding control systems/OT, auditing a control system/OT should involve ensuring that security controls operate correctly after validation testing, ensuring that production systems are free from security compromises, and ensuring that change management programs are thoroughly executed and rigorously documented. As control systems/OT vary greatly, it is important for control system/OT operators to use the system's vendor auditing tools and techniques when traditional auditing practices are not available. Additionally, auditing a control system/OT should include the use of configuration management tools, auditing engineering workstations, and situational awareness surrounding the control system/OT for effective examination.

Awareness and Training (AT)

Organizations must:

- (i) Ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and
- (ii) Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Frequently, security incidents occur as a result of poor security practices by end users. Awareness and Training is focused on improving systems security by improving end users' security behaviors and awareness. Effective organizational training, combined with effective system security controls, can reduce the system threats from poor end user security practices.

From a control systems/OT perspective, ensuring that all personnel are able to adequately secure control systems/OT and recognize potential threat indicators are essential aspects of effective security implementation. Cross training control system/OT and IT engineers is essential in ensuring the proper application of cybersecurity to control systems/OT. Moreover, due to the large variety and complexity of control systems/OT, vendor/system specific training is often necessary to properly train personnel to operate in specific control system/OT environments.

Security Assessment and Authorization Controls (CA)

Organizations must:

- (i) Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application;
- (ii) Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems;
- (iii) Authorize the operation of organizational information systems and any associated information system connections; and
- (iv) Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

The application of security controls to information systems has been commonplace for a long time. Lessons learned from years of experience tell us that organizations need to check to see whether these security controls were implemented, whether they were implemented correctly and whether they are effective. A process that provides this testing helps an organization understand the risks associated with the system being inspected and can ensure that decisions about accepting the risk associated with that system are made by someone with the correct authority. Additionally, it provides the opportunity to identify shortcomings in the system. Once identified, these systems shortcomings can be managed, and fixes can be planned. In the U.S. Government these are referred to as Plans of Actions and Milestones (POA&M). Finally, this assessment creates a baseline that can be monitored against. The monitoring of systems ensures that the known security state of a system can be maintained and ensures that the organization does not unknowingly begin assuming more risk as a result of systems falling out of the known security state.

A senior official must be responsible for authorizing system control implementation and accepting any residual risk that follows.

Configuration Management (CM)

Organizations must:

- (i) Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and
- (ii) Establish and enforce security configuration settings for information technology products employed in organizational information systems.

Configuration management focuses on identifying a secure configuration for the system, and the system components, and actively managing any changes that may need to occur to that configuration. Configuration management extends from specific configuration settings in software and hardware all the way to system interconnections with other systems. Principles, such as least privilege, focus on minimizing the number of people who can make changes to the minimum number of individuals. Also, management oversight of the systems current state, and any changes to that state, through an active change control process are contained in this family.

Regarding control systems/OT, remote access for configuration changes must involve strong authentication measures and close monitoring. Additionally, risk assessment must be performed when changing the configuration of any control system/OT network or device. Lastly, configuring the control system/OT to operate at a level of least functionality is emphasized to establish a baseline for secure implementation.

Contingency Planning (CP)

Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

Contingency planning ensures that the system can continue operations, at the appropriate level, in the event of an emergency that interrupts normal operation. The exact implementation of a contingency plan is driven heavily by organizational, business and mission requirements. Failover options such as Hot, Warm and Cold sites depend heavily on contingency and continuity requirements. Additionally, backup requirements are heavily impacted by recovery requirements.

Particularly with control systems/OT, contingency planning needs to be tested and then coordinated with business continuity planning to meet the needs of recovery objectives so the business mission can be satisfied. Due to the criticality of many control systems/OT, redundancy and backup operations should be considered at multiple levels to maintain system functionality and business continuity.

Identification and Authentication (IA)

Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

As stated above, Identification deals with identifying users and devices interacting with a system. This may be accomplished by use of username and password, cryptographic certificates, or other technologies that can be used to create an identity with a system. Authentication is leveraging this identifier to determine the level of access or permissions to system resources or

information. Access Controls and Identification and Authentication are often mutually supporting families. Frequently the controls, or technologies, used in the IA family are the technology capabilities that are leveraged to achieve AC outcomes.

Secure implementation of control systems/OT demands strong authentication measures such as DoW-acceptable password complexity and multi-factor authentication where advisable. If authentication measures are not feasible to implement, rigorous compensating controls must be implemented to provide the same security capability.

Incident Response (IR)

Organizations must:

- (i) Establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and
- (ii) Track, document, and report incidents to appropriate organizational officials and/or authorities.

An incident in a system may be the result of a number of things. It could be a result of a bug in the software or hardware, user error, or adversarial behavior. At the point in time that an incident is discovered it is difficult to determine the true cause of the incident. A systematic plan to handle these incidents, including procedures for escalation, ensures incidents are handled appropriately and that lessons learned can be captured.

Any control system/OT personnel must receive testing pertaining to incident response to prove their knowledgeability on potential incidents and the corresponding responses the incidents require.

Maintenance (MA)

Organizations must:

- (i) Perform periodic and timely maintenance on organizational information systems; and
- (ii) Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

The failure to maintain a system can lead to a failure of system availability, which is a cybersecurity concern. Therefore, maintenance must be performed. However, maintenance personnel, particularly from outside of an organization, can pose a significant threat to sensitive systems. The Maintenance family of controls contains security controls that ensure system maintenance is performed but done so in a way that minimizes risk to the system.

From a control systems/OT perspective, any attack surfaces need to be minimized. Remote access maintenance tools and local access for maintenance should be carefully reviewed and configured to avoid additional vulnerabilities to the system. Cybersecurity of control systems/OT requires strict periodic maintenance schedules that reflect the criticality of devices.

Media Protection (MP)

Organizations must:

- (i) Protect information system media, both paper and digital;
- (ii) Limit access to information on information system media to authorized users; and
- (iii) Sanitize or destroy information system media before disposal or release for reuse.

Unauthorized exfiltration, or the unauthorized removal of data from a system is a significant concern for cybersecurity. This exfiltration may occur via electronic or by physical means. Media protection controls focus on securing the various forms of media that may be used for this exfiltration. Control systems/OT emphasize the prohibition of any unauthorized removable media from interacting with a control system/OT on any node.

Physical and Environmental Protection (PE)

Organizations must:

- (i) Limit physical access to information systems, equipment, and the respective operating environments to authorized individuals;
- (ii) Protect the physical plant and support infrastructure for information systems;
- (iii) Provide supporting utilities for information systems;
- (iv) Protect information systems against environmental hazards; and
- (v) Provide appropriate environmental controls in facilities containing information systems.

Failure to physically secure systems make them highly susceptible to theft. Additionally, failure to protect sensitive technology from environmental factors can lead to the destruction or degradation of that technology.

Regarding control systems/OT, components like the control center require stringent access controls. Additionally, preventative measures must be taken to avoid unauthorized physical tampering and unauthorized introduction of foreign systems to a control system/OT implementation. Portable devices directly associated with control system/OT functions must also be carefully monitored, patched and confined within a secure area. Physical security must be maintained at all locations that can access control system/OT networks or components.

Planning (PL)

Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

Security plans must be revisited upon installation or introduction of a new control system/OT to ensure that security is emphasized throughout the entire system lifecycle.

Program Management (PM)

Organizations must implement security controls at the organizational level in addition to the information system level. Given the criticality of control systems/OT to overall business functionality, it is crucial to ensure that organizational objectives and information system security configurations are aligned.

Personnel Security (PS)

Organizations must:

- (i) Ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions;
- (ii) Ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and
- (iii) Employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

Personnel represent a major threat to systems and their cybersecurity. As such, a personnel security program can greatly impact system cybersecurity. The Personnel Security family sets our controls for implementation in a personnel security program. The development of carefully tailored training programs and position screenings for personnel are measures that need to be taken prior to authorizing access to control systems/OT.

Risk Assessment (RA)

Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

Regarding control systems/OT, any risk mitigation measure must be derived by considering the mitigation costs, affects to business continuity, physical safety concerns and the value of data flowing from the control system/OT network to any devices or systems outside of the network.

System and Services Acquisition (SA)

Organizations must:

- (i) Allocate sufficient resources to adequately protect organizational information systems;
- (ii) Employ system development life cycle processes that incorporate information security considerations;
- (iii) Employ software usage and installation restrictions; and
- (iv) Ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

How systems are acquired and from whom can lead to increased risk to a system. The System and Services Acquisition family contain controls intended to minimize the risks associated with acquiring systems. Areas of concern include Supply Chain Risk Management and Software development practices. It is crucial to understand the effects of each entity to the organization's supply chain and to hold external suppliers to the same security standards as that of the organization to maintain the overall level of control system/OT security.

System and Communications Protection (SC)

Organizations must:

- (i) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and
- (ii) Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

The system and communications family of security controls covers a wide array of controls that address a variety of system security elements. This control family contains a variety of system and network protections such as mobile code protections, honeypots, Public Key Infrastructure, information at rest protections and denial of service protection.

From a control systems/OT perspective, it is advisable to employ cryptographic systems and a VPN where they are deemed appropriate after extensive performance testing. Configuring control systems/OT so they do not depend entirely on the network is also imperative to secure

Unclassified

implementation. As stated in Section 3.4, limiting the interconnections amongst systems to those necessary to satisfy the system's purposes minimizes the attack surface area of the system.

System and Information Integrity (SI)

Organizations must:

- (i) Identify, report, and correct information and information system flaws in a timely manner;
- (ii) Provide protection from malicious code at appropriate locations within organizational information systems; and
- (iii) Monitor information system security alerts and advisories and take appropriate actions in response.

System and Information integrity security focuses on ensuring that system flaws are identified and remediated. Included into this family are controls for malicious code protection, system monitoring and security alerts, functional alarms, advisories and directives.

Prior to implementing any controls from the SI family, ensure that system functionality is retained within the control system/OT and that the environment can satisfy required performance levels. Employing a patch to a control system/OT environment poses risks to the functionality of the system. As such, the employment of a patch must be assessed before it is introduced to a production environment. If implementation is permitted, it is critical to ensure that patches to a control system/OT are frequently tested and deployed.

3.3 DoW Policy Regarding Security Controls

DoWI 8500.01 requires DoW organizations to categorize all DOW systems in accordance with CNSSI 1253 and implement a corresponding set of security C/CEs as published in NIST SP 800-53, regardless of whether they are National Security Systems (NSS) or non-NSS.

DoWI 8510.01 establishes DoW policy for RMF, guides the creation of associated cybersecurity policy, and assigns responsibilities for executing and maintaining the RMF. This DoW policy is consistent with NIST SP 800-37, *Guide for Applying the Risk Management Framework*, CNSSI 1253 and NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*.

The CNSSI 1253 baselines are comprised of NIST SP 800-53 baselines coupled with the additional NIST SP 800-53 security controls required for NSS. These baselines act as a starting point for securing all DoW systems and organizations can tailor these further to address specific systems and situations.

The following requirements are not to be confused with the cybersecurity activities illuminated in the CSF, which are shown in Section 2.

3.4 System Security Requirements Mapping Tables

The following tables illustrate the basic and derived security requirements developed for DoW. The basic requirements were adopted from FIPS 200 and the derived requirements were developed in accordance with NIST SP 800-82, creating tailored security requirements specific to the unique characteristics of control systems/OT. The requirements were then mapped to the security controls listed in each control family of NIST SP 800-53 to be implemented in a DoW control system/OT environment throughout the control system/OT lifecycle.

Table 1-1: Mapping Access Control Requirements to Controls

CONTROL FAMILY	NIST 800-53 Relevant Security Controls	
AC - Access Control	#	CONTROL DESCRIPTION
SECURITY REQUIREMENTS		
<i>Basic Security Requirements</i>		
1.1 Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems) and to the types of transactions and functions that authorized users are permitted to exercise.	AC-2	ACCOUNT MANAGEMENT
	AC-3	ACCESS ENFORCEMENT
<i>Derived Security Requirements</i>		
1.2 Utilize role-based access controls to enhance security from remote access points.	AC-2(7)	ACCOUNT MANAGEMENT Privileged User Accounts
	AC-3(2)	ACCESS ENFORCEMENT Dual Authorization
1.3 Employ the principle of least privilege, including for specific security functions and privileged accounts. 1.4 Deploy virtual local area networks (VLANs) where feasible, to increase system performance, improve manageability, and simplify network design.	AC-6	LEAST PRIVILEGE

CONTROL FAMILY	NIST 800-53 Relevant Security Controls	
AC - Access Control	#	CONTROL DESCRIPTION
<p>1.5 Ensure remote access software employs carefully reviewed and configured security options. often use remote control software that provide the remote user powerful (administrative or root) access to the target system.</p>	AC-17	REMOTE ACCESS
<p>1.6 Ensure wireless local area networks (LANs) are deployed only where operational risk implications are low</p>	AC-18	WIRELESS ACCESS

Table 1-2: Mapping Awareness and Training Requirements to Controls

CONTROL FAMILY	NIST 800-53 Relevant Security Controls	
AT - Awareness and Training	#	CONTROL DESCRIPTION
SECURITY REQUIREMENTS		
<i>Basic Security Requirements</i>		
<p>1.1 Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable security policies, standards, and procedures for those systems.</p> <p>1.2 Ensure that organizational personnel are adequately trained to carry out their assigned security-related duties and responsibilities.</p>	AT-2	LITERACY TRAINING AND AWARENESS
	AT-3	ROLE BASED TRAINING
<i>Derived Security Requirements</i>		
<p>1.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat</p>	AT-2(2)	LITERACY TRAINING AND AWARENESS <i>Insider Threat</i>
<p>1.4. Ensure personnel have taken specific information security awareness training and know the responsibilities involved for control system/OT applications. Awareness training must cover the physical process being controlled as well as the system itself.</p> <p>1.5 Ensure training programs demonstrate why control system/OT environments require new access and control methods, covers ways personnel can reduce risk, and addresses the impact of not incorporating control methods.</p>	AT-3(3)	ROLE BASED TRAINING <i>Practical Exercises</i>

Table 1-3: Mapping Audit and Accountability Requirements to Controls

CONTROL FAMILY	NIST 800-53 Relevant Security Controls	
AU - Audit and Accountability	#	CONTROL DESCRIPTION
SECURITY REQUIREMENTS		
<i>Basic Security Requirements</i>		
<p>1.1 Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.</p> <p>1.2 Ensure contain a method for tracing actions to individual system users so organizations can hold those users accountable for their actions.</p>	AU-2	EVENT LOGGING
	AU-3	CONTENT OF AUDIT RECORDS
	AU-6	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING
	AU-11	AUDIT RECORD RETENTION
	AU-12	AUDIT RECORD GENERATION
<i>Derived Security Requirements</i>		
<p>It is necessary to determine that the system is performing as intended. Organizations must perform periodic audits of the control system/OT to validate the following items:</p> <p>1.3 The production system contains correctly installed and operating security controls originally present at system validation testing (e.g., factory acceptance testing and site acceptance testing).</p> <p>1.4 The production system is free from security compromises and provides information on the nature and extent of compromises as feasible, should they occur.</p> <p>1.5 The change program is being managed rigorously and creates an auditable trail of reviews and approvals for all changes. Organizations should also monitor sensors, logs, Intrusion Detection Systems</p>	AU-6	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING
	AU-7	AUDIT RECORD REDUCTION AND REPORT GENERATION

CONTROL FAMILY	NIST 800-53 Relevant Security Controls	
AU - Audit and Accountability	#	CONTROL DESCRIPTION
<p>(IDS), antivirus, patch management, policy management software, and other security mechanisms in real-time, when feasible. First-line monitoring services receive alarms, perform rapid initial problem determination and take action to alert appropriate facility personnel to intervene. Organizations should incorporate system auditing utilities into new and existing control system/OT projects, and should test these auditing utilities (e.g., off-line on a comparable control system) before being deployed on an operational control system. These tools can provide tangible records of evidence and system integrity. Additionally, active log management utilities may actually flag an attack or event in progress and provide location and tracing information to help respond to the incident. Additionally, organizations need a method for tracing all console activities to a user, either manually (e.g., control room sign in) or automatic (e.g., login at the application or OS layer). Organizations should also develop policies and procedures for determining log content, storage (or printing), protection, accessibility, and reviewability of the logs. These policies and procedures will vary with the control system/OT application and platform. Legacy systems typically employ printer loggers, which are reviewed by administrative, operational, and security staff. Logs maintained by the control system/OT application may be stored at various locations and may or may not be encrypted.</p>	AU-9	PROTECTION OF AUDIT INFORMATION
	AU-10(1)	NON-REPUDIATION Association of Identities
	AU-12	AUDIT RECORD GENERATION

Table 1-4: Mapping Certification, Accreditation, and Security Assessment Requirements to Controls

CONTROL FAMILY	NIST 800-53 Relevant Security Controls	
CA - Certification, Accreditation, and Security Assessments	#	CONTROL DESCRIPTION
SECURITY REQUIREMENTS		
<i>Basic Security Requirements</i>		
<p>1.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application;</p> <p>1.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems;</p> <p>1.3 Authorize the operation of organizational systems and any associated system connections;</p> <p>1.4 Monitor system security controls on an ongoing basis to ensure the continued effectiveness of the controls.</p>	CA-2	CONTROL ASSESSMENTS
	CA-5	PLAN OF ACTION AND MILESTONES
	CA-6	AUTHORIZATION
	CA-7	CONTINUOUS MONITORING
<i>Derived Security Requirements</i>		
<p>1.5 A senior organizational official must accept residual risk and grant the system authorization to operate.</p>	CA-2(1)	CONTROL ASSESSMENTS <i>Independent Assessors</i>
<p>1.6 Limit control system/OT interconnections to only those necessary to satisfy the system's purpose. Additional unnecessary connections increase the control system's attack surface area and create more vulnerabilities.</p>	CA-3	INFORMATION EXCHANGE
	CA-9	INTERNAL SYSTEM CONNECTIONS

Table 1-5: Mapping Configuration Management Requirements to Controls

CONTROL FAMILY	NIST 800-53 Relevant Security Controls	
CM - Configuration Management	#	CONTROL DESCRIPTION
SECURITY REQUIREMENTS		
<i>Basic Security Requirements</i>		
<p>1.1 Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles;</p> <p>1.2 Establish and enforce security configuration settings for information technology products employed in organizational information systems.</p>	CM-2	BASELINE CONFIGURATION
	CM-6	CONFIGURATION SETTINGS
	CM-8	SYSTEM COMPONENT INVENTORY
	CM-8(1)	SYSTEM COMPONENT INVENTORY Updates During Installations and Removal
	CM-9	CONFIGURATION MANAGEMENT PLAN
<i>Derived Security Requirements</i>		
<p>1.3 Configure remote control software to use unique usernames and passwords, strong authentication, encryption if determined appropriate, and audit logs. Organizations should monitor remote users who utilize this software on an almost real-time frequency.</p> <p>1.4 Ensure remote access software employs carefully reviewed and configured security options. often use remote control software that provide the remote user powerful (administrative or root) access to the target system.</p>	CM-3	CONFIGURATION CHANGE CONTROL

CONTROL FAMILY	NIST 800-53 Relevant Security Controls	
CM - Configuration Management	#	CONTROL DESCRIPTION
1.5 Perform risk assessment when dealing with any configuration change to a control system/OT network or device.	CM-4	IMPACT ANALYSES
1.6 Restrict configuration and security setting access to the most stringent mode consistent with control system/OT operational requirements.	CM-5	ACCESS RESTRICTIONS FOR CHANGE
1.7 Configure the control system/OT to operate at a level of least functionality required for its specific purpose, disabling any ports, protocols, and services not specifically needed by the control system.	CM-7	LEAST FUNCTIONALITY
	CM-8(6)	SYSTEM COMPONENT INVENTORY <i>Assessed Configurations and Approved Deviations</i>

Table 1-6: Mapping Contingency Planning Requirements to Controls

CONTROL FAMILY	NIST 800-53 Relevant Security Controls	
CP - Contingency Planning	#	CONTROL DESCRIPTION
SECURITY REQUIREMENTS		
<i>Basic Security Requirements</i>		
<p>1.1 Establish, maintain, and effectively implement emergency response, backup operations, and post-disaster recovery plans for organizational information systems to ensure continuity of operations and the availability of critical information in emergency situations.</p>	CP-2	CONTINGENCY PLAN
	CP-9	SYSTEM BACKUP
<i>Derived Security Requirements</i>		
<p>1.2 Establish trainings to ensure employees are familiar with the contents of the contingency plans.</p>	CP-3	CONTINGENCY TRAINING
	CP-4	CONTINGENCY PLAN TESTING
<p>1.3 Coordinate contingency planning with management responsible for business continuity planning to meet the needs of the recovery objectives.</p>	CP-6	ALTERNATE STORAGE SITE
	CP-7	ALTERNATE PROCESSING SITE
<p>1.4 Formulate a comprehensive disaster recovery plan (DRP) consisting of actions to take place before, during, and after a disaster. A DRP related to must include components such as up-to-date logical network diagrams, current configuration information for all components, and scheduled DRP testing to ensure continued availability of the control system.</p>	CP-10	SYSTEM RECOVERY AND RECONSTITUTION

Table 1-7: Mapping Identification and Authentication Requirements to Controls

CONTROL FAMILY	NIST 800-53 Relevant Security Controls	
IA - Identification and Authentication	#	CONTROL DESCRIPTION
SECURITY REQUIREMENTS		
Basic Security Requirements		
<p>1.1 Identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.</p>	IA-2	IDENTIFICATION AND AUTHENTICATION (Organizational Users)
	IA-3	DEVICE IDENTIFICATION AND AUTHENTICATION
	IA-5	AUTHENTICATOR MANAGEMENT
Derived Security Requirements		
<p>1.2 In situations where authentication mechanisms may improperly effect control system/OT functionality, compensating controls (such as rigorous physical security controls) must provide an equivalent security capability.</p>	IA-2(1)	IDENTIFICATION AND AUTHENTICATION <i>Multi-factor Authentication to Privileged Accounts</i>
<p>1.3 Organizations must consider system functionality, ease of use, cost, and overall risk when incorporating additional authentication measures such as physical tokens, smart cards, biometric devices, etc. within a control system/OT environment.</p>	IA-4	IDENTIFIER MANAGEMENT
<p>1.4 Specify password complexity at DoW-defined values where practical (see DoW password policy).</p>	IA-5(1)	AUTHENTICATOR MANAGEMENT <i>Password-Based Authentication</i>
<p>1.5 Configure per 1.4 so that systems do not use default passwords for authentication.</p>		
<p>1.6 If organizations deem authentication mechanisms advisable, they should implement multi-factor authentication.</p>	IA-11	RE-AUTHENTICATION

Table 1-8: Mapping Incident Response Requirements to Controls

CONTROL FAMILY	NIST 800-53 Relevant Security Controls	
IR - Incident Response	#	CONTROL DESCRIPTION
SECURITY REQUIREMENTS		
Basic Security Requirements		
<p>1.1 Establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; 1.2 Track, document, and report incidents to appropriate organizational officials and authorities.</p>	IR-2	INCIDENT RESPONSE TRAINING
	IR-4	INCIDENT HANDLING
	IR-5	INCIDENT MONITORING
	IR-6	INCIDENT REPORTING
	IR-7	INCIDENT RESPONSE ASSISTANCE
Derived Security Requirements		
<p>1.3 Establish incident response training for control system/OT personnel.</p>	IR-3	INCIDENT RESPONSE TESTING
	IR-5(1)	INCIDENT MONITORING <i>Automated Tracking, Data Collection, and Analysis</i>
<p>1.4 Implement periodic IR testing sessions to ensure personnel know about the differing severities of potential control system/OT incidents and the corresponding response measures that must occur for each situation.</p>	IR-8	INCIDENT RESPONSE PLAN
	IR-9	INFORMATION SPILLAGE RESPONSE

Table 1-9: Mapping Maintenance Requirements to Controls

CONTROL FAMILY	NIST 800-53 Relevant Security Controls	
MA - Maintenance	#	CONTROL DESCRIPTION
SECURITY REQUIREMENTS		
<i>Basic Security Requirements</i>		
<p>1.1 Perform periodic and timely maintenance on organizational information systems;</p> <p>1.2 Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.</p>	MA-2	CONTROLLED MAINTENANCE
	MA-3	MAINTENANCE TOOLS
	MA-3(1)	MAINTENANCE TOOLS <i>Inspect Tools</i>
	MA-3(2)	MAINTENANCE TOOLS <i>Inspect Media</i>
<i>Derived Security Requirements</i>		
<p>1.3 Ensure the careful review and configuring of security options for remote access maintenance tools. often use remote control maintenance via operating system login.</p>	MA-4	NONLOCAL MAINTENANCE
	MA-5	MAINTENANCE PERSONNEL

Table 1-10: Mapping Media Protection Requirements to Controls

CONTROL FAMILY	NIST 800-53 Relevant Security Controls	
MP - Media Protection	#	CONTROL DESCRIPTION
SECURITY REQUIREMENTS		
<i>Basic Security Requirements</i>		
1.1 Protect information system media, both paper and digital; 1.2 Limit access to information on information system media to authorized users; 1.3 Sanitize or destroy information system media before disposal or release for reuse.	MP-2	MEDIA ACCESS
	MP-4	MEDIA STORAGE
	MP-6	MEDIA SANITIZATION
<i>Derived Security Requirements</i>		
1.4 Ensure safe and secure maintenance of information system media.	MP-3	MEDIA MARKING
1.5 Provide secure guidance for transporting, handling, erasing, and destroying media assets.	MP-5	MEDIA TRANSPORT
1.6 Securely store media to prevent theft, unintentional distribution, or environmental damage.	MP-7	MEDIA USE
1.7 Prohibit personnel from using any unauthorized removable media to interact with a control system/OT on any node.		
1.8 Incorporate policy management software to enforce media protection policy where applicable.		

Table 1-11: Mapping Physical and Environmental Protection Requirements to Controls

CONTROL FAMILY	NIST 800-53 Relevant Security Controls	
PE - Physical and Environmental Protection	#	CONTROL DESCRIPTION
SECURITY REQUIREMENTS		
<i>Basic Security Requirements</i>		
<p>1.1 Limit physical access to information systems, equipment, and the respective operating environments to authorized individuals;</p> <p>1.2 Protect the physical plant and support infrastructure for information systems;</p> <p>1.3 Provide supporting utilities for information systems;</p> <p>1.4 Protect information systems against environmental hazards;</p> <p>1.5 Provide appropriate environmental controls in facilities containing information systems.</p>	PE-2	PHYSICAL ACCESS AUTHORIZATIONS
	PE-3	PHYSICAL ACCESS CONTROL
	PE-4	ACCESS CONTROL FOR TRANSMISSION
	PE-5	ACCESS CONTROL FOR OUTPUT DEVICES
	PE-6	MONITORING PHYSICAL ACCESS
<i>Derived Security Requirements</i>		
<p>1.6 Provide stringent access controls for a control system/OT control center or control room. Additional authentication measures such as smart cards or biometric devices may be deemed necessary depending on the number of critical nodes the center contains</p>	PE-3(2)	PHYSICAL ACCESS CONTROL <i>Facility and Systems</i>
	PE-3(4)	PHYSICAL ACCESS CONTROL <i>Lockable Casings</i>
<p>1.7 Prevent unauthorized physical modification, manipulation, theft, removal, or destruction of existing control system/OT environment.</p>	PE-3(5)	PHYSICAL ACCESS CONTROL <i>Tamper Protection</i>
<p>1.8 Prevent unauthorized introduction of new systems, infrastructure, communication interfaces or other hardware into a control system/OT environment.</p>		

CONTROL FAMILY	NIST 800-53 Relevant Security Controls	
PE - Physical and Environmental Protection	#	CONTROL DESCRIPTION
<p>1.9 Use proper cabling when designing the control system/OT network. Network cables must be above the grade of unshielded twisted pair and should not be susceptible to interference. Limit cabling access to authorized personnel.</p>	PE-9	POWER EQUIPMENT AND CABLING
	PE-14	ENVIRONMENTAL CONTROLS
<p>1.10 Prohibit portable devices such as computers and computerized devices used for critical control system/OT functions from leaving the control system/OT area. Ensure that portable engineering workstations and handhelds containing sensitive information are never allowed outside of the control system/OT network. Prevent unauthorized devices from entering control system/OT facilities and connecting to control system/OT networks. Maintain up-to-date patch management on portable devices.</p>	PE-20	ASSET MONITORING AND TRACKING

Table 1-12: Mapping Planning Requirements to Controls

CONTROL FAMILY	NIST 800-53 Relevant Security Controls	
PL - Planning	#	CONTROL DESCRIPTION
SECURITY REQUIREMENTS	NIST 800-53 Relevant Security Controls	
<i>Basic Security Requirements</i>		
<p>1.1 Develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.</p> <p>1.2 Implement antivirus tools when deemed acceptable within the control system/OT. Follow vendor recommendations on all relevant servers and computers and ensure up-to-date patching of any antivirus software.</p>	PL-2	SYSTEM SECURITY AND PRIVACY PLANS
	PL-4	RULES OF BEHAVIOR
	PL-9	CENTRAL MANAGEMENT
<i>Derived Security Requirements</i>		
<p>1.3 Revisit the security plan upon installing or introducing a new control system/OT to the environment to ensure security is addressed throughout the system lifecycle.</p>	PL-7	CONCEPT OF OPERATIONS
<p>1.4 Incorporate "forward-looking" objectives into the security plan to account for the dynamic landscape of control system/OT security.</p>	PL-8(1)	SECURITY AND PRIVACY ARCHITECTURE <i>Defense-in-Depth</i>

Table 1-13: Mapping Program Management Requirements to Controls

CONTROL FAMILY	NIST 800-53 Relevant Security Controls	
PM - Program Management	#	CONTROL DESCRIPTION
SECURITY REQUIREMENTS		
<i>Basic Security Requirements</i>		
1.1 Implement security controls at an organizational level on top of the information security level; 1.2 Clearly define the business mission so that an organization can successfully implement protection measures to satisfy the mission objective	PM-2	INFORMATION SECURITY PROGRAM LEADERSHIP ROLE
	PM-3	INFORMATION SECURITY AND PRIVACY RESOURCES
	PM-5	SYSTEM INVENTORY
	PM-6	MEASURES OF PERFORMANCE
	PM-10	AUTHORIZATION PROCESS
	PM-11	MISSION AND BUSINESS PROCESS DEFINITION
<i>Derived Security Requirements</i>		
None		

Table 1-14: Mapping Personnel Security Requirements to Controls

CONTROL FAMILY		NIST 800-53 Relevant Security Controls
PS - Personnel Security	#	CONTROL DESCRIPTION
SECURITY REQUIREMENTS		NIST 800-53 Relevant Security Controls
<i>Basic Security Requirements</i>		
<p>1.1 Ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions;</p> <p>1.2 Ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers;</p> <p>1.3 Employ formal sanctions for personnel failing to comply with organizational security policies and procedures.</p>	PS-3	PERSONNEL SCREENING
	PS-4	PERSONNEL TERMINATION
	PS-5	PERSONNEL TRANSFER
	PS-8	PERSONNEL SANCTIONS
<i>Derived Security Requirements</i>		
<p>1.4 Establish a risk designation and screening criteria for relevant positions maintaining and controlling the control system.</p>	PS-2	POSITION RISK DESIGNATION
<p>1.5 Screen personnel in critical positions against specified criteria before granting them access to a particular control system.</p>		
<p>1.6 Carefully develop training programs to ensure that each employee has received relevant training to satisfy their job functions.</p>	PS-6	ACCESS AGREEMENTS

Table 1-15: Mapping Risk Assessment Requirements to Controls

SECURITY REQUIREMENTS	NIST 800-53 Relevant Security Controls	
RA - Risk Assessment	#	CONTROL DESCRIPTION
Basic Security Requirements		
<p>1.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.</p>	RA-3	RISK ASSESSMENT
Derived Security Requirements		
<p>1.2 Categorize the value of the data flowing from the control network to the corporate network. Fiscal justification for any risk mitigation must be derived by comparing the mitigation cost to the effects of data compromise.</p>	RA-2	SECURITY CATEGORIZATION
<p>1.3 Utilize vulnerability scanning on necessary assets where risk and mitigation values justify the scan and do not diminish system functionality.</p>	RA-5	VULNERABILITY MONITORING AND SCANNING
	RA-5(5)	VULNERABILITY MONITORING AND SCANNING <i>Privileged Access</i>

Table 1-16: Mapping System and Services Acquisition Requirements to Controls

SECURITY REQUIREMENTS	NIST 800-53 Relevant Security Controls	
SA - System and Services Acquisition	#	CONTROL DESCRIPTION
Basic Security Requirements		
<p>1.1 Allocate sufficient resources to adequately protect organizational information systems; 1.2 Employ system development life cycle processes that incorporate information security considerations; 1.3 Employ software usage and installation restrictions; 1.4 Ensure that third-party providers employ adequate security measures to protect information, applications, and services outsourced from the organization.</p>	SA-2	ALLOCATION OF RESOURCES
	SA-3	SYSTEM DEVELOPMENT LIFE CYCLE
	SA-4	ACQUISITION PROCESS
	SA-5	SYSTEM DOCUMENTATION
	SA-8	SECURITY AND PRIVACY ENGINEERING PRINCIPLES
	SA-11	DEVELOPER TESTING AND EVALUATION
Derived Security Requirements		
<p>1.5 Hold external suppliers to the same security policies and procedures as that of the organization to maintain the overall level of control system/OT security.</p>	SA-9	EXTERNAL SYSTEM SERVICES
	SA-9(3)	EXTERNAL SYSTEM SERVICES <i>Establish and Maintain Trust Relationship with Providers</i>

Table 1-17: Mapping System and Communications Protection Requirements to Controls

CONTROL FAMILY	NIST 800-53 Relevant Security Controls	
SC - System and Communications Protection	#	CONTROL DESCRIPTION
SECURITY REQUIREMENTS		
Basic Security Requirements		
<p>1.1 Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems;</p> <p>1.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.</p>	SC-2	SEPARATION OF SYSTEM AND USER FUNCTIONALITY
	SC-3	SECURITY FUNCTION ISOLATION
	SC-7	BOUNDARY PROTECTION
Derived Security Requirements		
<p>1.3 Employ cryptographic systems if and only if they are deemed an appropriate solution after extensive performance testing. Organizations must reference existing security policy and perform risk assessment for a control system/OT before selecting cryptographic protection.</p>	SC-5	DENIAL OF SERVICE PROTECTION
	SC-8	TRANSMISSION CONFIDENTIALITY AND INTEGRITY
	SC-8(1)	TRANSMISSION CONFIDENTIALITY AND INTEGRITY <i>Cryptographic Protection</i>
<p>1.4 Implement a virtual private network (VPN) in the control system/OT environment if the control system/OT network must be accessed from an untrusted network (i.e. via the Internet). VPN devices should be thoroughly tested to verify that the VPN technology is compatible with the application and</p>	SC-11(1)	TRUSTED PATH Irrefutable Communications Path
<p>that implementing the VPN does not unacceptably affect network traffic.</p>	SC-13	CRYPTOGRAPHIC PROTECTION

CONTROL FAMILY	NIST 800-53 Relevant Security Controls	
SC - System and Communications Protection	#	CONTROL DESCRIPTION
<p>1.5 Configure so they do not depend entirely on the network to function. Ensure that systems can fail to a "secure" state if communications fail. This protects against denial-of-service attacks.</p>	SC-24	FAIL IN KNOWN STATE

Table 1-18: Mapping System and Information Integrity Requirements to Controls

CONTROL FAMILY	NIST 800-53 Relevant Security Controls	
SI - System and Information Integrity	#	CONTROL DESCRIPTION
SECURITY REQUIREMENTS		
Basic Security Requirements		
<p>1.1 Identify, report, and correct information and information system flaws in a timely manner;</p> <p>1.2 Provide protection from malicious code at appropriate locations within organizational information systems;</p> <p>1.3 Monitor information system security alerts and advisories and take appropriate actions in response.</p>	SI-2	FLAW REMEDIATION
	SI-3	MALICIOUS CODE PROTECTION
	SI-5	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES
Derived Security Requirements		
<p>1.5 Deploy intrusion detection systems (IDS) and intrusion prevention systems (IPS) when deemed acceptable within the control system/OT environment. Organizations should deploy network-based IDS between the control network and the corporate network in conjunction with a firewall. Organizations should deploy host-based IDS on computers that use general-purpose operating systems or applications such as HMIs, SCADA servers, and engineering workstations.</p>	SI-4(1)	SYSTEM MONITORING <i>System Wide Intrusion Detection System</i>
	SI-4(13)	SYSTEM MONITORING <i>Analyze Traffic and Event Patterns</i>
<p>1.6 When deploying patches to a control system/OT, adequately test the patch to determine the acceptability of its side effects. Organizations should implement a systematic, accountable, and documented control system/OT patch management process for managing exposure to vulnerabilities.</p>	SI-7	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY

Appendix A References

- Deputy Secretary of Defense Memorandum, “Enhancing Cybersecurity Risk Management for Control systems Supporting DOD-Owned Defense Critical Infrastructure,” July 19, 2018
- UFC 4-010-06, Cybersecurity of Facility-Related Control Systems, January 2017
- Joint DoW Memorandum, “Department of Defense Facility-Related Control Systems Cybersecurity,” September 30, 2025
- NIST 800-82, Revision 2, Guide to Industrial Control Systems (ICS) Security, May 2015
- Department of Homeland Security, “Developing an Industrial Control Systems Cybersecurity Incident Response Capability, 2009
- Department of Homeland Security, “Creating Cyber Forensics Plans for Control Systems”, 2008
- NIST Framework for Improving Critical Infrastructure Cybersecurity (“Cybersecurity Framework”), 2018

This document falls under the authority of DoW Instruction (DoWI) 8500.01 and DoWI 8510.01. DoWI 8500.01 instructs the Director of DISA, under the authority, direction, and control of the DOW CIO, to develop and maintain Control Correlation Identifiers (CCIs), Security Requirements Guides (SRGs), Security Technical Implementation Guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DOW cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the National Security Agency Central Security Service (NSA/CSS), using input from stakeholders, and using automation whenever possible.

DoWI 8500.01 further directs DOW Component heads to ensure all DOW IT under their purview complies with applicable STIGs, [NSA] security configuration guides, and SRGs. The responsible AO must document and approve any exceptions to these policies.

DoWI 8510.01 implements NIST Special Publication (SP) 800-37, NIST SP 800-53, Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253, and the FISMA by establishing the DOW Risk Management Framework (RMF) for DOW systems, establishing associated cybersecurity policy, and assigning responsibilities for executing and maintaining the DoW RMF.

Per DoW Directive (DoWD) 8000.01, all aspects of the DoW IE, including the DoW information network infrastructure, DoW enterprise IT service and solutions, National Security Systems, industrial control systems/OT, and embedded computing of wired, wireless, mobile

communication, and platforms will be planned, designed, developed, architected, configured, acquired, managed, operated, and protected to attain an information advantage, achieve full spectrum superiority, deliver mission assurance, improve mission effectiveness, and realize IT efficiencies.

All DoW Components must manage control systems/OT and implement cybersecurity activities for control systems/OT in accordance with DoWD 8000.01, DoWD 3020.40, DoWI 8500.01, 8510.01, 8530.01, and other existing statutes, regulations, and issuances regarding mission assurance and cybersecurity risk management.

DoWI 8510.01 establishes policy and assigns responsibilities for executing and maintaining the DoW RMF. Any DoW Component's use of control systems/OT, like all DoW technology systems, is subject to DoWI 8510.01 authority and decision making. The RMF incorporates system criticality and DoW mission objectives when assessing control system/OT risk and providing system authorization.

Appendix B Glossary

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/OT acts upon an environment. The control system/OT 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.

Authenticity: The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.

Availability: The property of being accessible and useable upon demand by an authorized entity.

Classified Information: Information that has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Continuous Process: A process that operates on the basis of continuous flow, as opposed to batch, intermittent, or sequenced operations.

Control: The part of the control system/OT used to perform the monitoring and control of the physical process. This includes all control servers, field devices, actuators, sensors, and their supporting communication systems.

Control/Control Enhancement (C/CE): National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Security and Privacy controls and their enhancements which are selected and assembled in various baselines and overlays.

Control Center: An equipment structure or group of structures from which a process is measured, controlled, and/or monitored.

Controller: A device or program that operates automatically to regulate a controlled variable.

Control Loop: A control loop consists of sensors for measurement, controller hardware such as PLCs, actuators such as control valves, breakers, switches and motors, and the communication of variables. Controlled variables are transmitted to the controller from the sensors. The controller interprets the signals and generates corresponding manipulated variables, based on set points, which it transmits to the actuators. Process changes from disturbances result in new sensor signals, identifying the state of the process, to again be transmitted to the controller.

Control Network: The networks of an enterprise typically connected to equipment that controls physical processes and that is time or safety critical. The control network can be subdivided into zones, and there can be multiple separate control networks within one enterprise and site.

Control System: networked controllers and user interfaces that monitor control equipment. NIST defines a control system as one in which deliberate guidance or manipulation is used to achieve a prescribed value for a variable (e.g. SCADA, industrial and process control systems, cyber-physical systems, facilities-related control systems and other types of industrial measurement and control systems).

Control System Service: Refers to a control system's product or capability.

Critical Infrastructure: A body of systems, networks, and assets that are essential to the security, economy, public health, and safety of the United States.

Cyber Incident: Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.

Distributed Control System (DCS): Refers to control achieved by intelligence that is distributed about the process to be controlled, rather than by a centrally located single unit.

DoW Component: A DoW Service or Agency including their sub-elements/commands/organizations

DoW Control System: Will refer to a DoW organization utilizing a control system implementation which may be owned and operated by DoW or a contractor for the benefit of the Department.

Facility-Related Control System (FRCS): a subset of control systems/OT that are used to monitor and control equipment and systems related to DOW facilities. The Unified Facilities Criteria (UFC) defines FRCS as control systems/OT which control equipment and infrastructure that are part of a building, structure, or linear structure on DOW installations. Some examples of FRCS* include:

1. Control System Enclaves
2. Airfield Systems
3. Pier Systems
4. Environmental Monitoring
5. Electronic Security Systems
6. Fire and Life Safety

7. Dam, Lock, and Levee Systems
8. Medical Control systems/OT
9. Traffic Control systems/OT
10. Transportation and Fueling Systems
11. Meteorological Control systems/OT
12. Building Control systems/OT
13. Utility Control systems/OT
14. Utility Monitoring and Control systems/OT

*FRCS may exist in other operating environments beyond DOW facilities.

Field Device: Equipment that is connected to the field side on a control system. Types of field devices include RTUs (remote terminal unit), PLCs (programmable logic controller), actuators, sensors, HMIs (human-machine interface), and associated communications.

Field Site: A subsystem that is identified by physical, geographical, or logical segmentation within the control system. A field site may contain RTUs, PLCs, actuators, sensors, HMIs, and associated communications.

Human-Machine Interface (HMI): A hardware or software through which an operator interacts with a controller. An HMI can range from a physical control panel with buttons and indicator lights to an industrial PC with a color graphics display running dedicated HMI software.

Incident: An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. Source: [OMB Memorandum M-17-12](#); [DoWI 8530.03](#)

Integrity: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. Source: CNSSI 4009-2022; 44 U.S.C § 3552.

Local Area Network (LAN): A group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables any device to interact with any other on the network.

Machine Controller: A control system or motion network that electronically synchronizes drives within a machine system instead of relying on synchronization via mechanical linkage.

Mission Owner (MO): Mission Owners are entities such as IT system/ owner/operators or program managers within the DoW Components/Agencies responsible for instantiating and operating one or more information systems and applications who may leverage a control system in fulfillment of their IT missions. In this context, the Mission Owner is not the DoW Enterprise or DoW Component/Agency Enterprise even though these entities may control and have oversight for Component/Agency level policies and Mission Owner's acquisitions. The Mission Owner is also responsible to the Information Owner and the information system's AO.

Non-DoW Control System /Acquired or third-party Control System: refers to a commercial or Federal Government owned and operated control system.

Physical ICS: a control system including associated instrumentation, devices, networks, and controls that have the capability to directly interact with and manipulate aspects of the physical world.

Programmable Logic Controller (PLC): 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, communication, arithmetic, and data and file processing.

Risk Assessment: A systematic examination of risk using disciplined processes, methods, and tools. A risk assessment provides an environment for decision makers to evaluate and prioritize risks continuously and to recommend strategies to remediate or mitigate those risks.

Source: [CNSSI 4009-2022](#); [DoWI 8540.01](#)

Risk Management Framework (RMF): As described in DoWI 8510.01 and in accordance with NIST SP 800-37, RMF is a six-step risk-based approach to information system security, the purpose of which is compliance with various public laws including FISMA. The RMF replaces the traditional certification and accreditation C&A processes.

Remote Terminal Unit (RTU): A computer with radio interfacing used in remote situations where communication via wire is unavailable. Usually used to communicate with remote field equipment.

Supervisory Control and Data Acquisition (SCADA): A generic name for a computerized system that is capable of gathering and processing data and applying operational controls over long distances. Typical uses include power transmission and distribution and pipeline systems.

Sensor: A device that measures a physical quantity and converts it into a signal which can be read by an observer or by an instrument. A sensor is a device, which responds to an input quantity by generating a functionally related output usually in the form of an electrical or optical signal.

Supervisory Control: A term that is used to imply that the output of a controller or computer program is used as input to other controllers.

- Control system
- Mission Owner (MO)
- DoW control system
- DoW Component
- Non-DoW control system or acquired or third-party control system
- Control system service
- System criticality
- System component or control component
- Human-machine interface (HMI)
- Physical Industrial Control System (ICS)
- Control network or control center
- Control/control enhancement (C/CE)
- FRCS

System Component/Control Component: an element that contributes to the greater function of the control system and can consist of sensors, actuators, controllers, HMIs etc.

System Criticality: With relation to a superior system, system criticality refers to the effect a subsystem control system disturbance/incident/failure would have on the overall functionality of the superior system.

Appendix C Framework Glossary

Category: The subdivision of a Function into groups of cybersecurity outcomes, closely tied to programmatic needs and particular activities. Examples of Categories include “Asset Management,” “Identity Management and Access Control,” and “Detection Processes.”

Critical Infrastructure: Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on cybersecurity, national economic security, national public health or safety, or any combination of those matters.

Cybersecurity Event: A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation).

Cybersecurity Incident: A cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery

Detect (Function): Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

Framework: A risk-based approach to reducing cybersecurity risk composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. Also known as the “Cybersecurity Framework.”

Framework Core: A set of cybersecurity activities and references that are common across critical infrastructure sectors and are organized around particular outcomes. The Framework Core comprises four types of elements: Functions, Categories, Subcategories, and Informative References.

Framework Implementation Tiers: A lens through which to view the characteristics of an organization’s approach to risk – how an organization views cybersecurity risk and the processes in place to manage that risk.

Framework Profile: A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories.

Function: One of the main components of the Framework. Functions provide the highest level of structure for organizing basic cybersecurity activities into Categories and Subcategories. The five functions are Identify, Protect, Detect, Respond, and Recover.

Identify (Function): Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

Informative Reference: A specific section of standards, guidelines, and practices common among critical infrastructure sectors that illustrates a method to achieve the outcomes associated with each Subcategory. An example of an Informative Reference is ISO/IEC 27001 Control A.10.8.3, which supports the “Data-in-transit is protected” Subcategory of the “Data Security” Category in the “Protect” function.

Protect (Function): Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

Recover (Function): 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.

Respond (Function): Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

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.”