
# DEPARTMENT OF DEFENSE
# CONTROL SYSTEMS
# SECURITY REQUIREMENTS GUIDE

## Version 1, Release 1

**July 14, 2021**

**Table of Contents**

**1. Control Systems in the Department of Defense**

1.1 Introduction
1.2 Scope and Applicability
1.3 Terms and Concepts
1.4 Security Requirements Guides / Security Technical Implementation Guides
1.5 Document Revisions, Comments, Availability Update Cycle
1.6 Business Mission Objectives for Control Systems
1.7 System Security Objectives for Control Systems
1.8 Control System Security Architecture
1.9 Cybersecurity Governance for Control Systems
1.10 System Authorization for Control Systems
1.11 Cyberspace Defense and Incident Response in the Control System Environment
1.12 Control System Incident Response

**2. Cybersecurity Framework Control Systems Organizational Profile**

2.1 Cybersecurity Profile Purpose and Scope
2.2 CSF Profile Priority Matrix
2.3 CSF High Priority Rationale

**3. System Security Requirements for Control Systems**

3.1 Minimum Standards for Cybersecurity
3.2 Adapted Scope and Intent of Security Control Families
3.3 DoD Policy Regarding Security Controls
3.4 System Security Requirements Mapping Tables

**Appendices**

A) References
B) Glossary
C) NIST Cybersecurity Framework Glossary

# 1 CONTROL SYSTEMS IN THE DEPARTMENT OF DEFENSE (DoD)

## 1.1 Introduction

Control systems underpin the operation of all DoD missions and are key elements in many diverse DoD operating environments. Control systems – 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 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 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 is a priority and those dependencies should be a factor for all system owners when managing risks to their systems.

The Control Systems Security Requirements Guide (SRG) seeks to streamline and unify the Department's risk-based approach to managing control systems' cybersecurity. It utilizes and integrates the Cybersecurity Framework (CSF) to aid organizational risk management and the DoD 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 activities for all control systems in the DoD in addition to providing guidance on security requirements for control systems, regardless of individual system type or unique operating environment. This broader approach is necessary to enhance planning and overall execution of cybersecurity risk

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

management for control systems as cybersecurity maturity in many of these systems is minimal or technically unfeasible in contrast to traditional systems.

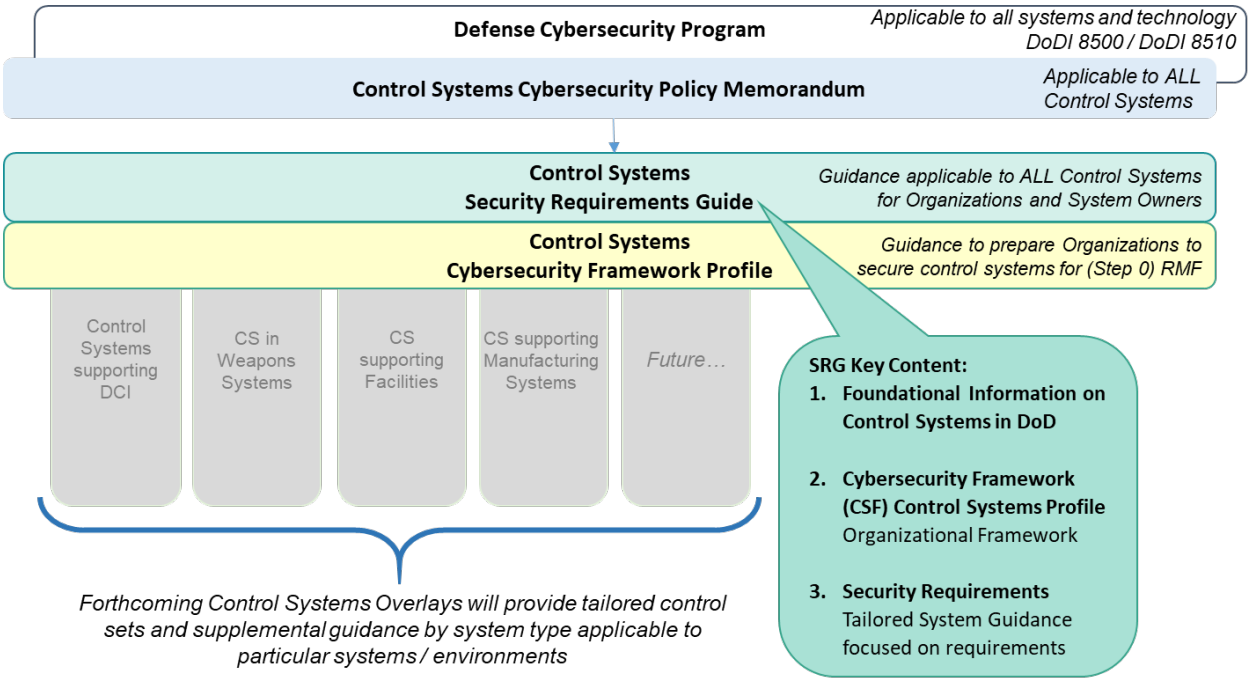
The audience for this SRG includes:

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

### 1.2 Scope and Applicability

This SRG, in support of DoDI 8510.01, establishes the DoD security objectives for all control systems. Personnel may apply this SRG to environments classified as publicly releasable up to and including TOP SECRET General Service (GENSER). Missions including control systems with a Sensitive Compartmented Information (SCI) classification must follow existing DoD 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 DoD 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 DoD SRG applies to all control systems operated by or on behalf of the DoD by a contractor or other entity. The SRG does not apply retroactively to already-fielded systems; however, the guidance should be leveraged as DoD control systems undergo updates, upgrades, and enhancements, where feasible.

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

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

This DoD SRG complements the existing RMF procedures for cybersecurity programs described in DoDI 8500.01, *Cybersecurity*, by providing consistent requirements based on common strategic objectives for deploying Control Systems and the cybersecurity activities that are most critical for meeting those objectives. Each DoD organization retains the autonomy to determine its own risk tolerance for Control Systems using the policy requirements articulated by the DoDI 8500 series, guidelines found on the RMF KS, and the parameters of organization-specific cybersecurity programs, and can adjust the requirements in this DoD 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 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 environments rather than apply traditional information system methods that may not be applicable to control system environments.

Control systems are systems in which deliberate guidance or manipulation is used to achieve a prescribed value for a variable. Control systems include Supervisory Control and Data Acquisition (SCADA), industrial and process controls systems, cyber-physical systems, facilities-related control systems and other types of industrial measurement and control systems. Control systems 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 implementation that support DoD 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 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. Essential characteristics of a control system 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 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.

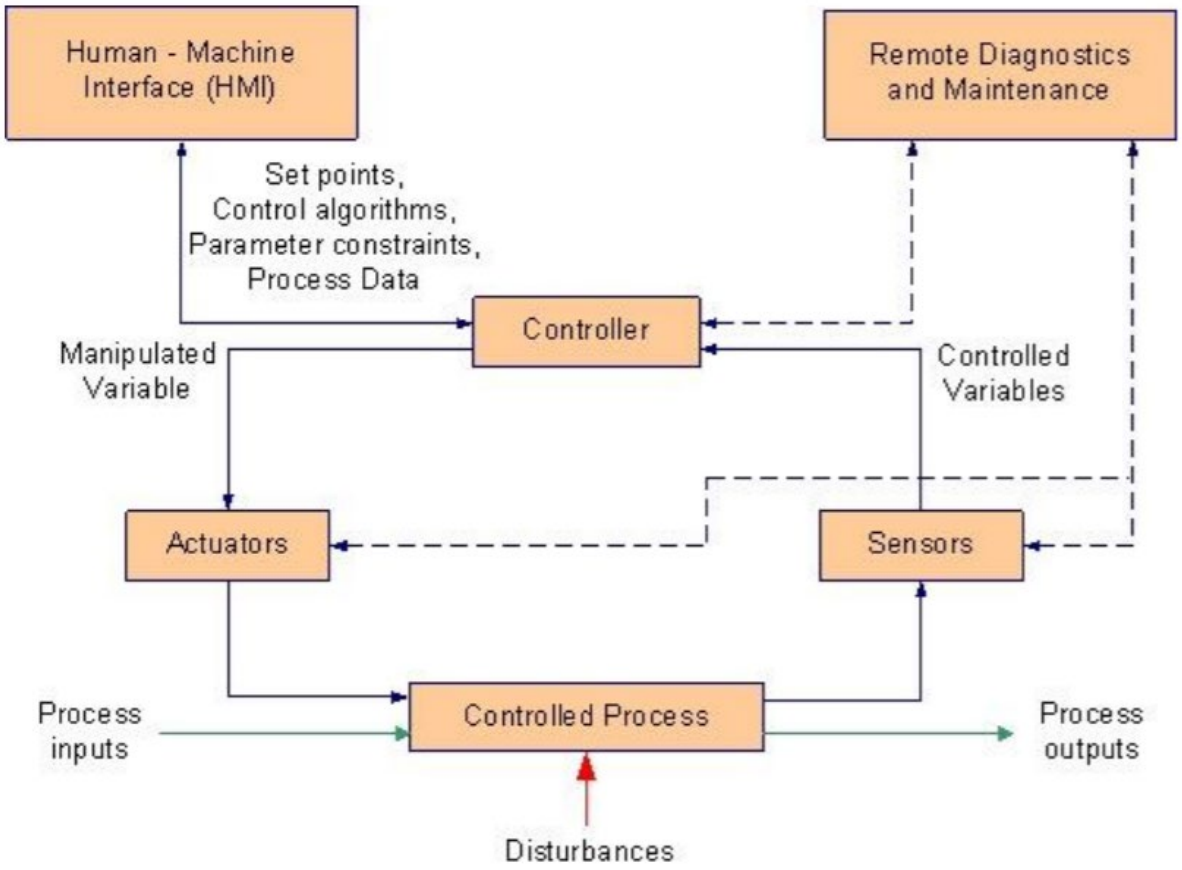



**Figure 1: NIST 800-82 (Fig. 2-1 Control System Components)**

These key components are what allow control systems 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 types that can be implemented individually or in concordance with one another. NIST SP 800-82 defines these control system 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 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. 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 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 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 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 that regulates electricity distribution would prioritize availability controls. As a result, NIST SP 800-82, lists the following factors as additional considerations when developing a control system design:

**Control timing:** Control system 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.

DoD Components must understand these additional considerations when integrating control systems 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. DoD 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 DoD-administered systems, all systems connected to DoD networks, and all systems operated or administrated on behalf of the DoD. Mission Owners must meet this requirement for all control

systems. The intent is to pursue more specific STIGs for particular control system 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 DoDI 8500.01, DISA performs this role on behalf of DoD under the authority, direction, and control of the DoD 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 DoDI 8500.01, the RMF TAG Secretariat has developed this document on behalf of DoD under the authority, direction, and control of the DoD CIO.

For this document, the RMF TAG Secretariat coordinates all change requests with relevant DoD 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 DoD 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.rmf-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 assessment, starting after the release of the Control Systems SRG update, will be assessed against the updated requirements.
- Control systems currently in the process of being assessed against the requirements in the previous Control Systems SRG will continue on this track but must transition to compliance with the current Control Systems SRG update in coordination with their next DoD annual assessment.
- Control systems currently in continuous monitoring under the previous Control Systems SRG will provide a Plan of Action and Milestones (POA&M) within 30 days for becoming compliant with the current Control Systems SRG requirements as soon as possible, but no later than, their next DoD annual assessment if scheduled six months after the Control Systems 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 DoD control systems' processes and risk management activities.

### 1.6 Business Mission Objectives for Control Systems

The following Business/Mission Objectives enable DoD to broadly express the business goals and targeted outcomes of DoD organizations utilizing control system 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 DoD control systems, which appears in Section 2.2 of this DoD SRG. Business/Mission Objectives do not replace any DoD 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 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. Additionally, operational safety to both personnel and the environment are of great importance to organizations operating control systems given the degree to which control systems interact with the physical world. As such, the DoD developed the following Business/Mission Objectives for organizations operating control systems:

***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 that pose cybersecurity risks that threaten system availability.
- Initiate risk management procedures related to control systems' 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 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 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 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 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. Preventing unauthorized access to a control system environment and preventing damage or tampering with physical assets directly related to the control system 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 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 environment.
- Apply Continuous Monitoring to physical assets associated with the control system 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 environments they protect.
- Ensure that physical security personnel are aware of which areas of a control system 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

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 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 Security Architecture

The reference architecture below (Figure 2) is the 5-level Control System 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. For many Department control systems the 5L- Control Systems reference architecture is a key tool for understanding the layering aspect of control system security architecture and IP/non-IP delineation; however, this architecture may not be a useful representation for all control system environments. Given the diversity of control systems in their complexity and capabilities, this architecture will not apply to all DoD control systems. Rather, the architecture can be used to understand key security architecture concepts that may benefit system owners when securing their control system environments.

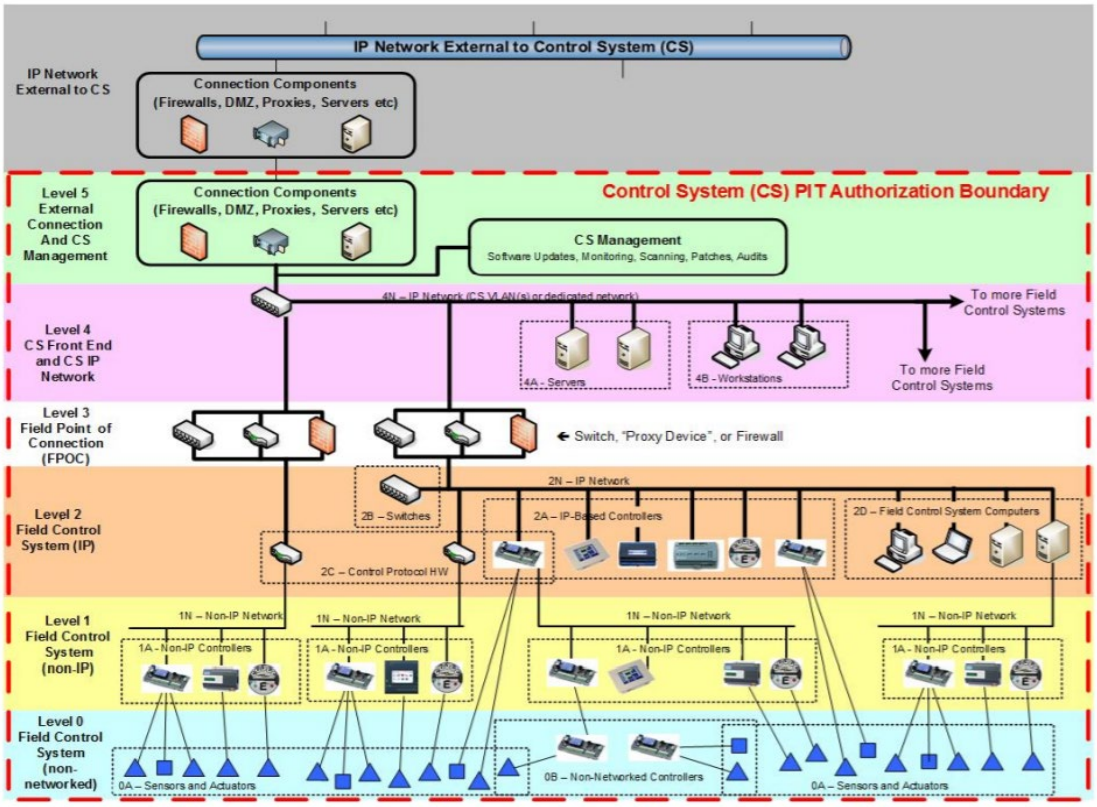



**Figure 2: UFC-4-101-06 (5-Level Control System Architecture)**

In designing and implementing secure control system security architectures, DoD 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.

DoD 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 environment. Control systems differ from traditional IT in their common attack vectors and the security needs to avoid exploitation. A list of common control system 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 encompasses a multitude of systems with varying degrees of complexity, connectivity, and security needs. Control systems are utilized across business mission functions ranging from weapons systems to medical and facilities purposes. While control systems operate across a broad spectrum of environments, the following design principles should be incorporated where applicable across all control system 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 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 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.

***Firewalls:*** Control the flow of network traffic between networks employing differing security postures. This is critical for any control system environment where data flows to and from a control system and amongst systems with differing security needs. Firewalls can restrict control system 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 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 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 network to be entirely separated from the corporate network. If communication between the control 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 environment is critical in creating a secure control system architecture.

### 1.9 Cybersecurity Governance for Control Systems

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

The Information Security Risk Management Committee (ISRMC) is a DoD entity that performs the DoD Risk Executive Function. The panel provides strategic guidance to Tiers 2 (Mission/Business Processes) and 3 (Systems) of the DoD 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 DoD 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 DoD Information Enterprise.

**1.10 System Authorization of Control Systems**

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

1. Control System (at Boundary)
    a. In this case all internal connections and field control systems are system components within the control system Authorization Boundary requiring an ATO

2. Control Systems Components (of a Larger System Boundary)
    a. In this case the control systems components may leverage the Assess Only approach (Ref: https://rmfks.osd.mil/rmf/guidance/Pages/AssessOnly.aspx)

As with any system, control system 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 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, DoD needs to know the type, quantity and purpose of control system it owns and uses. Type authorization for DoD control systems 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 DoD 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. (Ref: https://rmfks.osd.mil/rmf/RMFImplementation/ImplementControls/Pages/TypeAuthorization.aspx)

The benefit of leveraging reciprocal use of an authorized control system 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 DoD artifacts to understand the risks that the mission will inherit when using the selected control system 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 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 DoD systems and data. DoD cyberspace defense actions provide the means to react to threats and incidents to defend the DoD Information Network (DODIN). This section addresses critical cyberspace defense actions; roles and responsibilities; incident reporting and response; and other cybersecurity processes relevant to control systems.

DoD operates a cybersecurity structure as defined in DoDI 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations". The structure establishes United States Cyber Command (USCYBERCOM) and Joint Forces Headquarters DoDIN (JFHQ-DoDIN) with directive oversight of a network of Cybersecurity Service Providers (CSSPs), accredited by USCYBERCOM, IAW DoD policy. Each DoD 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 DoD 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 DoD 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 DoD 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 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 DoD 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 DoD 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 DoD 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. However, the CSF provides an opportunity to provide a link between cybersecurity activities and DoD 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 DoD 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 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 an organizational understanding to manage cybersecurity risk to systems, people, 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 appropriate safeguards to ensure delivery of critical services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event.

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

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

***Recover –*** Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. 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 DoD control systems. 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 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 in table-1 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 ••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | Informative References |
|---|---|---|---|---|---|---|---|---|---|
| | | | | 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. | • **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.<br>•• **Moderate:** Employ data flow mapping techniques, Enterprise Resource Planning software. Evaluate | **ID.AM-1:** Physical devices and systems within the organization are inventoried | ••• | ••• | •• | •• | ••• | DoDI 8530.01, DoDI 8320.03, DoDI 5000.64 |
| | | | **ID.AM-2:** Software platforms and applications within the organization are inventoried | ••• | ••• | • | • | • | DoDI 8530.01 |
| | | | **ID.AM-3:** Organizational communication and data flows are mapped | ••• | ••• | ••• | • | • | DoDI 8530.01 |

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 DoD 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 DoD 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 ••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | Informative References |
|---|---|---|---|---|---|---|---|---|---|
| | | | | 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. | • **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.<br><br>•• **Moderate:** Employ data flow mapping techniques, Enterprise Resource Planning software. Evaluate | **ID.AM-1:** Physical devices and systems within the organization are inventoried | ••• | ••• | •• | •• | ••• | DoDI 8530.01, DoDI 8320.03, DoDI 5000.64 |
| | | | **ID.AM-2:** Software platforms and applications within the organization are inventoried | ••• | ••• | • | • | • | DoDI 8530.01 |
| | | | **ID.AM-3:** Organizational communication and data flows are mapped | ••• | ••• | ••• | • | • | DoDI 8530.01 |

| Function | Category | Criticality | Subcategory | Mission Objectives ••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | Informative References |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Security | |
| | | personnel that have cybersecurity roles and responsibilities. Identify individuals who are both responsible and accountable for administering control systems.<br><br>••• **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 | ••• | ••• | • | • | ••• | DoDI 5000.64 |
| | | | **ID.AM-5:** Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value | ••• | ••• | ••• | ••• | ••• | DoDI 8530.01 |
| | | | **ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established | •• | •• | • | • | •• | DoDD 8140.01, DoDD 8140.01 |

| Function | Category | Criticality | Subcategory | Mission Objectives ••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | Informative References |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Security | |
| | **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. | • **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 DoD control system missions, objectives, and activities with consideration for security. Have awareness of critical business functions and their dependencies.<br><br>•• **Moderate:** Understand typical failures that occur to control systems and dependencies. Establish | **ID.BE-1:** The organization's role in the supply chain is identified and communicated | •• | •• | • | • | • | DoDI 5200.44 |
| | | | **ID.BE-2:** The organization's place in critical infrastructure and its industry sector is identified and communicated | ••• | •• | • | •• | •• | DoDI 3020.45 |

| Function | Category | Criticality | Subcategory | Mission Objectives ••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | Informative References |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Security | |
| | | recovery metrics to inform reliance efforts by specifying recovery objectives (Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs)) for the control system environment and component control systems involved based on typical business needs. Identify critical control system components and functions by performing a criticality analysis.<br><br>••• **High:** Protect against threats to the control system environment by employing security safeguards as part of a | **ID.BE-3:** Priorities for organizational mission, objectives, and activities are established and communicated | •• | •• | ••• | •• | •• | Prioritized at the Component or organization level |
| | | | **ID.BE-4**: Dependencies and critical functions for delivery of critical services are established | ••• | ••• | • | • | •• | DoDI 8530.01, DoDI 8500.01, DoD O-8530.01-M |

| Function | Category | Criticality | Subcategory | Mission Objectives ••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | Informative References |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Security | |
| | | comprehensive, defense-in-depth security strategy. Conduct contingency planning for the continuance of essential control system functions and services with little or no loss of operational continuity that sustains until full system restoration. | **ID.BE-5**: Resilience requirements to support delivery of critical services are established | ••• | ••• | • | • | ••• | DoDD 3020.40 |
| | **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 | • **Low:** Apply DoD-level and Component cybersecurity policy and local risk governance processes. Address risk from an IS and PIT system perspective that is guided by risk decisions at Tiers 1 and 2 in accordance with DODI 8500.01.Assure the policy is approved by necessary entities or senior officials with responsibility and accountability for the risk | **ID.GV-1:** Organizational information security policy is established | ••• | ••• | • | • | •• | DoDI 8500.01 |
| | | | **ID.GV-2:** Information security roles & responsibilities are coordinated and aligned with internal roles and external partners | •• | •• | • | • | •• | DoDI 8500.01 |

| Function | Category | Criticality | Subcategory | Mission Objectives ••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | Informative References |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Security | |
| | management of cybersecurity risk. | incurred by control system operations.<br><br>•• **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 accordance with DODI 8500.01.<br><br>••• **High:** Address risk from an organizational perspective that is informed and influenced by risk decisions made in Tiers 2 and 3, in accordance with DODI 8500.01. | **ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed | •• | •• | •• | • | •• | DoDI 5144.02 |
| | | | **ID.GV-4**: Governance and risk management processes address cybersecurity risks | ••• | ••• | • | • | ••• | DoDI 8510.01 |

| Function | Category | Criticality | Subcategory | Mission Objectives •••= High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | Informative References |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Security | |
| | **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 DoD 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 informed by their impact to operations, assets, and individuals. Establish risk tolerances to mitigate with | **ID.RA-1:** Asset vulnerabilities are identified and documented | •• | •• | •• | •• | •• | DoDI 3020.01, DoDI 8510.01 |
| | | | **ID.RA-2:** Threat and vulnerability information is received from information sharing forums and sources | •• | •• | •• | •• | •• | DoDI 8500.01, DoDI 8530.01 |
| | | | **ID.RA-3:** Threats, both internal and external, are identified and documented | ••• | ••• | ••• | ••• | ••• | DoDI 8500.01, DoDI 8530.01 |
| | | | **ID.RA-4:** Potential business impacts and likelihoods are identified | ••• | •• | • | • | •• | DoDI 8500.01, DoDI 8510.01 |

| Function | Category | Criticality | Subcategory | Mission Objectives ••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | Informative References |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Security | |
| | | 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-5**: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk | ••• | ••• | ••• | ••• | ••• | DoDI 8500.01, DoDI 8510.01 |
| | | | **ID.RA-6:** Risk responses are identified and prioritized | ••• | ••• | ••• | ••• | ••• | DoDI 8500.01, DoDI 8510.01 |
| | **Risk Management Strategy (ID.RM):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. | | **ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders | •• | •• | •• | • | •• | DoDI 8500.01, DoDI 8510.01 |
| | | | **ID.RM-2:** Organizational risk tolerance is determined and clearly expressed | •• | •• | •• | •• | •• | DoDI 8500.01, DoDI 8510.01 |

| Function | Category | Criticality | Subcategory | Mission Objectives ••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | Informative References |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Security | |
| | | | **ID.RM-3**: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis | •• | •• | • | • | •• | DoDI 8500.01, DoDI 8510.01 |

| Function | Category | Criticality | Subcategory | Mission Objectives •••= High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | Informative References |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Safety | |
| **PROTECT (PR)** | **Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions. | • **Low:** Establish and manage identification mechanisms and credentials for users of assets and facilities of control systems. Define and manage access permissions for users of the control systems including emergency situations.<br><br>Protect physical access to control system assets or facilities . Maintain and review visitor access records to control system related facilities .<br><br>Establish usage restrictions, connection requirements, implementation guidance, and authorizations for remote access to control systems. Use secure protocols for any remote access activity where feasible. Protect network integrity of the control system | **PR.AC-1: I**dentities and credentials are managed for authorized devices and users | •• | ••• | • | • | ••• | DoDI 8520.03, DoDI 8500.01 DoDD 8521.01; |
| | | | **PR.AC-2:** Physical access to assets is managed and protected | ••• | ••• | ••• | ••• | ••• | DoDI 8520.03, DoDD 8521.01, DoDI 8500.01 |

| Function | Category | Criticality | Subcategory | Mission Objectives ••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | Informative References |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Safety | |
| | | and incorporate network segmentation where appropriate.<br><br>•• **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).<br><br>Only allow remote access through approved and managed devices or access points while employing multi-factor authentication for authorized personnel where feasible. Limit and monitor connections to the control system while allowing only connections necessary to system functionality and only allowing connections to approved management interfaces (HMI).<br><br>Audit the execution of privileged functions on the | **PR.AC-3:** Remote access is managed | ••• | ••• | • | • | •• | JIE Enterprise Remote Access STIG, v1 and Release Memo, DoDI 8500.01, DoDD 8521.01 |
| | | | **PR.AC-4:** Access permissions are managed, incorporating the principles of least privilege and separation of duties | ••• | ••• | • | • | ••• | DoDI 8520.03, DoDI 8500.01, DoDD 8521.01 |

| Function | Category | Criticality | Subcategory | Mission Objectives ••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | Informative References |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Safety | |
| | | control system environment.<br><br>••• **High:** Monitor control systems 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).<br><br>Employ strict access controls to control systems to enhance the physical protection of the control system facility. Maintain logs of all remote access activity and only allow the use of privileged functions for control systems via authorized remote access<br><br>Protect all components of a DoD control system from accidental damage, disruption, and physical tampering. Employ redundant and physically separated power supplies for control systems essential to business operations.<br><br>Airgap the control system | **PR.AC-5:** Network integrity is protected, incorporating network segregation where appropriate | ••• | ••• | • | • | •• | DoDI 8520.03, DoDI 8500.01, DoDD 8521.01 |
| | | | **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, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and | | | | | | |

| Function | Category | Criticality | Subcategory | Mission Objectives ••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | Informative References |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Safety | |
| | | environment where feasible to limit external connections to only those both necessary for system functionality and beneficial to operational continuity. | other organizational risks) | | | | | | |
| | **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. | • **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.<br><br>•• **Moderate:** Require service providers to identify the functions, ports, protocols, and services necessary for connection services. .<br><br>••• **High:** Perform personnel and service provider testing and exercises. | **PR.AT-1:** All users are informed and trained | ••• | ••• | ••• | ••• | ••• | DoDI 8500.01 |
| | | | **PR.AT-2:** Privileged users understand roles & responsibilities | •• | •• | •• | •• | •• | DoDI 8500.01. DoD 8570.01-M, DoDD 8140.01 |
| | | | **PR.AT-3:** Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities | •• | •• | •• | •• | •• | DoDD 8570.01-M |
| | | | **PR.AT-4:** Senior executives understand roles & responsibilities | •• | •• | •• | •• | •• | DoDD 8140.01, DoD 8570.01-M |
| | | | **PR.AT-5:** Physical and information security personnel understand roles & responsibilities | ••• | •• | •• | •• | ••• | DoDD 8140.01, DoD 8570.01-M |

| Function | Category | Criticality | Subcategory | Mission Objectives<br>••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | Informative References |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Safety | |
| | **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. | • **Low:** Enforce accountability for all control system components throughout the system lifecycle, including removal, transfers, and disposal. Protect any information at rest critical to business operations. Ensure the control system environment has adequate resources available to accommodate business functionality (e.g., information processing, networking, and data storage if necessary). Protect the control system from data leakage by developing and documenting access agreements for all users of control systems. When implementing any major change to a control system configuration in an off-line setting where the changes are tested prior to integration into the control system environment.<br><br>•• **Moderate:** Protect control systems' data when in transit. | **PR.DS-1:** Data-at-rest is protected | • | ••• | • | • | • | DoDD 8100.02; DoDI 8420.01 |
| | | | **PR.DS-2:** Data-in-transit is protected | •• | ••• | • | • | • | DoDD 8100.02; DoDI 8420.01 |
| | | | **PR.DS-3:** Assets are formally managed throughout removal, transfers, and disposition | •• | ••• | • | • | •• | DoDI 8500.01 |
| | | | **PR.DS-4:** Adequate capacity to ensure availability is maintained | ••• | • | • | • | •• | DoDI 8500.01 |

| Function | Category | Criticality | Subcategory | Mission Objectives ••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | Informative References |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Safety | |
| | | Implement cryptographic mechanisms where determined necessary to prevent unauthorized access, distortion, or modification of system data and audit records. Update the inventory of control system components as an integral part of the component installations, removals, and system updates. Ensure availability is maintained by protecting the control system against denial of service (DoS) attacks. 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 environment.<br><br>••• **High:** Employ automated tools, where feasible, to provide notification upon discovering discrepancies during integrity verification. Employ automated response capability with pre-defined security safeguards when | **PR.DS-5:** Protections against data leaks are implemented | • | •• | • | • | •• | DoDI 8500.01 |
| | | | **PR.DS-6:** Integrity checking mechanisms are used to verify software, firmware, and information integrity | •• | ••• | • | • | • | DoDI 8500.01 |
| | | | **PR.DS-7:** The development and testing environment(s) are separate from the production environment | ••• | ••• | •• | •• | •• | D0DI 5000.02 |

| Function | Category | Criticality | Subcategory | Mission Objectives ••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | Informative References |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Safety | |
| | | integrity violations are discovered. | | | | | | | |
| | **Information Protection Processes and Procedures (PR.IP):** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and | • **Low:** Develop, document, and maintain a baseline configuration for control systems. Manage control systems using a system development life cycle provided by guidance from the control system vendor that includes security considerations (PR.IP-2). Employ configuration change control and security impact analyses for control systems and its components. Conduct and maintain backups | **PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained | ••• | ••• | • | • | • | DoD 8310.01 |

| Function | Category | Criticality | Subcategory | Mission Objectives ••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | Informative References |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Safety | |
| | coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets. | for control system data. Ensure safe handling of system data including the destruction of data according to policy (PR.IP-3).<br><br>Require the developer of the control system 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. Employ configuration management and change control during the development of the control system environment and its components the includes flaw tracking and resolution and | **PR.IP-2:** A System Development Life Cycle to manage systems is implemented | •• | •• | • | • | •• | DoDI 8580.01, DoDI 5000.02; DoDI 5200.44 |
| | | | **PR.IP-3:** Configuration change control processes are in place | ••• | ••• | • | • | ••• | DoDI 5200.44 |

| Function | Category | Criticality | Subcategory | Mission Objectives<br>••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | Informative References |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Safety | |
| | | security testing, where feasible (PR.IP-2).<br><br>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.IP-9). Review response and recovery plans to determine the effectiveness of, and the readiness to execute the plans (PR.IP-10).<br><br>Define, implement, and enforce policy and regulations regarding emergency and safety systems, fire protection | **PR.IP-4:** Backups of information are conducted, maintained, and tested periodically | ••• | ••• | • | • | • | DoDI 3020.26 |
| | | | **PR.IP-5:** Policy and regulations regarding the physical operating environment for organizational assets are met | ••• | •• | ••• | ••• | ••• | DoDI 8500.01 |

| Function | Category | Criticality | Subcategory | Mission Objectives ••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | Informative References |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Safety | |
| | | systems, and environment controls for control systems. Fire suppression mechanisms should take the control system environment into account (e.g., water sprinkler systems could be hazardous in specific environments) (PR.IP-5)<br><br>Incorporate improvements derived from the monitoring, measurements, assessments, and lessons learned into protection process revisions. Ensure that the security plan for the control system environment facilitates reviewing, testing, and the continual improvement of the security protection processes (PR.IP-7).<br><br>Develop and maintain a personnel security program for control system environments (PR.IP-11). | **PR.IP-6:** Data is destroyed according to policy | •• | •• | • | • | • | DoDI 8500.01 |
| | | | **PR.IP-7:** Protection processes are continuously improved | •• | •• | •• | •• | •• | DoDI 8500.01 |

| Function | Category | Criticality | Subcategory | Mission Objectives<br>••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | Informative References |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Safety | |
| | | Establish and maintain a process that continuously reviews vulnerabilities and their exposure to adversaries, and defines strategies to mitigate them (PR.IP-12).<br><br>•• **Moderate:** Review and update the baseline configurations of the control systems as an integral part of system component installations and upgrades. Retain previous versions of the baseline configurations to allow for rollback. Develop configuration management plans for control system 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 | **PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties | • | • | • | • | • | DoDI 8500.01 |
| | | | **PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed | ••• | ••• | ••• | ••• | ••• | DoDI 8500.01, DoDI 3020.26 |

| Function | Category | Criticality | Subcategory | Mission Objectives ••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | Informative References |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Safety | |
| | | 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).<br><br>Test, validate, and document changes to the control system environment before implementing the changes on the component control system. Review and authorize proposed configuration-controlled changes prior to implementing them on the control system environment (PR.IP-3).<br><br>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). | **PR.IP-10:** Response and recovery plans are tested | •• | •• | •• | •• | •• | DoDI 8500.01 |
| | | | **PR.IP-11:** Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) | •• | •• | •• | •• | •• | DoDI 8500.01, DoDD 8140, DoDI 5000.02 Encl. 13, DoD 8570.01-M |

| Function | Category | Criticality | Subcategory | Mission Objectives ••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | Informative References |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Safety | |
| | | Coordinate contingency and response and recovery plan development, testing and execution with stakeholders responsible for related plans(PR.IP-9).<br><br>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).<br>Restrict access to privileged vulnerability data (PR.IP-12).<br><br>••• **High:** Conduct security impact analysis in a separate test environment before implementation into an operational environment for planned changes to control systems.<br><br>Employ automated mechanisms where feasible to maintain an up-to-date, complete, accurate, and readily available baseline configuration of control systems. Automated | **PR.IP-12:** A vulnerability management plan is developed and implemented | ••• | ••• | •• | •• | ••• | DoDI 8500.01, DoDI 8530.02; DoD 8570.01-M |

| Function | Category | Criticality | Subcategory | Mission Objectives ••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | Informative References |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Safety | |
| | | system support includes for example, documentation, notification, and management of the change control process on control systems (PR.IP-3).<br><br>Review system changes to determine whether unauthorized changes have occurred (PR.IP-1).<br>Include restorations from backup data into contingency plan testing (PR.IP-4).<br><br>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 environment, when feasible (PR.IP-6). | | | | | | | |

| Function | Category | Criticality | Subcategory | Mission Objectives<br>••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | Informative References |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Safety | |
| | **Maintenance (PR.MA):** Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures. | • **Low:** Establish a process for maintenance personnel authorization and escort non-authorized 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.<br><br>•• **Moderate:** Schedule, perform, document and review records of maintenance and repairs to control system components. Enforce approval requirements, control, and monitoring of maintenance | **PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools | •• | •• | ••• | ••• | ••• | DoDI 8500.01 |

| Function | Category | Criticality | Subcategory | Mission Objectives ••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | Informative References |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Safety | |
| | | tools for use on control systems, where feasible. Maintenance tools can include, for example, hardware/software diagnostic test equipment, hardware/software packet sniffers and laptops.<br><br>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.<br><br>••• **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 information. Require that diagnostic services pertaining to remote maintenance be performed from a system that implements | **PR.MA-2:** Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access | ••• | ••• | •• | •• | •• | DoDI 8500.01 |

| Function | Category | Criticality | Subcategory | Mission Objectives ••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | Informative References |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Safety | |
| | | a security capability comparable to the capability implemented on the control system. | | | | | | | |

| Function | Category | Criticality | Subcategory | Mission Objectives<br>••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | Informative References |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Safety | |
| | **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. | • **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.<br><br>•• **Moderate:** Audit logs are reviewed and updated after cybersecurity related events. Disable defined functions, ports, protocols, and services within the control systems 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.<br><br>Control the flow of information within control systems and between interconnected systems.<br><br>••• **High:** Integrate audit logs with physical access monitoring. Employ automated | **PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | ••• | ••• | • | • | • | DoDI 8500.01 |
| | | | **PR.PT-2:** Removable media is protected and its use restricted according to policy | •• | ••• | • | • | •• | DoDI 8540.01; Removable Storage and External Connections STIG,, DoD 5200.01, v3 |
| | | | **PR.PT-3:** Access to systems and assets is controlled, incorporating the principle of least functionality | ••• | •• | •• | •• | ••• | DoDI 8500.01 |

| Function | Category | Criticality | Subcategory | Mission Objectives ••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | Informative References |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Safety | |
| | | mechanisms to integrate audit review, analysis, and reporting. Scan all portable storage devices for malicious code before use on control systems. Limit external connections to the control system 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 | ••• | ••• | •• | •• | •• | DoDI 8550.01 |

| Function | Category | Criticality | Subcategory | Mission Objectives ••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | DoD Document Cache |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Safety | |
| **DETECT (DE)** | **Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood. | • **Low:** Ensure that a baseline awareness of network operations and expected data flows for control systems is developed and maintained to detect events. Review and analyze detected events within the control system environment to understand attack targets and methods.<br><br>Define incident alert thresholds for control systems and determine negative impacts to DoD operations, assets, and individuals resulting from detected events.<br><br>•• **Moderate:** Ensure that event data is compiled and correlated across the control system environment using various sources such as event reports, audit monitoring, network monitoring, physical access monitoring, and | **DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed | ••• | •• | • | • | • | DoDI 8320.02, DoDI 8330.01, DoD 8530.01 |
| | | | **DE.AE-2:** Detected events are analyzed to understand attack targets and methods | •• | •• | •• | •• | •• | DoDI 8530.01, DoDI S-5240.23, CJCSM 6510.01B |
| | | | **DE.AE-3:** Event data are aggregated and correlated from multiple sources and sensors | •• | •• | •• | •• | •• | DoDI 8530.01, CJCSM 6510.01B |

| Function | Category | Criticality | Subcategory | Mission Objectives ••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | DoD Document Cache |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Safety | |
| | | user/administrator reports.<br><br>••• **High:** Integrate analysis of events and vulnerability scanning information, performance data, control system monitoring and other monitoring systems to enhance the ability to identify unusual activity.<br><br>Collate detected event information and responses to achieve perspective on event impact across the organization.<br><br>Employ automated mechanisms to assist in the identification of security alert thresholds and to support impact analysis, where feasible. | **DE.AE-4:** Impact of events is determined | ••• | ••• | ••• | ••• | ••• | DoDI 8560.01, CJCSM 6510.01B; DoDI 8530.01 |
| | | | **DE.AE-5:** Incident alert thresholds are established | • | • | •• | •• | •• | DoDI 8510.01, DoDI 8530.01 |
| | **Security Continuous Monitoring (DE.CM):** The information system and | • **Low:** Where feasible, conduct ongoing security status monitoring of DoD control system environment to detect defined cybersecurity events. Detect unauthorized local, | **DE.CM-1:** The network is monitored to detect potential cybersecurity events | ••• | ••• | • | • | • | DoDI 8560.01, DoDI 8530.01, DoDI 8551.01 |

| Function | Category | Criticality | Subcategory | Mission Objectives ••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | DoD Document Cache |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Safety | |
| | assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures. | network, and remote connections to the control system environment<br><br>Employ proper personnel to monitor the security of the physical environment<br><br>Conduct ongoing security status monitoring of the control system facility to detect physical security incidents.<br>Monitor for unauthorized personnel, connections, devices, access points, and software.<br>Monitor for and report atypical usage of the control system.<br>Conduct ongoing security status monitoring of service provider activity on control systems.<br>Monitor compliance of external providers with personnel security policies and procedures, and contract security requirements.<br><br>•• **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 | ••• | ••• | •• | •• | ••• | DoD 5220.22-M, DoD 5200.08-R |
| | | | **DE.CM-3:** Personnel activity is monitored to detect potential cybersecurity events | ••• | ••• | ••• | •• | ••• | DoDI 8500.01 |
| | | | **DE.CM-4:** Malicious code is detected | ••• | ••• | • | • | • | DoDI 8510.01, CJCSM 6510.01B, DoDI 8530.01 |
| | | | **DE.CM-5:** Unauthorized mobile code is detected | •• | •• | • | • | • | DoDI 8510.01, DoDI 8530.01, CJCSM 6510.01B |

| Function | Category | Criticality | Subcategory | Mission Objectives ••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | DoD Document Cache |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Safety | |
| | | when indications of compromise or potential compromise occur.<br><br>Deploy monitoring devices strategically within the control system environment to collect essential information. Employ control system specific vulnerability scanning tools and techniques where safe and feasible.<br><br>••• **High:** Continually monitor for unauthorized configuration changes to control systems. Define and detect acceptable and unacceptable mobile code and mobile code technologies. Automatically update malicious code protection mechanisms.<br><br>Actively incorporate vulnerability scanning of network traffic and of critical control systems into the monitoring process to ensure that system functions are not adversely impacted by any threat actors. | **DE.CM-6:** External service provider activity is monitored to detect potential cybersecurity events | •• | ••• | • | • | •• | DoDI 8510.01 |
| | | | **DE.CM-7:** Monitoring for unauthorized personnel, connections, devices, and software is performed | ••• | ••• | ••• | •• | ••• | DoDI 8530.01, DoDI 8530.03, DoDI 8500.01 |
| | | | **DE.CM-8:** Vulnerability scans are performed | ••• | ••• | • | • | • | DoDI 8510.01, DoDI 8530.01, DoDI 8500.01 |

| Function | Category | Criticality | Subcategory | Mission Objectives ••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | DoD Document Cache |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Safety | |
| | **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 and ensure accountability. Conduct detection activities in accordance with applicable federal and state laws, industry regulations, standards, policies, and other applicable requirements.<br><br>Communicate event detection information to defined personnel and ensure the security plans in place for control systems provide for the review, testing, and continual improvement of security detection processes.<br><br>•• **Moderate:** Employ proper personnel to assess the detection process and validate that event detection processes are | **DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability | •• | •• | •• | •• | •• | DoDI 8500.01, DoDI 8530.01, CJCSM 6510.01B |
| | | | **DE.DP-2:** Detection activities comply with all applicable requirements | • | • | • | • | • | DoDI 8530.01, CJCSM 6510.01B |
| | | | **DE.DP-3:** Detection processes are tested | •• | •• | • | • | •• | DoDI 8500.01 |

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

| Function | Category | Criticality | Subcategory | Mission Objectives ••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | Informative References |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Safety | |
| **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 environment | **RS.RP-1:** Response plan is executed during or after an event | ••• | ••• | ••• | ••• | ••• | DoDI 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 DoD control system. Ensure that these reporting procedures are consistent with the response plan and follow any and all DoD Cybersecurity incident handling polices.<br><br>Share cybersecurity event information voluntarily, as appropriate, with DoD | **RS.CO-1:** Personnel know their roles and order of operations when a response is needed | •• | •• | ••• | • | •• | DoDD 8140.01, DoDI 8510.01 |
| | | | **RS.CO-2:** Events are reported consistent with established criteria | • | • | • | • | • | DoDI 8510.01 |

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

| Function | Category | Criticality | Subcategory | Mission Objectives ••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | Informative References |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Safety | |
| | **Analysis (RS.AN):** Analysis is conducted to ensure adequate response and support recovery activities. | •**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.<br><br>Categorize cybersecurity incidents according to level of severity and impact consistent with the response plan.<br><br>••**Moderate:** Investigate cybersecurity-related notifications generated from detection systems. Provide on-demand audit review, analysis, and reporting of cybersecurity incidents.<br><br>Conduct forensic analysis on collected cybersecurity event information to determine root cause. | **RS.AN-1:** Notifications from detection systems are investigated | •• | •• | •• | • | •• | DoDI 8510.01 |
| | | | **RS.AN-2:** The impact of the incident is understood | ••• | ••• | ••• | ••• | ••• | DoDI 8510.01 |
| | | | **RS.AN-3:** Forensics are performed | •• | •• | • | • | •• | DoDI 8510.01 |

| Function | Category | Criticality | Subcategory | Mission Objectives ••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | Informative References |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Safety | |
| | | ••• **High:** Employ automated mechanisms to assist in the investigation of a cybersecurity-related notification and support incident impact analysis, where feasible | **RS.AN-4:** Incidents are categorized consistent with response plans | •• | •• | •• | •• | •• | DoDI 8510.01 |
| | **Mitigation (RS.MI):** Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident. | • **Low: , •• Moderate:** Contain and mitigate cybersecurity incidents to minimize impact on the control system environment and business objectives. Ensure that vulnerabilities identified while responding to a cybersecurity incident are also mitigated or documented as | **RS.MI-1:** Incidents are contained | ••• | ••• | ••• | ••• | ••• | CJSCM 6510.01B |

| Function | Category | Criticality | Subcategory | Mission Objectives ••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | Informative References |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Safety | |
| | | accepted risks.<br><br>•••**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 environment. | **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 ••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | Informative References |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Safety | |
| | **Improvements (RS.IM):** Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities. | **•Low:, ••Moderate, •••High:** Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly.<br><br>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.<br><br>Enable a process for the response plan to evolve to reflect new threats, improved technology, and lessons learned. | **RS.IM-1:** Response plans incorporate lessons learned | •• | •• | •• | •• | •• | DoDI 8500.01, DoDI 8510.01 |
| | | | **RS.IM-2:** Response strategies are updated | •• | •• | •• | •• | •• | DoDI 8500.01, DoDI 8510.01 |

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

| Function | Category | Criticality | Subcategory | Mission Objectives ••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | Informative References |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Safety | |
| | **Improvements (RC.IM):** Recovery planning and processes are improved by incorporating lessons learned into future activities. | **•Low, ••Moderate, •••High:** Incorporate lessons learned from ongoing recovery activities into system recovery procedures, training, and testing. Implement the resulting changes accordingly.<br><br>Update the recovery plan to address changes to the organization, to the control systems, or to the operational environment. Document all problems encountered during plan implementation, execution, and testing. | **RC.IM-1:** Recovery plans incorporate lessons learned | •• | •• | •• | •• | •• | DoDI 8500.01, CJCSM 6510.01B |
| | | | **RC.IM-2:** Recovery strategies are updated | •• | •• | •• | •• | •• | DoDI 8500.01, CJCSM 6510.01B |
| | **Communications (RC.CO):** Restoration activities are coordinated with internal and external parties, such as coordinating | **•Low, ••Moderate, •••High:** Manage the public-facing representation of the organization or of the DoD Component through a coordinated effort. Ensure information is distributed to in a manner that is beneficial to the reputation of the organization | **RC.CO-1:** Public relations are managed | • | • | •• | • | • | DoDI 8500.01, CJCSM 6510.01B |

| Function | Category | Criticality | Subcategory | Mission Objectives ••• = High Priority, •• = Moderate Priority, • = Low Priority / Other Implemented Subcategories | | | | | Informative References |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Maintain System Availability | Maintain System Integrity | Maintain Human Safety | Maintain Environmental Safety | Maintain Physical Safety | |
| | centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors. | according to DoD policies and procedures.<br><br>Communicate recovery activities to all relevant stakeholders, and executive management teams within DoD and any external participating parties.<br><br>Assign a Public Affairs Officer and coordinate with DoD PAO. | **RC.CO-2:** Reputation after an event is repaired | •• | • | •• | • | • | DoDI 8500.01, CJCSM 6510.01B |
| | | | **RC.CO-3:** Recovery activities are communicated to internal stakeholders and executive and management teams | •• | •• | •• | •• | •• | DoDI 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 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 that pose cybersecurity risks that threaten system availability.
- Initiate risk management procedures related to control systems' 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 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 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 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 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 DoDI 8510.01's external IT service requirements that external information systems are catalogued. DoD organizations that use external IT services provided by a commercial or other non-federal government entity must ensure the security protections of the IS delivering the service is appropriate to the availability needs of the DoD 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 environment. |
| | **ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established | *Rationale only provided for High Priority Subcategories* |
| **Business Environment** | **ID.BE-1:** The organization's role in the supply chain is identified and communicated | *Rationale only provided for High Priority Subcategories* |
| | **ID.BE-2:** The organization’s place in critical infrastructure and its industry sector is identified and communicated | Control Systems are vital to the operation of the DoD and of the U.S. critical infrastructures that are often highly interconnected and mutually dependent systems. |

| Detailed Specifications | | |
|---|---|---|
| Category | Subcategory | Rationale for High Priority |
| | **ID.BE-3:** Priorities for organizational mission, objectives, and activities are established and communicated | *Rationale only provided for High Priority Subcategories* |
| | **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 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 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 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. |
| **Governance** | **ID.GV-1:** Organizational information security policy is established | It is DoD policy that: the DoD will establish and use an integrated enterprise-wide decision structure for cybersecurity risk management (the RMF) that includes and integrates DoD mission areas (MAs) pursuant to DoDD 8115.01. Without an organizational information security policy, organizations run the unacceptable risk of having either no protection of control systems or an ad-hoc, disparate policy that is not aligned with overall availability requirements of the control system environment. |

| Detailed Specifications | | |
|---|---|---|
| Category | Subcategory | Rationale for High Priority |
| | **ID.GV-2:** Information security roles & responsibilities are coordinated and aligned with internal roles and external partners | *Rationale only provided for High Priority Subcategories* |
| | **ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberty obligations, are understood and managed | *Rationale only provided for High Priority Subcategories* |
| | **ID.GV-4:** Governance and risk management processes address cybersecurity risks | It is DoD policy that: the DoD will establish and use an integrated enterprise-wide decision structure for cybersecurity risk management (the RMF) that includes and integrates DoD mission areas (MAs) pursuant to DoDD 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 or an ad-hoc, disparate policy that is not aligned with overall availability requirements of the control system environment. |
| **Risk Assessment** | **ID.RA-1:** Asset vulnerabilities are identified and documented | *Rationale only provided for High Priority Subcategories* |
| | **ID.RA-2:** Threat and vulnerability information is received from information sharing forums and sources | *Rationale only provided for High Priority Subcategories* |

| 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 and mitigating cybersecurity risks. Organizations must identify these threats to control system security throughout the lifecycle of the component control systems from architecture to procurement to installation to maintenance to decommissioning. Due to the rapidly evolving nature of control systems, it is important to identify and review new control system capabilities and their associated emerging threats, particularly to system availability. The identification process should leverage organizations that identify emerging threats such as the ICS-CERT. |
| | **ID.RA-4:** Potential business impacts and likelihoods are identified | Due to the assumption that cybersecurity events in the control system 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' processes and their strong availability requirements. |

| Detailed Specifications | | |
|---|---|---|
| Category | Subcategory | Rationale for High Priority |
| | **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 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 environment to multiple, unacceptable risks to system availability. |
| | **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 | *Rationale only provided for High Priority Subcategories* |
| | **ID.RM-2:** Organizational risk tolerance is determined and clearly expressed | *Rationale only provided for High Priority Subcategories* |

| 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 | *Rationale only provided for High Priority Subcategories* |

| Protect | For control systems, 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 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 environment. |
|---|---|

| | High Priority Subcategories | Moderate Priority Subcategories |
|---|---|---|
| Access Control | **PR.AC-2, PR.AC-3, PR.AC-4, PR.AC-5** | 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-3, PR.DS-6 |
| Information Protection Process and Procedures | **PR.IP-1, PR.IP-3, PR.IP-4, PR.IP-5, PR.IP-6, PR.IP-9, PR.IP-12** | PR.IP-2, 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 | *Rationale only provided for High Priority Subcategories* |
| | **PR.AC-2**: Physical access to assets is managed and protected | Unauthorized physical access to the control system 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 environments to prevent physical modification, manipulation, or destruction of existing system infrastructure. Any malicious tampering with the control system 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 | 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 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 environment as malicious physical access. As such, remote access must be carefully managed to maintain system availability. |
| | **PR.AC-4:** Access permissions are managed, incorporating the principles of least privilege and separation of duties | 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 environment to prevent any accidental or intentional tampering that could lead to system failure and hinder system availability. |

| 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 environment, it is beneficial to separate the control system 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 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 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 environment must receive proper training to maintain a safe control system environment. |
| | **PR.AT-2:** Privileged users understand roles & responsibilities | *Rationale only provided for High Priority Subcategories* |

| Detailed Specifications | | |
|---|---|---|
| Category | Subcategory | Rationale for High Priority |
| | **PR.AT-3**: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities | *Rationale only provided for High Priority Subcategories* |
| | **PR.AT-4:** Senior executives understand roles & responsibilities | *Rationale only provided for High Priority Subcategories* |
| | **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 environment and are aware of the risks of and threats to the control system environment. Particularly with control systems, 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 reasonability to protect control systems. |
| **Data Security** | **PR.DS-3**: Assets are formally managed throughout removal, transfers, and disposition | *Rationale only provided for High Priority Subcategories* |

| Detailed Specifications | | |
|---|---|---|
| Category | Subcategory | Rationale for High Priority |
| | **PR.DS-4:** Adequate capacity to ensure availability is maintained | 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 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 environment with adequate capacity (computing power, networking capability, storage space, etc.) is essential to maintain system availability. |
| | **PR.DS-6**: Integrity checking mechanisms are used to verify software, firmware, and information integrity | *Rationale only provided for High Priority Subcategories* |
| | **PR.DS-7:** The development and testing environment(s) are separate from the production environment | 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 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 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. |

| Detailed Specifications | | |
|---|---|---|
| Category | Subcategory | Rationale for High Priority |
| **Information Protection Process and Procedures** | **PR.IP-1:** A baseline configuration of information technology/industrial control systems 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 environment. Each of these factors contribute to supporting system availability and business continuity. Without a baseline configuration for the control system 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 | *Rationale only provided for High Priority Subcategories* |
| | **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 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 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 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 environment is maintained. |
| | **PR.IP-6:** Data is destroyed according to policy | *Rationale only provided for High Priority Subcategories* |
| | **PR.IP-7:** Protection processes are continuously improved | *Rationale only provided for High Priority Subcategories* |
| | **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. |

| Detailed Specifications | | |
|---|---|---|
| Category | Subcategory | Rationale for High Priority |
| | **PR.IP-10:** Response and recovery plans are tested | *Rationale only provided for High Priority Subcategories* |
| | **PR.IP-11:** Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) | *Rationale only provided for High Priority Subcategories* |
| | **PR.IP-12:** A vulnerability management plan is developed and implemented | Incorporating a vulnerability management plan into the control system environment is vital in protecting control system 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 environment. Ensuring that vulnerabilities are managed minimizes the potential for system exploits, supporting the mission objective of maintaining system availability. |
| **Maintenance** | **PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools | *Rationale only provided for High Priority Subcategories* |
| | **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 environment for maintenance could result in serious disruption to control system functionality. Any malicious tampering with the control system 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. |

| 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 | The security architecture of a control system must incorporate mechanisms to monitor, log, and audit activities occurring within the control system environment and on control system 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. |
| | **PR.PT-2:** Removable media is protected and its use restricted according to policy | *Rationale only provided for High Priority Subcategories* |
| | **PR.PT-3**: Access to systems and assets is controlled, incorporating the principle of least functionality | 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 environment. As aforementioned, unauthorized access to a control system 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 environment by limiting the capabilities of the system itself. |

| Detailed Specifications | | |
|---|---|---|
| Category | Subcategory | Rationale for High Priority |
| | **PR.PT-4:** Communications and control networks are protected | Network security is critical in any control system environment. At minimum, the control system control 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 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 of control system 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-5, DE.CM-7, DE.CM-8** | 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 | *Rationale only provided for High Priority Subcategories* |
| | **DE.AE-3:** Event data are aggregated and correlated from multiple sources and sensors | *Rationale only provided for High Priority Subcategories* |
| | **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' 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 and other informational assets. |
| | **DE.CM-4:** Malicious code is detected | Detecting malicious code rapidly before the code can negatively affect a control system is critical for maintaining system availability. Implementing antivirus tools into a control system 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 | *Rationale only provided for High Priority Subcategories* |
| | **DE.CM-6:** External service provider activity is monitored to detect potential cybersecurity events | *Rationale only provided for High Priority Subcategories* |
| | **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 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 environment (e.g., legacy control systems) 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 | *Rationale only provided for High Priority Subcategories* |
| | **DE.DP-3:** Detection processes are tested | *Rationale only provided for High Priority Subcategories* |
| | **DE.DP-4:** Event detection information is communicated to appropriate parties | *Rationale only provided for High Priority Subcategories* |
| | **DE.DP-5:** Detection processes are continuously improved | *Rationale only provided for High Priority Subcategories* |

| **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 | *Rationale only provided for High Priority Subcategories* |
| | **RS.CO-3:** Information is shared consistent with response plans | *Rationale only provided for High Priority Subcategories* |
| | **RS.CO-4:** Coordination with stakeholders occurs consistent with response plans | *Rationale only provided for High Priority Subcategories* |
| | **RS.CO-5:** Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness | *Rationale only provided for High Priority Subcategories* |
| **Analysis** | **RS.AN-1:** Notifications from detection systems are investigated | *Rationale only provided for High Priority Subcategories* |

| Detailed Specifications | | |
|---|---|---|
| Category | Subcategory | Rationale for High Priority |
| | **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 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 | *Rationale only provided for High Priority Subcategories* |
| | **RS.AN-4:** Incidents are categorized consistent with response plans | *Rationale only provided for High Priority Subcategories* |
| **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 to minimize any damage or impact to DoD information networks, control system 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. |

| 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 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. |
| | **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 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 | *Rationale only provided for High Priority Subcategories* |
| | **RS.IM-2:** Response strategies are updated | *Rationale only provided for High Priority Subcategories* |

| **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 | *Rationale only provided for High Priority Subcategories* |
| | **RC.IM-2**: Recovery strategies are updated | *Rationale only provided for High Priority Subcategories* |
| **Communications** | **RC.CO-2:** Reputation after an event is repaired | *Rationale only provided for High Priority Subcategories* |
| | **RC.CO-3:** Recovery activities are communicated to internal stakeholders and executive and management teams | *Rationale only provided for High Priority Subcategories* |

## 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 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 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-3, ID.AM-4, ID.AM-5** | ID.AM-1, ID.AM-2, 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 | *Rationale only provided for High Priority Subcategories* |
| | **ID.AM-2:** Software platforms and applications within the organization are inventoried | *Rationale only provided for High Priority Subcategories* |

| 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 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 DoDI 8510.01's external IT service requirements that external information systems are catalogued. DoD organizations that use external IT services provided by a commercial or other non-federal government entity must ensure the security protections of the IS delivering the service is appropriate to the integrity needs of the DoD organization's information and mission. Otherwise, the organization opens itself to vulnerabilities from external sources that could negatively impact system integrity. |
| | **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 integrity of the organization's control system environment. |

| Detailed Specifications | | |
|---|---|---|
| Category | Subcategory | Rationale for High Priority |
| | **ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established | *Rationale only provided for High Priority Subcategories* |
| **Business Environment** | **ID.BE-1:** The organization's role in the supply chain is identified and communicated | *Rationale only provided for High Priority Subcategories* |
| | **ID.BE-2:** The organization's place in critical infrastructure and its industry sector is identified and communicated | *Rationale only provided for High Priority Subcategories* |
| | **ID.BE-3:** Priorities for organizational mission, objectives, and activities are established and communicated | *Rationale only provided for High Priority Subcategories* |
| | **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 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 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 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. |

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

| Detailed Specifications | | |
|---|---|---|
| Category | Subcategory | Rationale for High Priority |
| | **ID.RA-2:** Threat and vulnerability information is received from information sharing forums and sources | *Rationale only provided for High Priority Subcategories* |
| | **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 and mitigating cybersecurity risks. Organizations must identify these threats to control system security throughout the lifecycle of the component control systems from architecture to procurement to installation to maintenance to decommissioning. Due to the rapidly evolving nature of control systems, it is important to identify and review new control system 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. |
| | **ID.RA-4:** Potential business impacts and likelihoods are identified | *Rationale only provided for High Priority Subcategories* |
| | **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 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 environment to multiple, unacceptable risks to system integrity. |

| 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 integrity. |
| **Risk Management Strategy** | **ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders | *Rationale only provided for High Priority Subcategories* |
| | **ID.RM-2:** Organizational risk tolerance is determined and clearly expressed | *Rationale only provided for High Priority Subcategories* |
| | **ID.RM-3:** The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis | *Rationale only provided for High Priority Subcategories* |

| **Protect** | For control systems, security protections must be implemented with a focus on maintaining system integrity due to the high potential impact on the control system 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 environment. |
|---|---|

| | **High Priority Subcategories** | **Moderate Priority Subcategories** |
|---|---|---|
| Access Control | **PR.AC-1, PR.AC-2, PR.AC-3, PR.AC-4, 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-6, PR.IP-9, PR.IP-12** | PR.IP-2, PR.IP-5, PR.IP-7,PR.IP-10, PR.IP-11 |
| 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 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 environment is unacceptable. Ensuring that only authorized users access systems for approved uses is critical in maintaining system integrity. |
| | **PR.AC-2:** Physical access to assets is managed and protected | Unauthorized physical access to the control system 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 |

| Detailed Specifications | | |
|---|---|---|
| Category | Subcategory | Rationale for High Priority |
| | | environments to prevent physical modification, manipulation, or destruction of existing system infrastructure. Any malicious tampering with the control system 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 may need to be remotely accessed, including vendors and system integrators performing system maintenance functions, and control system engineers accessing geographically remote system components. Remote access capabilities must be adequately controlled to prevent unauthorized individuals from gaining access to the control system environment. Unauthorized remote access offers an adversary many avenues to manipulate control system data or the control system environment as a whole. As such, remote access must be carefully managed to maintain system integrity. |
| | **PR.AC-4:** Access permissions are managed, incorporating the principles of least privilege and separation of duties | 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 environment to prevent any accidental or intentional tampering that could lead to the alteration of data or system configuration and damage system integrity. |

| 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 environment, it is beneficial to separate the control system 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. |
| **Awareness and Training** | **PR.AT-1:** All users are informed and trained | A key measure in maintaining a control system 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 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 environment must receive proper training to maintain a safe control system environment. |
| | **PR.AT-2:** Privileged users understand roles & responsibilities | *Rationale only provided for High Priority Subcategories* |

| Detailed Specifications | | |
|---|---|---|
| Category | Subcategory | Rationale for High Priority |
| | **PR.AT-3:** Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities | *Rationale only provided for High Priority Subcategories* |
| | **PR.AT-4:** Senior executives understand roles & responsibilities | *Rationale only provided for High Priority Subcategories* |
| | **PR.AT-5:** Physical and information security personnel understand roles & responsibilities | *Rationale only provided for High Priority Subcategories* |
| **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 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 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 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 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 environment. Therefore, it is essential for organizations to formally manage all assets in a control system environment throughout removal, transfers, and disposition. |
| | **PR.DS-5:** Protections against data leaks are implemented | *Rationale only provided for High Priority Subcategories* |
| | **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 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 |
| | **PR.DS-7:** The development and testing environment(s) are separate from the production environment | 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 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. |

| Detailed Specifications | | |
|---|---|---|
| Category | Subcategory | Rationale for High Priority |
| **Information Protection Process and Procedures** | **PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained | 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 environment. Without a baseline configuration for the control system environment, it would be very challenging for organizations to securely implement new systems or components into the control system environment. If two of the same devices were incorporated into the control system 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. |
| | **PR.IP-2:** A System Development Life Cycle to manage systems is implemented | *Rationale only provided for High Priority Subcategories* |
| | **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 har, to system integrity. Vulnerabilities typically arise when the configuration of a system or environment changes. As such, any alteration to a control system 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. |

| 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 integrity. Incidents within a control system 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 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 | *Rationale only provided for High Priority Subcategories* |
| | **PR.IP-6:** Data is destroyed according to policy | *Rationale only provided for High Priority Subcategories* |
| | **PR.IP-7:** Protection processes are continuously improved | *Rationale only provided for High Priority Subcategories* |
| | **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 | *Rationale only provided for High Priority Subcategories* |

| Detailed Specifications | | |
|---|---|---|
| Category | Subcategory | Rationale for High Priority |
| | **PR.IP-11:** Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) | *Rationale only provided for High Priority Subcategories* |
| | **PR.IP-12:** A vulnerability management plan is developed and implemented | Incorporating a vulnerability management plan into the control system environment is vital in protecting control system 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 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 environment and inhibit system availability. |
| **Maintenance** | **PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools | *Rationale only provided for High Priority Subcategories* |
| | **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 environment for maintenance could result in serious disruption to control system functionality. Any malicious tampering with the control system 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. |

| 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 | The security architecture of a control system must incorporate mechanisms to monitor, log, and audit activities occurring within the control system environment and on control system 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 environment that would indicate damage to system integrity. As such, audit and log records are integral to maintaining system integrity. |
| | **PR.PT-2:** Removable media is protected and its use restricted according to policy | 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 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. |
| | **PR.PT-3:** Access to systems and assets is controlled, incorporating the principle of least functionality | *Rationale only provided for High Priority Subcategories* |

| Detailed Specifications | | |
|---|---|---|
| Category | Subcategory | Rationale for High Priority |
| | **PR.PT-4:** Communications and control networks are protected | Network security is critical in any control system environment. At minimum, the control system control 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 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 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-5, DE.CM-6, DE.CM-7, DE.CM-8** | |
| 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 | *Rationale only provided for High Priority Subcategories* |
| | **DE.AE-2:** Detected Events are analyzed to understand attack targets and methods | *Rationale only provided for High Priority Subcategories* |
| | **DE.AE-3:** Event data are aggregated and correlated from multiple sources and sensors | *Rationale only provided for High Priority Subcategories* |
| | **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' 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 and other informational assets. |
| | **DE.CM-4:** Malicious code is detected | Detecting malicious code rapidly before the code can negatively affect a control system is critical for maintaining system integrity. Implementing antivirus tools into a control system 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 | *Rationale only provided for High Priority Subcategories* |
| | **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 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 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 | *Rationale only provided for High Priority Subcategories* |
| | **DE.DP-3:** Detection processes are tested | *Rationale only provided for High Priority Subcategories* |
| | **DE.DP-4:** Event detection information is communicated to appropriate parties | *Rationale only provided for High Priority Subcategories* |
| | **DE.DP-5:** Detection processes are continuously improved | *Rationale only provided for High Priority Subcategories* |

| **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 | *Rationale only provided for High Priority Subcategories* |
| | **RS.CO-3:** Information is shared consistent with response plans | *Rationale only provided for High Priority Subcategories* |
| | **RS.CO-4:** Coordination with stakeholders occurs consistent with response plans. | *Rationale only provided for High Priority Subcategories* |
| | **RS.CO-5:** Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness | *Rationale only provided for High Priority Subcategories* |
| **Analysis** | **RS.AN-1:** Notifications from detection systems are investigated. | *Rationale only provided for High Priority Subcategories* |

| Detailed Specifications | | |
|---|---|---|
| Category | Subcategory | Rationale for High Priority |
| | **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 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 | *Rationale only provided for High Priority Subcategories* |
| | **RS.AN-4:** Incidents are categorized consistent with response plans | *Rationale only provided for High Priority Subcategories* |
| **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 to minimize any damage or impact to DoD information networks, control system 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 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 | *Rationale only provided for High Priority Subcategories* |
| | **RS.IM-2:** Response strategies are updated | *Rationale only provided for High Priority Subcategories* |

| **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 environments are operating with sustained integrity at both the system and data level. |
| **Improvements** | **RC.IM-1:** Recovery plans incorporate lessons learned | *Rationale only provided for High Priority Subcategories* |
| | **RC.IM-2:** Recovery strategies are updated | *Rationale only provided for High Priority Subcategories* |
| **Communications** | **RC.CO-3:** Recovery activities are communicated to internal stakeholders and executive and management teams | *Rationale only provided for High Priority Subcategories* |

## Mission Objective 3: Maintain Human Safety

**Description**: Recognizing cybersecurity effects on control systems 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, 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 | *Rationale only provided for High Priority Subcategories* |
| | **ID.AM-3:** Organizational communication and data flows are mapped | *Rationale only provided for High Priority Subcategories* |

| 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 human safety of the organization's control system 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 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, 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 environment. |
| **Governance** | **ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberty obligations, are understood and managed | *Rationale only provided for High Priority Subcategories* |
| **Risk Assessment** | **ID.RA-1:** Asset vulnerabilities are identified and documented | *Rationale only provided for High Priority Subcategories* |
| | **ID.RA-2:** Threat and vulnerability information is received from information sharing forums and sources | *Rationale only provided for High Priority Subcategories* |

| 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 and mitigating cybersecurity risks. Organizations must identify these threats to control system security throughout the lifecycle of the component control systems form architecture to procurement to installation to maintenance to decommissioning. Due to the rapidly evolving nature of control systems, it is important to identify and review new control system 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. |
| | **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 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 to multiple, unacceptable risks to human safety. |

| 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 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. |
| **Risk Management Strategy** | **ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders | *Rationale only provided for High Priority Subcategories* |
| | **ID.RM-2:** Organizational risk tolerance is determined and clearly expressed | *Rationale only provided for High Priority Subcategories* |

| **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 environment. These measures minimize the potential for catastrophic human safety failures in the control system 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 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 environments to prevent physical modification, manipulation, or destruction of existing system infrastructure. Because control systems 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 causing system failure resulting in a fire within the control system 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 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 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 environment must receive proper training to maintain a safe control system environment. |
| | **PR.AT-2:** Privileged users understand roles & responsibilities | *Rationale only provided for High Priority Subcategories* |
| | **PR.AT-3:** Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities | *Rationale only provided for High Priority Subcategories* |
| | **PR.AT-4:** Senior executives understand roles & responsibilities | *Rationale only provided for High Priority Subcategories* |
| | **PR.AT-5:** Physical and information security personnel understand roles & responsibilities | *Rationale only provided for High Priority Subcategories* |
| **Data Security** | **PR.DS-7:** The development and testing environment(s) are separate from the production environment | *Rationale only provided for High Priority Subcategories* |

| 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 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 environments can help protect against catastrophic system failure, which could directly result in human harm. |
| | **PR.IP-7:** Protection processes are continuously improved | *Rationale only provided for High Priority Subcategories* |
| | **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 | *Rationale only provided for High Priority Subcategories* |
| | **PR.IP-11:** Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) | *Rationale only provided for High Priority Subcategories* |
| | **PR.IP-12:** A vulnerability management plan is developed and implemented | *Rationale only provided for High Priority Subcategories* |

| 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 | *Rationale only provided for High Priority Subcategories* |
| | **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 environment for maintenance could result in serious disruption to control system functionality. Because control systems have the ability to interact with the physical world, malicious tampering could jeopardize human safety. As such, remote interaction with the control system environment must be approved and logged. |
| **Protective Technology** | **PR.PT-3:** Access to systems and assets is controlled, incorporating the principle of least functionality | *Rationale only provided for High Priority Subcategories* |
| | **PR.PT-4:** Communications and control networks are protected | *Rationale only provided for High Priority Subcategories* |

| **Detect** | Implementing detection measures for continuous monitoring of control system 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 | *Rationale only provided for High Priority Subcategories* |
| | **DE.AE-3:** Event data are aggregated and correlated from multiple sources and sensors | *Rationale only provided for High Priority Subcategories* |
| | **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 | *Rationale only provided for High Priority Subcategories* |
| **Security Continuous Monitoring** | **DE.CM-2:** The physical environment is monitored to detect potential cybersecurity events | *Rationale only provided for High Priority Subcategories* |
| | **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 and other informational assets. |

| 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 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 | *Rationale only provided for High Priority Subcategories* |
| | **DE.DP-4:** Event detection information is communicated to appropriate parties | *Rationale only provided for High Priority Subcategories* |
| | **DE.DP-5:** Detection processes are continuously improved | *Rationale only provided for High Priority Subcategories* |

| **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 | It is essential when responding to an event with catastrophic consequences on the life and health of control system stakeholders that personnel know their roles and order of operations. Particularly with incidents that can cause human harm, personnel must know the proper procedures for securing their own safety and notifying the necessary parties of the incident. |
| | **RS.CO-3:** Information is shared consistent with response plans | *Rationale only provided for High Priority Subcategories* |
| **Analysis** | **RS.AN-1:** Notifications from detection systems are investigated. | *Rationale only provided for High Priority Subcategories* |

| Detailed Specifications | | |
|---|---|---|
| Category | Subcategory | Rationale for High Priority |
| | **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 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 | *Rationale only provided for High Priority Subcategories* |
| **Communications** | **RS.CO-1:** Personnel know their roles and order of operations when a response is needed | In the case of an incident that could cause human harm, personnel need to be aware of the proper response measures. Personnel need to know their roles to mitigate the response and to ensure their own safety. If individuals are not aware of proper response measures during an incident, they could be faced with unnecessary harm that would be avoidable with proper planning. |
| **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 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 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 and data that poses a threat to human safety must 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 | *Rationale only provided for High Priority Subcategories* |
| | **RS.IM-2:** Response strategies are updated | *Rationale only provided for High Priority Subcategories* |

| **Recover** | Effective recovery measures are critical to ensuring human safety in a control system 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-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 | *Rationale only provided for High Priority Subcategories* |
| | **RC.IM-2:** Recovery strategies are updated | *Rationale only provided for High Priority Subcategories* |
| **Communications** | **RC.CO-2:** Reputation after an event is repaired | *Rationale only provided for High Priority Subcategories* |
| | **RC.CO-3:** Recovery activities are communicated to internal stakeholders and executive and management teams | *Rationale only provided for High Priority Subcategories* |

## Mission Objective 4: Maintain Environmental Safety

**Description:** Recognizing cybersecurity effects on control systems 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 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 | *Rationale only provided for High Priority Subcategories* |

| 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 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 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, which in turn reduces risk of environmental incidents. In addition, by communicating organizational priorities as they relate to control systems, managers can demonstrate their commitment to, and value of, a cybersecurity program that can solicit valuable input from personnel contributing to the overall environmental safety of the control system environment. |
| **Risk Assessment** | **ID.RA-1:** Asset vulnerabilities are identified and documented | *Rationale only provided for High Priority Subcategories* |
| | **ID.RA-2:** Threat and vulnerability information is received from information sharing forums and sources | *Rationale only provided for High Priority Subcategories* |

| 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 and mitigating cybersecurity risks. Organizations must identify these threats to control system security throughout the lifecycle of the component control systems form architecture to procurement to installation to maintenance to decommissioning. Due to the rapidly evolving nature of control systems, it is important to identify and review new control system 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 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 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 | *Rationale only provided for High Priority Subcategories* |

| **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 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 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 environments to prevent physical modification, manipulation, or destruction of existing system infrastructure. Because control systems 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 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 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 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 environment must receive proper training to maintain a safe control system environment. |
| | **PR.AT-2**: Privileged users understand roles & responsibilities | *Rationale only provided for High Priority Subcategories* |
| | **PR.AT-3**: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities | *Rationale only provided for High Priority Subcategories* |
| | **PR.AT-4**: Senior executives understand roles & responsibilities | *Rationale only provided for High Priority Subcategories* |
| | **PR.AT-5**: Physical and information security personnel understand roles & responsibilities | *Rationale only provided for High Priority Subcategories* |
| Data Security | **PR.DS-7:** The development and testing environment(s) are separate from the production environment | *Rationale only provided for High Priority Subcategories* |

| 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 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 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 | *Rationale only provided for High Priority Subcategories* |
| | **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 | *Rationale only provided for High Priority Subcategories* |
| | **PR.IP-11:** Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) | *Rationale only provided for High Priority Subcategories* |
| | **PR.IP-12:** A vulnerability management plan is developed and implemented | *Rationale only provided for High Priority Subcategories* |

| 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 | *Rationale only provided for High Priority Subcategories* |
| | **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 environment for maintenance could result in serious disruption to control system functionality. Because control systems 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 environment must be approved and logged. |
| Protective Technology | **PR.PT-3**: Access to systems and assets is controlled, incorporating the principle of least functionality | *Rationale only provided for High Priority Subcategories* |
| | **PR.PT-4:** Communications and control networks are protected | *Rationale only provided for High Priority Subcategories* |

| **Detect** | Implementing detection measures for anomalies and events of control system 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 | *Rationale only provided for High Priority Subcategories* |
| | **DE.AE-3:** Event data are aggregated and correlated from multiple sources and sensors | *Rationale only provided for High Priority Subcategories* |
| | **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 | *Rationale only provided for High Priority Subcategories* |
| **Security Continuous Monitoring** | **DE.CM-2:** The physical environment is monitored to detect potential cybersecurity events | *Rationale only provided for High Priority Subcategories* |
| | **DE.CM-3:** Personnel activity is monitored to detect potential cybersecurity events | *Rationale only provided for High Priority Subcategories* |
| | **DE.CM-7:** Monitoring for unauthorized personnel, connections, devices, and software is performed | *Rationale only provided for High Priority Subcategories* |
| **Detection Processes** | **DE.DP-1:** Roles and responsibilities for detection are | *Rationale only provided for High Priority Subcategories* |

| Detailed Specifications | | |
|---|---|---|
| Category | Subcategory | Rationale for High Priority |
| | well defined to ensure accountability | |
| | **DE.DP-4:** Event detection information is communicated to appropriate parties | *Rationale only provided for High Priority Subcategories* |
| | **DE.DP-5:** Detection processes are continuously improved | *Rationale only provided for High Priority Subcategories* |

| **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 environment vulnerability or flaw that could relate to potential environmental harm. | |
|---|---|---|
| | **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 | *Rationale only provided for High Priority Subcategories* |
| **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 environments as an organization must understand the immediate and long-term effects an incident can have on environmental safety. |

| Detailed Specifications | | |
|---|---|---|
| Category | Subcategory | Rationale for High Priority |
| | **RS.AN-4:** Incidents are categorized consistent with response plans | *Rationale only provided for High Priority Subcategories* |
| **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 failure that leads to a chemical spill), it is particularly important to ensure that the incident is rapidly contained. |
| | **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 environment, an incident must be mitigated as quickly as possible to minimize the negative impacts, particularly when the incident causes harm to the environment. |

| 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 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 | *Rationale only provided for High Priority Subcategories* |
| | **RS.IM-2:** Response strategies are updated | *Rationale only provided for High Priority Subcategories* |

| **Recover** | Effective recovery measures are critical to ensuring environmental safety in a control system 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 | *Rationale only provided for High Priority Subcategories* |
| | **RC.IM-2:** Recovery strategies are updated | *Rationale only provided for High Priority Subcategories* |
| **Communications** | **RC.CO-3**: Recovery activities are communicated to internal stakeholders and executive and management teams | *Rationale only provided for High Priority Subcategories* |

## Mission Objective 5: Maintain Physical Security

**Description:** Recognizing and securing physical controls that impact control systems. Preventing unauthorized access to a control system environment and preventing unauthorized damage or tampering with physical assets directly related to the control system 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 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 environment.
- Apply Continuous Monitoring to physical assets associated with the control system 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 environments they protect.
- Ensure that physical security personnel are aware of which areas of a control system 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 and control system 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 |

| 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 environment. In order to properly protect critical IT and control system 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. |
| | **ID.AM-4:** External information systems are catalogued | It is essential for organizations to comply with DoDI 8510.01's external IT service requirements that external information systems are catalogued. DoD organizations that use external IT services provided by a commercial or other non-federal government entity must ensure the security protections of the information system delivering the service is appropriate to the availability needs of the DoD organization's information and mission. Moreover, the physical tampering with or damaging of external assets can also have detrimental effects on the control system environment. Therefore, it is crucial to ensure that all external information systems are catalogued for maintaining physical safety. |

| 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 physical risks and vulnerabilities to the control system environment. |
| | **ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established | *Rationale only provided for High Priority Subcategories* |
| **Business Environment** | **ID.BE-2:** The organization's place in critical infrastructure and its industry sector is identified and communicated | *Rationale only provided for High Priority Subcategories* |
| | **ID.BE-3:** Priorities for organizational mission, objectives, and activities are established and communicated | *Rationale only provided for High Priority Subcategories* |
| | **ID.BE-4:** Dependencies and critical functions for delivery of critical services are established | *Rationale only provided for High Priority Subcategories* |

| 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 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 environment and a risk to critical mission/business objectives. |
| **Governance** | **ID.GV-1:** Organizational information security policy is established | *Rationale only provided for High Priority Subcategories* |
| | **ID.GV-2:** Information security roles & responsibilities are coordinated and aligned with internal roles and external partners | *Rationale only provided for High Priority Subcategories* |
| | **ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberty obligations, are understood and managed | *Rationale only provided for High Priority Subcategories* |

| Detailed Specifications | | |
|---|---|---|
| Category | Subcategory | Rationale for High Priority |
| | **ID.GV-4:** Governance and risk management processes address cybersecurity risks | It is DoD policy that: the DoD will establish and use an integrated enterprise-wide decision structure for cybersecurity risk management (the RMF) that includes and integrates DoD mission areas (MAs) pursuant to DoDD 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 or an ad-hoc, disparate policy that is not aligned with overall physical safety requirements of the control system environment. |
| **Risk Assessment** | **ID.RA-1:** Asset vulnerabilities are identified and documented | *Rationale only provided for High Priority Subcategories* |
| | **ID.RA-2:** Threat and vulnerability information is received from information sharing forums and sources | *Rationale only provided for High Priority Subcategories* |

| 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 and mitigating cybersecurity risks. Organizations must identify these threats to control system security throughout the lifecycle of the component control systems. Due to the rapidly evolving nature of control systems, it is important to identify and review new control system capabilities and their associated emerging threats. This includes analyzing flaws and vulnerabilities to physical controls as they are critical in securing the control system environment. |
| | **ID.RA-4:** Potential business impacts and likelihoods are identified | *Rationale only provided for High Priority Subcategories* |

| Detailed Specifications | | |
|---|---|---|
| Category | Subcategory | Rationale for High Priority |
| | **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 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 environment to unacceptable risks. Therefore, analyzing and determining physical safety is critical in ensuring the secure implementation of a control system environment. |
| | **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. If risk responses are not identified and prioritized regarding physical controls and safeguards for control system assets, organizations will accept inappropriate risks to business continuity. |

| 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 | *Rationale only provided for High Priority Subcategories* |
| | **ID.RM-2:** Organizational risk tolerance is determined and clearly expressed | *Rationale only provided for High Priority Subcategories* |
| | **ID.RM-3:** | *Rationale only provided for High Priority Subcategories* |

| **Protect** | For control systems, security protections must be implemented with a focus on maintaining system integrity due to the high potential impact on the control system 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 an log management tools) to maintain the security and integrity of the control system environment. |
|---|---|

| | High Priority Subcategories | Moderate Priority Subcategories |
|---|---|---|
| Access Control | **PR.AC-1, PR.AC-2, PR.AC-3, PR.AC-4** | 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 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 environment is unacceptable. Ensuring that only authorized users access systems for approved uses is critical in maintaining physical security. |

| 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 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 environments to prevent physical modification, manipulation, or destruction of existing system infrastructure. Any malicious tampering with the control system 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 | *Rationale only provided for High Priority Subcategories* |
| | **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 environment to prevent any accidental or intentional physical tampering of a control system environment could lead to system failure and hinder business continuity. |

| Detailed Specifications | | |
|---|---|---|
| Category | Subcategory | Rationale for High Priority |
| | **PR.AC-5**: Network integrity is protected, incorporating network segregation where appropriate | *Rationale only provided for High Priority Subcategories* |
| **Awareness and Training** | **PR.AT-1**: All users are informed and trained | A key measure in maintaining the physical safety of a control system 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 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 environment. |
| | **PR.AT-2:** Privileged users understand roles & responsibilities | *Rationale only provided for High Priority Subcategories* |
| | **PR.AT-3**: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities | *Rationale only provided for High Priority Subcategories* |
| | **PR.AT-4:** Senior executives understand roles & responsibilities | *Rationale only provided for High Priority Subcategories* |

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

| 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 can harm a control system environment. Vulnerabilities typically arise when the configuration of a system or environment changes. Particularly regarding physical controls, any alteration to a control system environment, must be documented and tested. 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 environment. |
| | **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 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 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. |

| Detailed Specifications | | |
|---|---|---|
| Category | Subcategory | Rationale for High Priority |
| | **PR.IP-7:** Protection processes are continuously improved | *Rationale only provided for High Priority Subcategories* |
| | **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 | *Rationale only provided for High Priority Subcategories* |
| | **PR.IP-11:** Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) | *Rationale only provided for High Priority Subcategories* |

| Detailed Specifications | | |
|---|---|---|
| Category | Subcategory | Rationale for High Priority |
| | **PR.IP-12:** A vulnerability management plan is developed and implemented | Incorporating a vulnerability management plan into the control system environment is vital in protecting control system 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 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. |
| **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. |

| Detailed Specifications | | |
|---|---|---|
| Category | Subcategory | Rationale for High Priority |
| | **PR.MA-2:** Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access | *Rationale only provided for High Priority Subcategories* |
| **Protective Technology** | **PR.PT-2:** Removable media is protected and its use restricted according to policy | *Rationale only provided for High Priority Subcategories* |
| | **PR.PT-3**: Access to systems and assets is controlled, incorporating the principle of least functionality | 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 environment. As aforementioned, unauthorized access to a control system 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 environment if they were able to gain unauthorized physical access. |
| | **PR.PT-4:** Communications and control networks are protected | *Rationale only provided for High Priority Subcategories* |

| **Detect** | Implementing detection measures for anomalous events related to control system 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 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-6, DE.CM-7 |
| 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 | *Rationale only provided for High Priority Subcategories* |
| | **DE.AE-3:** Event data are aggregated and correlated from multiple sources and sensors | *Rationale only provided for High Priority Subcategories* |
| | **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 | *Rationale only provided for High Priority Subcategories* |

| 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 environment. Due to the nature of control systems' 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 environment. It is essential for maintaining physical safety that proper monitoring mechanisms exist throughout a control system facility to ensure that personnel are only carrying out authorized and appropriate tasks within the control system environment. |
| | **DE.CM-6:** External service provider activity is monitored to detect potential cybersecurity events | *Rationale only provided for High Priority Subcategories* |
| | **DE.CM-7:** Monitoring for unauthorized personnel, connections, devices, and software is performed | *Rationale only provided for High Priority Subcategories* |
| **Detection Processes** | **DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability | *Rationale only provided for High Priority Subcategories* |
| | **DE.DP-3:** Detection processes are tested | *Rationale only provided for High Priority Subcategories* |

| Detailed Specifications | | |
|---|---|---|
| Category | Subcategory | Rationale for High Priority |
| | **DE.DP-4:** Event detection information is communicated to appropriate parties | *Rationale only provided for High Priority Subcategories* |
| | **DE.DP-5:** Detection processes are continuously improved | *Rationale only provided for High Priority Subcategories* |

| **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 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 | *Rationale only provided for High Priority Subcategories* |
| | **RS.CO-3:** Information is shared consistent with response plans | *Rationale only provided for High Priority Subcategories* |

| Detailed Specifications | | |
|---|---|---|
| Category | Subcategory | Rationale for High Priority |
| **Analysis** | **RS.AN-1:** Notifications from detection systems are investigated. | *Rationale only provided for High Priority Subcategories* |
| | **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 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 | *Rationale only provided for High Priority Subcategories* |
| | **RS.AN-4:** Incidents are categorized consistent with response plans | *Rationale only provided for High Priority Subcategories* |

| 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 to minimize any damage or impact to DoD IT assets, control system 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. |
| | **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 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 environment. |

| 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 or control-system-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 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 environment. |
| **Improvements** | **RS.IM-1:** Response plans incorporate lessons learned | *Rationale only provided for High Priority Subcategories* |
| | **RS.IM-2:** Response strategies are updated | *Rationale only provided for High Priority Subcategories* |

| **Recover** | Effective recovery measures are critical to ensuring physical safety in a control system 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 they physical safety of assets within a control system environment. |
| **Improvements** | **RC.IM-1:** Recovery plans incorporate lessons learned | *Rationale only provided for High Priority Subcategories* |
| | **RC.IM-2:** Recovery strategies are updated | *Rationale only provided for High Priority Subcategories* |
| **Communications** | **RC.CO-3**: Recovery activities are communicated to internal stakeholders and executive and management teams | *Rationale only provided for High Priority Subcategories* |

## 3 System Security Requirements for Control Systems

The following sections take a system-oriented approach to control system security. Rather than addressing security from an organizational perspective as in the CSF, this section describes tailored implementation guidance for control systems 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, "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 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 DoD control systems. 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 environment. Finally, Section 3.4 contains tables of each control family mapping the DoD control systems derived security requirements to the appropriate controls established in NIST SP 800-53, providing guidance for secure implementation of control systems 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 perspective to include the applicability of each control family as it relates to control systems and implementing control systems 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 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 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, auditing a control system 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 vary greatly, it is important for control system operators to use the system's vendor auditing tools and techniques when traditional auditing practices are not available. Additionally, auditing a control system should include the use of configuration management tools, auditing engineering workstations, and situational awareness surrounding the control system 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 perspective, ensuring that all personnel are able to adequately secure control systems and recognize potential threat indicators are essential aspects of effective security implementation. Cross training control system and IT engineers is essential in ensuring the proper application of cybersecurity to control systems. Moreover, due to the large variety and complexity of control systems, vendor/system specific training is often necessary to properly train personnel to operate in specific control system 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 common place 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, 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 network or device. Lastly, configuring the control system 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, 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, 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 demands strong authentication measures such as DoD-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 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 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 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 emphasize the prohibition of any unauthorized removable media from interacting with a control system 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, 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 implementation. Portable devices directly associated with control system 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 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 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 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.

**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, 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 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 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 perspective, it is advisable to employ cryptographic systems and a VPN where they are deemed appropriate after extensive performance testing. Configuring control systems so they do not depend entirely on the network is also imperative to secure 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 and that the environment can satisfy required performance levels. Employing a patch to a control system 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 are frequently tested and deployed.

### 3.3 DoD Policy Regarding Security Controls

DoDI 8500.01 requires DoD organizations to categorize all DOD ISs 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.

DoDI 8510.01 establishes DoD policy for RMF, guides the creation of associated cybersecurity policy, and assigns responsibilities for executing and maintaining the RMF. This DoD 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 DoD 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 DoD control systems. 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. The requirements were then mapped to the security controls listed in each control family of NIST SP 800-53 to be implemented in a DoD control system environment throughout the control system lifecycle.

**Table 2-1: Mapping Access Control Requirements to Controls**

| CONTROL FAMILY | NIST 800-53 Relevant Security Controls | |
|---|---|---|
| **AC - Access Control** | # | CONTROL DESCRIPTION |
| **TABLE 2-1: MAPPING REQUIREMENTS TO CONTROLS** | | |
| **SECURITY REQUIREMENTS** | **NIST 800-53 Relevant Security Controls** | |
| **Family** | | |
| ***Basic Security Requirements*** | | |
| **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 |
| ***Derived Security Requirements*** | | |
| **1.2** Utilize role-based access controls to enhance security from remote access points. | AC-2(7) | ACCESS MANAGEMENT \| *Role-Based Schemes* |
| | AC-3(2) | ACCESS ENFORCEMENT \| *Role-Based Access Control* |
| **1.3** Employ the principle of least privilege, including for specific security functions and privileged accounts.<br><br>**1.4** Deploy virtual local area networks (VLANs) where feasible, to increase system performance, improve manageability, and simplify network design. | AC-6 | LEAST PRIVILEGE |
| **1.5** Ensure remote access software employs carefully reviewed and configured security options. Control systems often use remote control software that provide the remote user powerful (administrative or root) access to the target system. | AC-17 | REMOTE ACCESS |
| **1.6** Ensure wireless local area networks (LANs) are deployed only where operational risk implications are low | AC-18 | WIRELESS ACCESS |

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

| CONTROL FAMILY | NIST 800-53 Relevant Security Controls | |
|---|---|---|
| **AT - Awareness and Training** | # | CONTROL DESCRIPTION |
| **TABLE 2-2: MAPPING REQUIREMENTS TO CONTROLS** | | |
| **SECURITY REQUIREMENTS** | **NIST 800-53 Relevant Security Controls** | |
| **Awareness and Training** | | |
| ***Basic Security Requirements*** | | |
| **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.<br>**1.2** Ensure that organizational personnel are adequately trained to carry out their assigned security-related duties and responsibilities. | AT-2 | SECURITY AWARENESS AND TRAINING |
| | AT-3 | ROLE BASED SECURITY TRAINING |
| ***Derived Security Requirements*** | | |
| **1.3** Provide security awareness training on recognizing and reporting potential indicators of insider threat | AT-2(2) | SECURITY AWARENSS AND TRAINING \| *Insider Threat* |
| **1.4.** Ensure personnel have taken control systems-specific information security awareness training and know the responsibilities involved for control system applications. Awareness training must cover the physical process being controlled as well as the system itself.<br>**1.5** Ensure training programs demonstrate why control system environments require new access and control methods, covers ways personnel can reduce risk, and addresses the impact of not incorporating control methods. | AT-3(3) | ROLE BASED SECURITY TRAINING \| *Practical Exercises* |

**Table 2-3: Mapping Audit and Accountability Requirements to Controls**

| CONTROL FAMILY | NIST 800-53 Relevant Security Controls | |
|---|---|---|
| **AU - Audit and Accountability** | # | CONTROL DESCRIPTION |
| **TABLE 2-3: MAPPING REQUIREMENTS TO CONTROLS** | | |
| **SECURITY REQUIREMENTS** | **NIST 800-53 Relevant Security Controls** | |
| **Audit and Accountability** | | |
| ***Basic Security Requirements*** | | |
| **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;<br>**1.2** Ensure control systems contain a method for tracing actions to individual system users so organizations can hold those users accountable for their actions. | AU-2 | AUDIT EVENTS |
| | AU-3 | CONTENT OF AUDIT RECORDS |
| | AU-6 | AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING |
| | AU-11 | AUDIT RECORD RETENTION |
| | AU-12 | AUDIT RECORD GENERATION |
| ***Derived Security Requirements*** | | |
| It is necessary to determine that the system is performing as intended. Organizations must perform periodic audits of the control system to validate the following items:<br>**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).<br>**1.4** The production system is free from security compromises and provides information on the nature | AU-2(3) | EVENT LOGGING \| *Reviews and Updates* |
| | AU-6 | AUDIT REVIEW, ANALYSIS, AND REPORTING |

| | | |
|---|---|---|
| and extent of compromises as feasible, should they occur.<br>**1.5** The change program is being managed rigorously and creates an auditable trail of reviews and approvals for all changes.<br>Organizations should also monitor sensors, logs, Intrusion Detection Systems (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.<br>Organizations should incorporate system auditing utilities into new and existing control system 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 application and platform. Legacy systems typically employ printer loggers, which are reviewed by administrative, operational, and security staff. Logs maintained by the control system application may be stored at various locations and may or may not be encrypted. | AU-7 | AUDIT REDUCTION AND REPORT GENERATION |
| | AU-9 | PROTECTION OF AUDIT INFORMATION |
| | AU-10(1) | NON-REPUDIATION \| Association of Identities |
| | AU-12 | AUDIT GENERATION |

**Table 2-4: Mapping Certification, Accreditation, and Security Assessment Requirements to Controls**

| CONTROL FAMILY | NIST 800-53 Relevant Security Controls | |
|---|---|---|
| **CA - Certification, Accreditation, and Security Assessments** | | |
| **TABLE 2-4: MAPPING REQUIREMENTS TO CONTROLS** | | |
| **SECURITY REQUIREMENTS** | **NIST 800-53 Relevant Security Controls** | |
| **CA - Certification, Accreditation, and Security Assessments** | | |
| ***Basic Security Requirements*** | | |
| **1.1** Periodically assess the security controls in organizational systems to determine if the controls are effective in their application;<br>**1.2** Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems;<br>**1.3** Authorize the operation of organizational systems and any associated system connections;<br>**1.4** Monitor system security controls on an ongoing basis to ensure the continued effectiveness of the controls. | CA-2 | SECURITY ASSESSMENTS |
| | CA-5 | PLAN OF ACTION AND MILESTONES |
| | CA-6 | SECURITY AUTHORIZATION |
| | CA-7 | CONTINUOUS MONITORING |
| ***Derived Security Requirements*** | | |
| **1.5** A senior organizational official must accept residual risk and grant the system authorization to operate. | CA-2(1) | SECURITY ASSESSMENTS \| *Independent Assessors* |
| **1.6** Limit control system 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. | CA-3 | SYSTEM INTERCONNECTIONS |
| | CA-9 | INTERNAL SYSTEM CONNECTIONS |

**Table 2-5: Mapping Configuration Management Requirements to Controls**

| CONTROL FAMILY | NIST 800-53 Relevant Security Controls | |
|---|---|---|
| **CM - Configuration Management** | | |
| **TABLE 2-5: MAPPING REQUIREMENTS TO CONTROLS** | | |
| **SECURITY REQUIREMENTS** | **NIST 800-53 Relevant Security Controls** | |
| **CM - Configuration Management** | | |
| ***Basic Security Requirements*** | | |
| **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;<br>**1.2** Establish and enforce security configuration settings for information technology products employed in organizational information systems. | CM-2 | BASELINE CONFIGURATION |
| | CM-6 | CONFIGURATION SETTINGS |
| | CM-8 | SYSTEM COMPONENT INVENTORY |
| | CM-8(1) | SYSTEM COMPONENT INVENTORY \| Updates During Installations / Removals |
| | CM-9 | CONFIGURATION MANAGEMENT PLAN |
| ***Derived Security Requirements*** | | |
| **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.<br>**1.4** Ensure remote access software employs carefully reviewed and configured security options. Control systems often use remote control software that provide the remote user powerful (administrative or root) access to the target system. | CM-3 | CONFIGURATION CHANGE CONTROL |

| | | |
|---|---|---|
| **1.5** Perform risk assessment when dealing with any configuration change to a control system network or device. | CM-4 | SECURITY IMPACT ANALYSIS |
| **1.6** Restrict configuration and security setting access to the most stringent mode consistent with control system operational requirements. | CM-5 | ACCESS RESTRICTIONS FOR CHANGE |
| **1.7** Configure the control system 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) | INFORMATION SYSTEM COMPONENT INVENTORY \| *Assessed Configurations / Approved Deviations* |

**Table 2-6: Mapping Contingency Planning Requirements to Controls**

| CONTROL FAMILY | NIST 800-53 Relevant Security Controls | |
|---|---|---|
| **CP - Contingency Planning** | | |
| **TABLE 2-6: MAPPING REQUIREMENTS TO CONTROLS** | | |
| **SECURITY REQUIREMENTS** | **NIST 800-53 Relevant Security Controls** | |
| **CP - Contingency Planning** | | |
| ***Basic Security Requirements*** | | |
| **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. | CP-2 | CONTINGENCY PLAN |
| | CP-9 | INFORMATION SYSTEM BACKUP |
| ***Derived Security Requirements*** | | |
| **1.2** Establish trainings to ensure employees are familiar with the contents of the contingency plans. | CP-3 | CONTINGENCY TRAINING |
| | CP-4 | CONTINGENCY PLAN TESTING |
| **1.3** Coordinate contingency planning with management responsible for business continuity planning to meet the needs of the recovery objectives. | CP-6 | ALTERNATE SITE STORAGE |
| | CP-7 | ALTERNATE PROCESSING SITE |
| **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 control systems 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. | CP-10 | INFORMATION SYSTEM RECOVERY AND RECONSTITUTION |

**Table 2-7: Mapping Identification and Authentication Requirements to Controls**

| CONTROL FAMILY | NIST 800-53 Relevant Security Controls | |
|---|---|---|
| **IA - Identification and Authentication** | | |
| **TABLE 2-7: MAPPING REQUIREMENTS TO CONTROLS** | | |
| **SECURITY REQUIREMENTS** | **NIST 800-53 Relevant Security Controls** | |
| **IA - Identification and Authentication** | | |
| ***Basic Security Requirements*** | | |
| **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. | IA-2 | IDENTIFICATION AND AUTHENTICATION (Organizational Users) |
| | IA-3 | DEVICE IDENTIFICATION AND AUTHENTICATION |
| | IA-5 | AUTHENTICATOR MANAGEMENT |
| ***Derived Security Requirements*** | | |
| **1.2** In situations where authentication mechanisms may improperly effect control system functionality, compensating controls (such as rigorous physical security controls) must provide an equivalent security capability. | IA-2(1) | IDENTIFICATION AND AUTHENTICATION \| *Network Access to Privileged Accounts* |
| **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 environment. | IA-4 | IDENTIFIER MANAGEMENT |
| **1.4** Specify password complexity at DoD-defined values where practical (see DoD password policy). | IA-5(1) | AUTHENTICATOR MANAGEMENT \| *Password-Based Authentication* |
| **1.5** Configure control systems per 1.4 so that systems do not use default passwords for authentication. | | |
| **1.6** If organizations deem authentication mechanisms advisable, they should implement multi-factor authentication. | IA-11 | RE-AUTHENTICATION |

**Table 2-8: Mapping Incident Response Requirements to Controls**

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

| | | |
|---|---|---|
| | IR-9(1) | INFORMATION SPILLAGE RESPONSE \| *Responsible Personnel* |

**Table 2-9: Mapping Maintenance Requirements to Controls**

| CONTROL FAMILY | NIST 800-53 Relevant Security Controls | |
|---|---|---|
| MA - Maintenance | | |
| **TABLE 2-9: MAPPING REQUIREMENTS TO CONTROLS** | | |
| **SECURITY REQUIREMENTS** | **NIST 800-53 Relevant Security Controls** | |
| **MA - Maintenance** | | |
| ***Basic Security Requirements*** | | |
| **1.1** Perform periodic and timely maintenance on organizational information systems;<br>**1.2** Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance. | MA-2 | CONTROLLED MAINTENANCE |
| | MA-3 | MAINTENANCE TOOLS |
| | MA-3(1) | MAINTENANCE TOOLS \| *Inspect Tools* |
| | MA-3(2) | MAINTENANCE TOOLS \| *Inspect Media* |
| ***Derived Security Requirements*** | | |
| **1.3** Ensure the careful review and configuring of security options for remote access maintenance tools. Control systems often use remote control maintenance via operating system login. | MA-4 | NONLOCAL MAINTENANCE |
| | MA-5 | MAINTENANCE PERSONNEL |

**Table 2-10: Mapping Media Protection Requirements to Controls**

| CONTROL FAMILY | NIST 800-53 Relevant Security Controls | |
|---|---|---|
| MP - Media Protection | | |
| **TABLE 2-10: MAPPING REQUIREMENTS TO CONTROLS** | | |
| **SECURITY REQUIREMENTS** | **NIST 800-53 Relevant Security Controls** | |
| **MP - Media Protection** | | |
| ***Basic Security Requirements*** | | |
| **1.1** Protect information system media, both paper and digital;<br>**1.2** Limit access to information on information system media to authorized users;<br>**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 |
| ***Derived Security Requirements*** | | |
| **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 on any node. | MP-7(1) | MEDIA USE \| *Prohibit Use Without Owner* |
| **1.8** Incorporate policy management software to enforce media protection policy where applicable. | | |

**Table 2-11: Mapping Physical and Environmental Protection Requirements to Controls**

| CONTROL FAMILY | NIST 800-53<br>Relevant Security Controls | |
|---|---|---|
| PE - Physical and Environmental Protection | | |
| **TABLE 2-11: MAPPING REQUIREMENTS TO CONTROLS** | | |
| **SECURITY REQUIREMENTS** | **NIST 800-53<br>Relevant Security Controls** | |
| **PE - Physical and Environmental Protection** | | |
| ***Basic Security Requirements*** | | |
| **1.1** Limit physical access to information systems, equipment, and the respective operating environments to authorized individuals;<br>**1.2** Protect the physical plant and support infrastructure for information systems;<br>**1.3** Provide supporting utilities for information systems;<br>**1.4** Protect information systems against environmental hazards;<br>**1.5** Provide appropriate environmental controls in facilities containing information systems. | PE-2 | PHYSICAL ACCESS AUTHORIZATIONS |
| | PE-3 | PHYSICAL ACCESS CONTROL |
| | PE-4 | ACCESS CONTROL FOR TRANSMISSION MEDIUM |
| | PE-5 | ACCESS CONTROL FOR OUTPUT DEVICES |
| | PE-6 | MONITORING PHYSICAL ACCESS |
| ***Derived Security Requirements*** | | |
| **1.6** Provide stringent access controls for a control system 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 | PE-3(2) | PHYSICAL ACCESS CONTROL \| *Facility Information System Boundaries* |
| | PE-3(4) | PHYSICAL ACCESS CONTROL \| *Lockable Casings* |

| | | |
|---|---|---|
| **1.7** Prevent unauthorized physical modification, manipulation, theft, removal, or destruction of existing control system environment. | PE-3(5) | PHYSICAL ACCESS CONTROL \| *Tamper Protection* |
| **1.8** Prevent unauthorized introduction of new systems, infrastructure, communication interfaces or other hardware into a control system environment. | | |
| **1.9** Use proper cabling when designing the control system 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. | PE-9 | POWER EQUIPMENT AND CABLING |
| | PE-14 | TEMPERATURE AND HUMIDITY CONTROLS |
| **1.10** Prohibit portable devices such as computers and computerized devices used for critical control system functions from leaving the control system area. Ensure that portable engineering workstations and handhelds containing sensitive information are never allowed outside of the control system network. Prevent unauthorized devices from entering control system facilities and connecting to control system networks. Maintain up-to-date patch management on portable devices. | PE-20 | ASSET MONITORING AND TRACKING |

**Table 2-12: Mapping Planning Requirements to Controls**

| CONTROL FAMILY | NIST 800-53<br>Relevant Security Controls | |
|---|---|---|
| PL - Planning | | |
| **TABLE 2-12: MAPPING REQUIREMENTS TO CONTROLS** | | |
| **SECURITY REQUIREMENTS** | **NIST 800-53<br>Relevant Security Controls** | |
| **PL - Planning** | | |
| ***Basic Security Requirements*** | | |
| **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. | PL-2 | SYSTEM SECURITY PLAN |
| | PL-4 | RULES OF BEHAVIOR |
| | PL-9 | CENTRAL MANAGEMENT |
| ***Derived Security Requirements*** | | |
| **1.2** Revisit the security plan upon installing or introducing a new control system to the environment to ensure security is addressed throughout the system lifecycle. | PL-7 | SECURITY CONCEPT OF OPERATIONS |
| **1.3** Incorporate "forward-looking" objectives into the security plan to account for the dynamic landscape of control system security. | PL-8(1) | INFORMATION SECURITY ARCHITECTURE \| *Defense-in-Depth* |

**Table 2-13: Mapping Program Management Requirements to Controls**

| CONTROL FAMILY | NIST 800-53 Relevant Security Controls | |
|---|---|---|
| PM - Program Management | | |
| **TABLE 2-13: MAPPING REQUIREMENTS TO CONTROLS** | | |
| **SECURITY REQUIREMENTS** | **NIST 800-53 Relevant Security Controls** | |
| **PM - Program Management** | | |
| ***Basic Security Requirements*** | | |
| **1.1** Implement security controls at an organizational level on top of the information security level;<br>**1.2** Clearly define the business mission so that an organization can successfully implement protection measures to satisfy the mission objective;<br>Adapted partially from UFC doc, not sure if necessary to state | PM-2 | SENIOR INFORMATION SECURITY OFFICER |
| | PM-3 | INFORMATION SECURITY RESOURCES |
| | PM-5 | INFORMATION SYSTEM INVENTORY |
| | PM-6 | INFORMATION SECURITY MEASURES OF PERFORMANCE |
| | PM-10 | SECURITY AUTHORIZATION PROCESS |
| | PM-11 | MISSION/BUSINESS PROCESS DEFINITION |
| ***Derived Security Requirements*** | | |
| None | | |

**Table 2-14: Mapping Personnel Security Requirements to Controls**

| CONTROL FAMILY | NIST 800-53 Relevant Security Controls | |
|---|---|---|
| PS - Personnel Security | | |
| **TABLE 2-14: MAPPING REQUIREMENTS TO CONTROLS** | | |
| **SECURITY REQUIREMENTS** | **NIST 800-53 Relevant Security Controls** | |
| **PS - Personnel Security** | | |
| ***Basic Security Requirements*** | | |
| **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;<br>**1.2** Ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers;<br>**1.3** Employ formal sanctions for personnel failing to comply with organizational security policies and procedures. | PS-3 | PERSONNEL SCREENING |
| | PS-4 | PERSONNEL TERMINATION |
| | PS-5 | PERSONNEL TRANSFER |
| | PS-8 | PERSONNEL SANCTIONS |
| ***Derived Security Requirements*** | | |
| **1.4** Establish a risk designation and screening criteria for relevant positions maintaining and controlling the control system. | PS-2 | POSITION RISK DESIGNATION |
| **1.5** Screen personnel in critical positions against specified criteria before granting them access to a particular control system**.** | | |
| **1.6** Carefully develop training programs to ensure that each employee has received relevant training to satisfy their job functions. | PS-6 | ACCESS AGREEMENTS |

**Table 2-15: Mapping Risk Assessment Requirements to Controls**

| SECURITY REQUIREMENTS | NIST 800-53<br>Relevant Security Controls | |
|---|---|---|
| **RA - Risk Assessment** | | |
| ***Basic Security Requirements*** | | |
| **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. | RA-3 | RISK ASSESSMENT |
| ***Derived Security Requirements*** | | |
| **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. | RA-2 | SECURITY CATEGORIZATION |
| **1.3** Utilize vulnerability scanning on necessary assets where risk and mitigation values justify the scan and do not diminish system functionality. | RA-5 | VULNERABILITY SCANNING |
| | RA-5(1) | VULNERABILITY SCANNING \| *Update Tool Capability* |
| | RA-5(5) | VULNERABILITY SCANNING \| *Privileged Access* |

**Table 2-16: Mapping System and Services Acquisition Requirements to Controls**

| SECURITY REQUIREMENTS | NIST 800-53 Relevant Security Controls | |
|---|---|---|
| **SA - System and Services Acquisition** | | |
| ***Basic Security Requirements*** | | |
| **1.1** Allocate sufficient resources to adequately protect organizational information systems;<br>**1.2** Employ system development life cycle processes that incorporate information security considerations;<br>**1.3** Employ software usage and installation restrictions;<br>**1.4** Ensure that third-party providers employ adequate security measures to protect information, applications, and services outsourced from the organization. | SA-2 | ALLOCATION OF RESOURCES |
| | SA-3 | SYSTEM DEVELOPMENT LIFE CYCLE |
| | SA-4 | ACQUISITION PROCESS |
| | SA-5 | INFORMATION SYSTEM DOCUMENTATION |
| | SA-11 | DEVELOPER SECURITY TESTING AND EVALUATION |
| | SA-13 | TRUSTWORTHINESS |
| ***Derived Security Requirements*** | | |
| **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 security. | SA-9 | EXTERNAL INFORMATION SYSTEM SERVICES |
| | SA-9(3) | EXTERNAL INFORMATION SYSTEM SERVICES \| *Establish/Maintain Trust Relationship with Providers* |

**Table 2-17: Mapping System and Communications Protection Requirements to Controls**

| CONTROL FAMILY | NIST 800-53 Relevant Security Controls | |
|---|---|---|
| **SC - System and Communications Protection** | | |
| **TABLE 2-17: MAPPING REQUIREMENTS TO CONTROLS** | | |
| **SECURITY REQUIREMENTS** | **NIST 800-53 Relevant Security Controls** | |
| **SC - System and Communications Protection** | | |
| ***Basic Security Requirements*** | | |
| **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;<br>**1.2** Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems. | SC-2 | APPLICATION PARTITIONING |
| | SC-3 | SECURITY FUNCTION ISOLATION |
| | SC-7 | BOUNDARY PROTECTION |
| ***Derived Security Requirements*** | | |
| **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 before selecting cryptographic protection. | SC-5 | DENIAL OF SERVICE PROTECTION |
| | SC-8 | TRANSMISSION CONFIDENTIALITY AND INTEGRITY |
| | SC-8(1) | TRANSMISSION CONFIDENTIALITY AND INTEGRITY \| *Cryptographic or Alternate Physical Protection* |
| **1.4** Implement a virtual private network (VPN) in the control system environment if the control system control 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 | SC-11(1) | TRUSTED PATH \| *Logical Isolation* |

| | | |
|---|---|---|
| that implementing the VPN does not unacceptably affect network traffic. | SC-13 | CRYPTOGRAPHIC PROTECTION |
| **1.5** Configure control systems 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. | SC-24 | FAIL IN KNOWN STATE |

**Table 2-18: Mapping System and Information Integrity Requirements to Controls**

| CONTROL FAMILY | NIST 800-53 Relevant Security Controls | |
|---|---|---|
| **SI - System and Information Integrity** | | |
| **TABLE 2-18: MAPPING REQUIREMENTS TO CONTROLS** | | |
| **SECURITY REQUIREMENTS** | **NIST 800-53 Relevant Security Controls** | |
| **SI - System and Information Integrity** | | |
| ***Basic Security Requirements*** | | |
| **1.1** Identify, report, and correct information and information system flaws in a timely manner;<br>**1.2** Provide protection from malicious code at appropriate locations within organizational information systems;<br>**1.3** Monitor information system security alerts and advisories and take appropriate actions in response. | SI-2 | FLAW REMEDIATION |
| | SI-3 | MALICIOUS CODE PROTECTION |
| | SI-5 | SECURITY ALERTS, ADVISORIES, AND DIRECTIVES |
| ***Derived Security Requirements*** | | |
| **1.4** Implement antivirus tools when deemed acceptable within the control system. Follow vendor recommendations on all relevant servers and computers and ensure up-to-date patching of any antivirus software. | SI-2(1) | MALICIOUS CODE PROTECTION \| *Central Management* |
| **1.5** Deploy intrusion detection systems (IDS) and intrusion prevention systems (IPS) when deemed acceptable within the control system 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. | SI-4(1) | INFORMATION SYSTEM MONITORING \| *System-Wide Intrusion Detection System* |
| | SI-4(13) | INFORMATION SYSTEM MONITORING \| *Analyze Traffic / Event Patterns* |

| | | |
|---|---|---|
| **1.6** When deploying patches to a control system, adequately test the patch to determine the acceptability of its side effects. Organizations should implement a systematic, accountable, and documented control system patch management process for managing exposure to vulnerabilities. | 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
- Department of Defense Chief Information Officer Memorandum "Control Systems Cybersecurity," December 1, 2018
- UFC 4-010-06, Cybersecurity of Facility-Related Control Systems, January 2017
- 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 DoD Instruction (DoDI) 8500.01 and DoDI 8510.01. DODI 8500.01 instructs the Director of DISA, under the authority, direction, and control of the DOD 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 DOD 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.

DODI 8500.01 further directs DOD Component heads to ensure all DOD 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.

DoDI 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 DOD Risk Management Framework (RMF) for DOD IT, establishing associated cybersecurity policy, and assigning responsibilities for executing and maintaining the DoD RMF.

Per DoD Directive (DoDD) 8000.01, all aspects of the DoD IE, including the DoD information network infrastructure, DoD enterprise IT service and solutions, National Security Systems, industrial control systems, 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 DoD Components must manage control systems and implement cybersecurity activities for control systems in accordance with DoDD 8000.01, DoDD 3020.40, DoDI 8500.01, 8510.01,

8530.01, and other existing statutes, regulations, and issuances regarding mission assurance and cybersecurity risk management.

DoDI 8510.01 establishes policy and assigns responsibilities for executing and maintaining the DoD RMF. Any DoD Component's use of control systems, like all DoD technology systems, is subject to DoDI 8510.01 authority and decision making. The RMF incorporates system criticality and DoD mission objectives when assessing control system 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 acts upon an environment. The control system can be simple (a fixed mechanical or electronic system), software-based (e.g. a printer driver, robot control system), or a human or other agent.

**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 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:** A 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.

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

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

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

1. Control System Platform 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
9. Traffic Control Systems
10. Transportation and Fueling Systems
11. Meteorological Control Systems
12. Building Control Systems
13. Utility Control Systems
14. Utility Monitoring and Control Systems

**FRCS may exist in other operating environments beyond DOD 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 assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

**Integrity:** The property whereby an entity has not been modified in an unauthorized manner.

**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 DoD Components/Agencies responsible for instantiating and operating one or more information systems and applications who may leverage a control system in fulfilment of their IT missions. In this context, the Mission Owner is not the DoD Enterprise or DoD Component/Agency Enterprise even though these entities may control and have oversite

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-DoD 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:** The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact.

**Risk Management Framework (RMF)**: As described in DoDI 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)
- DoD control system
- DoD Component
- Non-DoD 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 sub-system 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."