U.S. Department of Homeland Security
Transportation Security Administration

Informational Supplement for TSA Security Directive 1580/82-2022-01

Version 1.0

October 27, 2022

Informational Supplement for TSA Security Directive 1580/82-2022-01

Introduction

This document provides information to supplement TSA Security Directive (SD) 1580/82-2022-01, originally issued on October 18, 2022. To ensure enforceability under the performance-based approach in SD 1580/82-2022-01, this SD requires Owner/Operators (O/Os) to develop a Cybersecurity Implementation Plan (CIP), identifying the O/O's specific proposed means of compliance with TSA's SD requirements. The CIP must specifically identify how the O/O will meet each of the actions necessary to reach the following security outcomes:

- Implement network segmentation policies and controls to ensure that the OT system can continue to safely operate in the event that an IT system has been compromised;
- Implement access control measures to secure and prevent unauthorized access to Critical Cyber Systems;
- Implement continuous monitoring and detection policies and procedures to detect cybersecurity threats and correct anomalies that affect Critical Cyber System operations; and
- Reduce the risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers, and firmware on Critical Cyber Systems in a timely manner using a risk-based methodology.

This plan must be submitted to, and approved by, TSA. The purpose of this supplement is to provide support to O/Os in developing a CIP that establishes how the O/O has met or will meet the security outcomes required by the SD.

The CIP and other requirements in the SD 1580/82-2022-01 series complement the requirements in the SD 1580-21-01 and SD 1582-21-01 series, which remain in place. The CIP should, similarly, ensure that it complements and does not conflict with actions required by these previously issued directives. For example, the results of the vulnerability assessment required by the SD 1580-21-01 and SD 1582-21-01 series, can be used to inform the CIP. There are also areas where actions required by SD 1580/82-2022-01 are relevant to the Cybersecurity Incident Response Plan required by SD 1580-21-01A and SD 1582-21-01A. O/Os should ensure there is no conflict between actions identified the CIP and those described in the Cybersecurity Incident Response Plan.

This supplement includes a series of questions that O/Os may wish to consider to ensure that they are appropriately addressing the full scope of the requirements in the SD and providing sufficient detail in their CIP. TSA is not requiring O/Os to answer these questions as part of their CIP nor are O/Os required to implement all of the concepts identified in the questions. TSA recognizes that O/Os may have other considerations and/or capabilities relevant to the requirements. The questions are intended only to assist O/Os with translating the requirements

into action and action into a documented program. Nothing in this document shall be interpreted or applied as superseding the SD or any other Federal statutory or regulatory requirements.

The following pages contain a section by section overview of the SD's requirements and references to NIST cybersecurity guidance documents.

Identifying Critical Cyber Systems

SD 1580/82-2022-01 Section III.A. (Identifying Critical Cyber Systems)		**Reference:** National Institute of Standards and Technology Internal Report (NISTIR) 8179

Requirement in SD 1580/82-2022-01:
III. A. Identify the Owner/Operator's Critical Cyber Systems as defined in Section VII. of this Security Directive.

For the purposes of this SD, TSA defines a Critical Cyber System as any Information Technology (IT) or Operational Technology (OT) system or data that, if compromised or exploited, could result in operational disruption. Critical Cyber Systems includes business services that if compromised or exploited could result in operational disruption. *See* Section VII.A.

Identifying Critical Cyber Systems is a necessary step in executing a cybersecurity risk management strategy which ensures appropriate cybersecurity measures are employed on essential systems. While some systems may pose more risk than others, any system that could impact the necessary capacity of the O/O should be considered a Critical Cyber System.

NOTE: Section III.A.2. provides procedures for an O/O to notify TSA in writing that they do not have any Critical Cyber Systems. Before making that notification, TSA encourages O/Os to review this section and the questions below and document their responses/rationale.

Below are questions to consider when developing or providing details on current actions that are intended to meet the required security outcome of the SD:

- Have all business services that if compromised or exploited could result in operational disruption been identified?
- Does the CIP address all of the types of control systems and associated instrumentation that could generally be considered part of the O/O's Operational Technology, including devices, systems, networks, and controls that are used to operate and/or automate industrial processes such as Supervisory Control and Data Acquisition (SCADA) Systems, Positive Train Control (PTC), Wayside Interface Units (WIU), and Programmable Logic Controllers (PLC)?
- Does the categorization of Critical Cyber Systems adequately consider hardware, software, information, and services? For example, has the O/O considered critical software or software dependencies that are used for capabilities such as running elevated privilege or managing privileges; directing privileged access to networking or computer resources; controlling access to data or OT; performing a function critical to trust; or operating outside of normal trust boundaries for privileged access?
- Is there a process for reviewing and identifying changes to Critical Cyber Systems and making updates to the CIP?

Implementing Network Segmentation Policies and Controls

SD 1580/82-2022-01 Section III.B. (Network segmentation)		**Reference:** PR.AC-5 (NIST Cybersecurity Framework (CSF) 1.1), NIST Special Publication (SP) 800-53 Rev. 5 AC-4; AC-10, SC-7, SC-10 and SC-20 (See Appendix A for a crosswalk to SD 1580/82-2022-01.)

Requirement in SD 1580/82-2022-01:

III.B. Implement network segmentation policies and controls designed to prevent operational disruption to the Operational Technology system if the Information Technology system is compromised or vice versa. As applied to Critical Cyber Systems, these policies and controls must include:

1. *A list and description of—*
   a. *Information Technology and Operational Technology system interdependencies;*
   b. *All external connections to the Information Technology and Operational Technology system;*
   c. *Zone boundaries including a description of how Information Technology and Operational Technology systems are organized and defined into logical zones based on criticality, consequence, and operational necessity; and*
   d. *Policies to ensure Information Technology and Operational Technology system services transit the other only when necessary for validated business or operational purposes.*
2. *An identification and description of measures for securing and defending zone boundaries, that includes security controls—*
   a. *To prevent unauthorized communications between zones; and*
   b. *To prohibit Operational Technology system services from traversing the Information Technology system, and vice-versa, unless the content is encrypted or, if not technologically feasible, otherwise secured and protected to ensure integrity and prevent corruption or compromise while the content is in transit.*

Network segmentation policies and controls reduce the risk of unauthorized communication between zone boundaries[1] and specifically unauthorized communication between IT and OT systems. Security controls, such as information flow enforcement and boundary protection (discussed in the resources identified above) are key to this effort. Implementing segmentation will impede adversaries who have successfully entered the environment from producing cascading consequences and limit their ability to impact the entire process simultaneously.

Below are questions to consider when developing or providing details on current actions that are intended to meet the required security outcome of the SD:

[1] "Zone boundary" is a concept that describes the perimeter of a zone within a network architecture. *See* CISA: *Trusted Internet Connections 3.0*, at 4, available at https://www.cisa.gov/sites/default/files/publications/CISA%20TIC%203.0%20Overlay%20Handbook%20v1.1.pdf.

- Is there a cohesive set of network/system architecture diagrams or other inventory documentation, including but not limited to nodes, interfaces, and information flows in which a Critical Cyber System resides?
- Is there a network security architecture (i.e., showing placement of IPS/IDS, firewall and router configuration, Security Information and Event Management (SIEM))?
- Do network segmentation policies and security controls consider the impact of a compromise in a particular segment of the OT system, *e.g.*, is the OT system segmented to ensure that it continues to safely operate when one in a cluster of connected OT systems is compromised?
- IT and OT systems are sometimes connected for efficiency or economy, such as common or public networks used for communication or as integral parts of a larger system. Are there controls or management in place that recognize these systems may be connected to OT systems or have access to data and capabilities that the system was not designed to protect?
- Are there procedures to ensure devices on either side of segmentation lines/zone boundaries are not connected unless they meet limited exceptions? If these connections are permitted, are logical access control measures such as firewalls in place to protect these devices?
- If relying on firewalls to protect networks, do the firewalls inspect for valid control system protocol content?
- Do policies and controls include processes or capabilities to identify and control network back doors?
- Is there a process to ensure systems are in working order with a secure connection?
- Do procedures establish and document business requirements for external connection to/from Critical Cyber Systems?

System Access Control Policies and Procedures: Preventing Unauthorized Access

SD 1580/82-2022-01 Sections III.C. (Preventing unauthorized access)		**Reference:** PR.AC-1 (NIST Cybersecurity Framework (CSF) 1.1), NIST Special Publication (SP) 800-53 Rev. 5, IA-1-5, IA-7-12 and NIST SP 800-63B

Requirement in SD 1580/82-2022-01:

III.C. Implement access control measures, including for local and remote access, to secure and prevent unauthorized access to Critical Cyber Systems. These measures must incorporate the following policies, procedures, and controls:

1. *Identification and authentication policies and procedures designed to prevent unauthorized access to Critical Cyber Systems that include—*
   a. *A policy for memorized secret authenticator resets that includes criteria for when resets must occur; and*
   b. *Documented and defined mitigation measures for components of Critical Cyber Systems that will not fall under the policy required by the preceding subparagraph (III.C.1.a), and a timeframe to complete these mitigations.*

Strong identification and authentication policies and procedures including a comprehensive password management policy are a core component of an access control system. The lack of effective password management policies and practices may allow for unauthorized access and the exploitation of vulnerabilities in Critical Cyber Systems. These policies should be compliant with the most current version of the NIST SP 800-63, *Digital Identity Guidelines.*

Below are questions to consider when developing or providing details on current actions that are intended to meet the required security outcome of the SD:

- Does the CIP cover account lockout, minimum password strength requirements, and changing default passwords before OT or IT devices are deployed? Are policy management tools/compliance measure tools/network architecture tools used to ensure devices are placed appropriately within your operational facilities?
- Are all new passwords screened against lists of commonly used and compromised passwords?
- Does the CIP include a policy for memorized secret authenticator resets that includes criteria for when resets must occur?
- Do identification and authentication policies distinguish between local and remote access?
- Do you have a policy for actions to be taken when a password is compromised?
- Do policies require resetting default passwords and provide a schedule for these resets?
- Are logical controls in place to manage access to the O/O's SCADA network infrastructure configuration?

- Does the CIP include a list of Critical Cyber Systems components and devices that do not have password resets applied within the established schedule? For each of these components/devices (or groups based on location or system),
  - What additional security measures are in place to mitigate risk of not having passwords updated within the approved timeframe?
    - What physical controls are in place to protect the system?
    - What logical controls are in place to protect the system?
- Do network controls enforce credential requirements?

System Access Control Policies and Procedures: Supplementing Password Authentication with Multi-Factor Authentication or Other Logical and Physical Security Controls

SD 15280/82-2022-01 Section III.C.2. (Multi-factor authentication or other controls)		**Reference:** PR.AC-7 (NIST Cybersecurity Framework (CSF) 1.1), AC-14, IA-I3, IA-5, IA-8 thru IA-11 and NIST Special Publication (SP) 800-63B

Requirement in SD 1580/82-2022-01:

III.C. Implement access control measures, including those for local and remote access, to secure and prevent unauthorized access to Critical Cyber Systems. These measures must incorporate the following policies, procedures, and controls:

2. *Multi-factor authentication, or other logical and physical security controls that supplement password authentication to provide risk mitigation commensurate to multi-factor authentication. If an Owner/Operator does not apply multi-factor authentication for access to Operational Technology components or assets, the Owner/Operator must specify what compensating controls are used to manage access.*

Accounts using only a username and password are vulnerable to known attack types, including password spraying and credential stuffing. MFA effectively protects against these attack types and associated unauthorized access. The intent is to employ MFA where appropriate and, where it is not, to ensure strong physical and other security controls are in place that meet or exceed the protection that MFA affords.

Below are questions to consider when developing or providing details on current actions that are intended to meet the required security outcome of the SD:

- If MFA is not being applied in operations centers, are there compensating controls for physical and logical access in place, such as isolating ICS workstations from the IT network to provide an equivalent level of security to that of MFA?
- Does the CIP identify what type of MFA is being used and the specific controls being provided through the capability, *e.g.*, if using logical tools such as password vault software paired with MFA to check out elevated credentials, is each use documented and accounted for?
- Does the CIP describe the policies and analysis used for determining if MFA will not be applied?
- For any systems where MFA is not being applied
  - Does the CIP articulate why MFA is not being applied?
  - Does the CIP require any of the following for securing access to OT systems that do not have MFA?
    - Workflow controls for access to covered devices: restrict and control access to OT equipment that only allow secured access to communicate with OT equipment through implementing firewall controls.

- Verifying that all physical security measures are in place to reduce exposure to onsite OT equipment, including programmable logic controllers (PLCs).
- PLCs are subject to network security controls that secure the connection between PLCs and control centers and remote/field PLCs.
- Network traffic is limited for remote PLC sites.
- PLCs are configured to only allow authorized communication to other PLCs.
- Operations (control) centers have countermeasures like access control systems, cameras, and other devices to assist with monitoring at all times.

- Does the CIP identify an array of overlapping and complementary physical controls such as—
  - Providing continuous 24/7 perimeter and interior monitoring by security guards or video surveillance.
  - Ensuring adequate perimeter fencing and locked gates to prevent unauthorized access.
  - Establishing badged-secure access to buildings, floors, and/or vestibules, as appropriate, for facilities with other Critical Cyber Systems that do not require MFA.
  - Limiting access to facilities with Critical Cyber Systems to individuals who require access in performance of their official duties.
  - Employing an alarm system to issue alerts when an individual is on-site at an unmanned facility.
  - Installing an inactivity timer on all OT workstations that locks the screen after a limited amount of time.
  - Disabling Universal Serial Bus (USB) ports on all OT devices and ensuring unauthorized media and hardware are never connected to OT infrastructure and related IT infrastructure.
- Does the CIP include an array of overlapping and complementary logical security controls, such as—
  - Policies requiring changing default passwords before installation or operationally deploying IT or OT devices.
  - Requiring MFA for all remote access.
  - Requiring single factor authentication with unique user IDs and passwords for local access to OT systems.
  - Providing continuous 24/7 monitoring for anomalous activity and security events.
  - Using layers of firewalls and intrusion prevention systems to protect Critical Cyber Systems.
  - Installing antivirus software on OT devices.
  - Prohibiting direct remote internet access to OT systems.
  - System-enforced requirements for minimum password length and prohibition of the use of dictionary words.
- If using "smartcards" as a second factor authentication instead of MFA—
  - Does the smartcard lockout after a specified number of failed combination events?
  - Are smartcard certificates cancelled within specified timeframe if the smartcard is reported lost or stolen?

  - Does the smartcard include security features such as "lockout?"
  - Does the smartcard restrict login events?
  - Does the smartcard have features that prevent tampering or creating replicas that could be used to gain access to IT or OT system?
- If not currently requiring MFA or other compensating security controls, does the CIP identify a detailed schedule for implementation that includes target dates, milestones, and a timeframe that recognizes the urgent need for applying these controls in light of current threat information?

System Access Control Policies and Procedures: Applying Principles of Least Privilege and Separation of Duties

SD 1580/82-2022-01 Section III.C.3. (Managing access rights)		**Reference:** PR.AC-4 (NIST CSF 1.1), AC-5-6, and AC-24

Requirement in SD 1580/82-2022-01:

III. C. Implement access control measures, including for local and/or remote access, to secure and prevent unauthorized access to Critical Cyber Systems. These measures must incorporate the following policies, procedures, and controls:

3. *Policies and procedures to manage access rights based on the principles of least privilege and separation of duties. Where not technically feasible to apply these principles, the policies and procedures must describe the compensating controls that the Owner/Operator will apply.*

Managing access rights based on the principles of least privilege[2] and separation of duties is an important initial step in mitigating the potential for identity compromises. Identity compromises are a common attack vector and implementing these controls greatly reduces the impact from successful compromises by limiting what can be done with any credentials and making intrusions more visible in the use of these credentials. Controlling access to and closely monitoring user accounts is a foundational control necessary to limit the extent of disruption and damage caused by potential intrusions.

Below are questions to consider when developing or providing details on current actions that are intended to meet the required security outcome of the SD:

- Do policies and procedures clearly delineate clear separation of duties? Is there any one person (e.g., CEO/COO/CIO) who has administrative access to all areas?
- Do policies and procedures recognize and apply policies of least privilege beyond "users," such as to entities, systems, services, etc.?
- Do policies limit access only for the duration of performing a given function whenever possible when there is not a persistent need for access?
- Does the CIP address access control policies that may apply, including access control lists within and between network segments and access to software and hardware? Are there access enforcement tools, mechanisms in place?
- Do access control policies include processes to perform policy enforcement, audit user accounts, manage user access and authenticate and authorize appropriate policies?
- Is there a schedule for verification of continued need of elevated privilege account access to IT and OT systems?
- Are documents establishing date of last verification maintained and is there a schedule for review of records and verification?

[2] "Least Privilege" refers to the principle that a security architecture should be designed so that each entity (system or user) is granted the minimum system resources and authorizations that the entity needs to perform its function. *See* https://csrc.nist.gov/glossary/term/least_privilege.

System Access Control Policies and Procedures: Limiting Use of Shared Accounts

SD 1580/82-2022-01 Section III.C.4 (Limit availability and use of shared accounts)		**Reference:** PR.AC-1, PR.AC-4 (NIST Cybersecurity Framework (CSF) 1.1) NIST 800-53 REV 5, AC-2(9) and NIST Special Publication (SP) 800-63B

Requirement in SD 1580/82-2022-01:

III. C. Implement access control measures, including for local and/or remote access, to secure and prevent unauthorized access to Critical Cyber Systems. These measures must incorporate the following policies, procedures, and controls:

4. *Enforcement of standards that limit the availability and use of shared accounts to those that are critical for operations, and then only if absolutely necessary. When the Owner/Operator uses shared accounts for operational purposes, the policies and procedures must ensure—*
    a. *Access to shared accounts is limited through account management that uses principles of least privilege and separation of duties; and*
    b. *Individuals who no longer need access do not have knowledge of the password necessary to access the shared account.*

TSA recognizes that, in some control system environments, management may make a risk-based decision to allow shared accounts. If that occurs, the risk associated with that decision needs to be managed with appropriate compensating controls. It is best to use individual user accounts where technically feasible. Establishing and enforced unique accounts for each individual user and administrator addresses this need, with security requirements for certain types of accounts and prohibited sharing accounts.

Below are questions to consider when developing or providing details on current actions that are intended to meet the required security outcome:

- If a risk-based decision has been made to allow shared accounts, how is the risk associated with that decision being managed with appropriate compensating controls?
- Does the CIP include policies and procedures that address measures that limit the availability and use of shared accounts to those that are critical for operations where the use of a unique account could compromise operational needs (including safety)?
- How is access to shared accounts limited through account management using principles of least privilege and separation of duties?
- What policies and mechanisms are used to ensure individuals who no longer need access to a shared account do not have knowledge of the password necessary to access the shared account?
- What policies are in place for resetting passwords for shared accounts after an employee leaves the company?

- If relying on a third-party/vendor to provide password vaults or other capabilities to limit access to specific shared accounts, which specific vendor/capability is being used and what features are being included to address the specific security outcome required by the SD?

System Access Control Policies and Procedures: Managing Domain Trust Relationships

1580/82-2022-01 **Section**: **III.C.5. (Domain trust relationships)**		**Reference:** SA-9(3), (NIST Cybersecurity Framework (CSF) 1.1), NIST 800.207 Zero Trust Architecture, and NIST 800-53 REV 5, SC1 – SC4

Requirement in 1580/82-2022-01:

III.C. Implement access control measures, including for local and/or remote access, to secure and prevent unauthorized access to Critical Cyber Systems. These measures must incorporate the following policies, procedures, and controls:

5. *Regularly updated schedule for review of existing domain trust relationships to ensure their necessity and establish policies to manage these relationships.*

In environments with shared trust between the OT and IT environments, a compromise to an IT system can immediately and directly place the OT system at risk. Severing these identity trusts is a critical safeguard in light of current threats. If credentials from a shared or trusted store have been previously comprised, any system that trusts those credentials is put in immediate risk.

Below are questions to consider when developing or providing details on current actions that are intended to meet the required security outcome of the SD:

- Does the CIP require a review of trust relationships and appropriate risk mitigation before making any changes or additions to IT or OT systems infrastructure or workflows connected to, or communicating with, Critical Cyber Systems?
- What procedures are required for authentication and authorization (by subject and device) before allowing access to IT or OT systems?
- If O/O uses cloud-based assets, remote access, or other capabilities that are not located within an enterprise-owned network boundary, how are assets, services, workflows, network accounts, etc., being reviewed and monitored to ensure security of Critical Cyber Systems?
- Does the CIP include a documented schedule for the review of existing domain trust relationships, including actors, assets, and processes using or potentially affecting Critical Cyber Systems?

Continuous Monitoring and Detection Policies: Implementing Measures to Prevent Malicious Code from Executing

1580/82-2022-01 Section: III.D.1.a.-e. (Continuous Monitoring and Prompt Detection)		**Reference:** DE.AE 1 – 5, DE.CM 1 – 8 (NIST Cybersecurity Framework (CSF) 1.1)

Requirement in 1580/82-2022-01:

III. D. Implement continuous monitoring and detection policies and procedures that are designed to prevent, detect, and respond to cybersecurity threats and anomalies affecting Critical Cyber Systems. These measures must include:

1. *Capabilities to—*
   a. *Defend against malicious email, such as spam and phishing emails, to preclude or mitigate against adverse impacts to operations;*
   b. *Block ingress and egress communications with known or suspected malicious Internet Protocol addresses;*
   c. *Control impact of known or suspected malicious web domains or web applications, such as by preventing users and devices from accessing malicious websites;*
   d. *Block and prevent unauthorized code, including macro scripts, from executing; and*
   e. *Monitor and/or block connections from known or suspected malicious command and control servers (such as Tor exit nodes, and other anonymization services).*

Implementing appropriate filters to detect and prevent the execution of malicious code is a necessary element of a defense-in-depth strategy. Protective Domain Name System (DNS) resolution is a best practice to proactively block communications with known or potentially malicious web domains. Basic access controls, such as filters and DNS analysis capabilities, provide protection from cyber-attacks by preventing the execution of malicious software and communication with unauthorized servers.

Below are questions to consider when developing or providing details on current actions that are intended to meet the required security outcome of the SD:

- What capabilities are present for continuous monitoring[3] and detection of cybersecurity threats and anomalies?
- Do these capabilities ensure immediate detection of cybersecurity threats and correct anomalies affecting the quality of their IT and OT system processes affecting Critical Cyber Systems?

[3] NIST 800-160 (Systems Security Engineering) defines "monitoring" as the continual checking, supervision, critically observing or determining the status in order to identify change from the performance level required or expected. The intent of monitoring is to detect and respond to cybersecurity threats and anomalies. Required monitoring and detection capabilities are listed in Section III.D.1., required procedures are listed in III.D.2., and required logging policies are listed in Section III.D.3.

- Does the CIP include identifying and responding to anomalies and events that occur beyond the network (e.g., unusual user access or modification or external environments) that could affect Critical Cyber Systems?
- Does the CIP include procedures to ensure detection processes and capabilities are maintained and tested?
- Is there continuous, end-to-end monitoring of IT and OT systems with capability to pinpoint cybersecurity incidents when they occur?
- What aspects of the systems are being monitored? For example, are the following being continually monitored: network, physical environments, users, and service provider activity?
- Are vulnerability scans performed on Critical Cyber Systems?
- Are there immediate alerts and logs for cybersecurity events (real-time detection and notifications)?
- What specific capabilities are being used to detect malicious email, ingress and egress communications with known or suspected malicious IP addresses, and known or suspected malicious web domains or web applications? If a specific third-party or vendor capability, what is the specific name of the program or capability and, if there are optional features, which are being deployed on the O/O's system to address the requirements in the SD?
- What capabilities are being used to block and prevent unauthorized code and block connections from known or suspected malicious command and control servers? If a specific third-party or vendor capability, what is the specific name of the program or capability and, if there are optional features, which are being deployed on the O/O's system to address the requirements in the SD?
- What controls are being implemented to limit the use of macros only for approved business purposes and block the use of macros across the rest of the organization?
- Are group policies being used to restrict the use of macros for non-business-related use?
- What complementary security controls are being used, such as software which scans for malicious macro activities, e-mail attachments, or suspicious web links?
- Does the CIP require developing and maintaining a software inventory list of approved software and procedures in place for fully evaluating software before it is added to approved list or authorized for a specific user or group?
- Are there policies and controls in place to prevent users from downloading software?

Continuous Monitoring and Detection Policies: Responding to Unauthorized Access and/or Code

1580/82-2022-01 Section: III.D.2.a.-d. (Auditing and responding to incidents)		**Reference:** DE.AE-1- 5, PR.PT-4, DE.CM 1 -7, and PR.PT - 1 (NIST Cybersecurity Framework (CSF) 1.1)

Requirement in 1580/82-2022-01:

III. D. Implement continuous monitoring and detection policies and procedures that are designed to prevent, detect, and respond to cybersecurity threats and anomalies affecting Critical Cyber Systems. These measures must include:

2. *Procedures to—*
   a. *Audit unauthorized access to internet domains and addresses;*
   b. *Document and audit any communications between the Operational Technology system and an external system that deviates from the Owner/Operator's identified baseline of communications;*
   c. *Identify and respond to execution of unauthorized code, including macro scripts; and*
   d. *Implement capabilities (such as Security, Orchestration, Automation, and Response) to define, prioritize, and drive standardized incident response activities.*

Risk to Critical Cyber Systems can be reduced by ensuring prompt procedures are in place for responding to the detection of cybersecurity threats and anomalies. This includes audits of unauthorized access and deviations from baseline communications[4] with external systems[5]. Often, when a cybersecurity incident occurs, the focus is primarily on recovery to normal operations. It is also critical to have strong procedures in place to ensure that critical data is not destroyed that could identify perpetrators and vulnerabilities.

Below are questions to consider when developing or providing details on current actions that are intended to meet the required security outcome of the SD:

- Does the CIP identify roles and responsibilities for the overall detection process, ensuring activities align with compliance needs and results are fully tested, communicated to senior managements, and continuously improved upon?

[4] Baseline of communications are the traffic patterns between systems and networks that are developed by continuous network monitoring. Baseline communication is the normal everyday traffic that occurs on an Owner/Operators' networks. Establishing communication baselines assist Owner/Operators in the identification of anomalous traffic and or events. For more information, refer to NIST 800-82R2 Section 5.16 Monitoring, Logging and Auditing.

[5] An external system is a system or component that is used by but is not a part of an organizational system and for which the organization has no direct control over the implementation of required security and privacy controls or the assessment of control effectiveness (see NIST SP 800-53R5).

- What policies and procedures are in place to document auditing of unauthorized access to internet domains or unauthorized communications between the OT system and external systems?
- What capabilities (such as SOAR) are in place to define, prioritize, and drive standardized incident response activities?
- Does the CIP include policies and procedures for identification, detection, and protection of Critical Cyber Systems against unauthorized software installation?
- Does the CIP include policies and procedures that demonstrate audits of unauthorized access to internet domains and addresses?
- What documentation and auditing procedures exist for communication traffic between OT systems and any external systems?

Continuous Monitoring and Detection Policies: Maintaining a Record to Support Response to Cybersecurity Incidents and Risk Mitigation

1580/82-2022-01 **Section: III.D.3. (Logging Policies)**		**Reference:** PR.PT-1, DE.AE-3, AU Family, and NIST 800-53 (NIST Cybersecurity Framework (CSF) 1.1)

Requirement in 1580/82-2022-01:

III. D. Implement continuous monitoring and detection policies and procedures that are designed to prevent, detect, and respond to cybersecurity threats and anomalies affecting Critical Cyber Systems. These measures must include:

3. *Logging policies that –*
    a. *Require continuous collection and analyzing of data for potential intrusions and anomalous behavior on Critical Cyber Systems and other Operational and Information Technology systems that directly connect with Critical Cyber Systems; and*
    b. *Ensure data is maintained for sufficient periods to provide effective investigation of cybersecurity incidents.*

Effective Log retention policies may assist an organization in determining the scope of a cyber intrusion. The collection and analysis of network traffic is required to determine whether a threat actor has penetrated an O/O's IT or OT systems. This includes logs of the systems that directly connect to the Critical Cyber Systems to provide the appropriate context for any cybersecurity incidents. Event logs provide important insights into system and network activity. Following security log retention best practices for event logs helps confirm that security logging processes are protecting Critical Cyber Systems. TSA recommends that logs be retained for no less than one (1) year.

Below are questions to consider when developing or providing details on current actions that are intended to meet the required security outcome of the SD:

- Where logging of cybersecurity incidents is not technically feasible (e.g., logging degrades system performance beyond acceptable operational limits), what appropriate compensating security controls are being used to mitigate the risk (e.g., monitoring at the network boundary)?
- How are your logs configured and stored to ensure they are secure and appropriately maintained?
- What steps are in place for analyzing log data, including prioritization of log entries for review?

Continuous Monitoring and Detection Policies: Isolating Industrial Control Systems

1580/82-2022-01 Section: III.D.4: (Isolation of Industrial Control Systems)		**Reference:** PR.AC-5 (NIST Cybersecurity Framework (CSF) 1.1) and NIST 800 – 82 – 5 – ICS Security Architecture

Requirement in 1580/82-2022-01:

III. D. Implement continuous monitoring and detection policies and procedures that are designed to prevent, detect, and respond to cybersecurity threats and anomalies affecting Critical Cyber Systems. These measures must include:

4. *Mitigation measures or manual controls to ensure industrial control systems can be isolated when a cybersecurity incident in the Information Technology system creates risk to the safety and reliability of the Operational Technology system.*

Due to many factors of an O/O's IT system, including size and complexity, external connections and potential vulnerabilities (hardware, software, systems), it is much more likely that an O/O will experience a cyber incident impacting their IT network. O/Os should have policies and procedures that allow for the prompt isolation of the OT network to minimize the potential for the spread of malicious or unauthorized data from their IT network to their OT network. These measures and controls may be in addition to those described in the O/O's Cybersecurity Incident Response Plan but should not conflict with this Plan.

Below are questions to consider when developing or providing details on current actions that are intended to meet the required security outcome of the SD:

- What procedures are in place that implement mitigation measures or manual controls to ensure industrial control systems can be isolated when a cybersecurity incident in the IT system creates risk to the safety and reliability of the OT system?
- Does the CIP address network segmentation and segregation procedures used to enable isolation?
- What policies and procedures are in place for deployment, configuration and maintenance of firewalls?
- Does the CIP include documented access points between Information Technology Operational Technology systems?

Patch Management Strategy: Keeping Patches and Updates Current to Reduce Risk of Exploitation

1580/82-2022-01 Section: III.E. (Applying security patches and updates)		**Reference:** ID.RA-1, ID.RA-6 (NIST Cybersecurity Framework (CSF) 1.1), RS.MI-3, and RS.AN - 5

Requirement in 1580/82-2022-01:

III.E. Reduce the risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers, and firmware on Critical Cyber Systems consistent with the Owner/Operator's risk-based methodology. These measures must include—

1. *A patch management strategy that ensures all critical security patches and updates on Critical Cyber Systems are current.*
2. *The strategy required by Section III.E.1. must include:*
   a. *The risk methodology for categorizing and determining criticality of patches and updates, and an implementation timeline based on categorization and criticality; and*
   b. *Prioritization of all security patches and updates on the Cybersecurity and Infrastructure Security Agency's Known Exploited Vulnerabilities Catalog.*
3. *If the Owner/Operator cannot apply patches and updates on specific Operational Technology systems without causing a severe degradation of operational capability to meet necessary capacity, the patch management strategy must include a description and timeline of additional mitigations that address the risk created by not installing the patch or update.*

There is substantially higher risk of compromise in cyber systems where security updates and patches are not installed. A strong patch and update management strategy is a critical characteristic of an effective cybersecurity program to appropriately address known vulnerabilities based on criticality of the underlying asset.

Below are questions to consider when developing or providing details on current actions that are intended to meet the required security outcome of the SD:

- Does the CIP describe the risk methodology used for categorizing and determining the criticality of, and implementation priority for, application of security patches and updates?
- Does this process include a severity rating system and process for prioritizing testing and application of patches/updates consistent with recognized application vulnerabilities?
- Are there procedures and policies in place to monitor for patch updates and prioritization identified by CISA?
- Does the CIP include processes for identifying vulnerabilities if patches/updates not applied either within the recommended timeframe or, in limited circumstances, never,

and ensure mitigation measures are in place to address those vulnerabilities, including timeline for implementation?

- Do required mitigation measures include both logical and physical security controls?
- Does the CIP include the policies and procedures used to document the application of security patches and updates?
- Does the CIP include timelines for implementation of patches and updates?

Acronyms

CFR	Code of Federal Regulation
CISA	Cybersecurity and Infrastructure Security Agency
CIP	Cybersecurity Implementation Plan
CRR	Cyber Resilience Review
CSF	Cyber Security Framework
DNS	Domain Name System
ICS	Industrial Control System
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
JIT PAM	Just-In-Time Privileged Account Management
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Internal Report
O/O	Owner/Operator
OT	Operational Technology
PLC	Programmable Logic Controllers
PTC	Positive Train Control
SCADA	Supervisory Control and Data Acquisition
SD	Security Directive
SIEM	Security Information and Event Management
SOAR	Security, Orchestration, Automation, and Response
SP	Special Publication
TSA	Transportation Security Administration
USB	Universal Serial Bus
VPN	Virtual Private Network
WIU	Wayside Interface Unit

Appendix A: NIST Publication Reference Chart

Resource	Resource Reference/ Framework Category	Applicability	URL	Section
NIST SP 800-53 Rev. 5 AC-1	Access Control(AC)	Policy and procedures development, documentation, and dissemination	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_0/home?element=AC-1	1580/82-2022-01 Section III.C.1 (Preventing unauthorized access)
NIST SP 800-53 Rev. 5 AC-2 (9)	Access Control(AC)	Restrictions on use of shared and group accounts -- Only permit the use of shared and group accounts that meet [Assignment: organization-defined conditions for establishing shared and group accounts	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_0/home?element=AC-2	1580/82-2022-01 Section III.C4 (Limit Availability and use of shared accounts)
NIST SP 800-53 Rev. 5 AC-4	Access Control(AC)	Information Flow Enforcement	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_0/home?element=AC-4	1580/82-2022-01 Section III.C4 (Limit Availability and use of shared accounts)
NIST SP 800-53 Rev. 5 AC-5	Access Control(AC)	Separations of Duties - Identify and document and Define system access authorizations to support separation of duties.	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_0/home?element=AC-5	1580/82-2022-01 Section III.C.3. (Managing access rights)
NIST SP 800-53 Rev. 5 AC-6	Access Control(AC)	Least Privilege - Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_0/home?element=AC-6	1580/82-2022-01 Section III.C.3. (Managing access rights)
NIST SP 800-53 Rev. 5 AC-10	Access Control(AC)	Concurrent Session Control	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_0/home?element=AC-10	1580/82-2022-01 Section III.B. (Network segmentation)
NIST SP 800-53 Rev. 5 AC-14	Access Control(AC)	Permit Actions without Identification or authentication	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_0/home?element=AC-14	1580/82-2022-01 Section III.C.2. (Multi-factor authentication or other controls)
NIST SP 800-53 Rev. 5 AC-24	Access Control(AC)	Access Control Decisions - Establish procedures, Implement mechanisms to ensure organization-defined access control decisions are applied to each access request prior to access enforcement.	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_0/home?element=AC-24	1580/82-2022-01 Section III.C.3. (Managing access rights)

Resource	Resource Reference/ Framework Category	Applicability	URL	Section
NIST SP 800-53 Rev. 5 AU Family	Audit and Accountability(AU)	AU-1: Audit And Accountability Policy And Procedures AU-2: Audit Events AU-2(3): Reviews And Updates AU-3: Content Of Audit Records AU-4: Audit Storage Capacity AU-5: Response To Audit Processing Failures AU-6: Audit Review, Analysis, And Reporting AU-7: Audit Reduction And Report Generation AU-8: Time Stamps AU-9: Protection Of Audit Information AU-10: Non-Repudiation AU-11: Audit Record Retention AU-12: Audit Generation AU-13: Monitoring For Information Disclosure AU-14: Session Audit AU-15: Alternate Audit Capability AU-16: Cross-Organizational Auditing	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_0/home?element=AU	1580/82-2022-01 Section: III.D.3. (Logging Policies)
NIST CSF 1.1 DE.CM-1	Detect (DE) Security Continuous monitoring (CM)	The network is monitored to detect potential cybersecurity events	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/CSF_1_1_0/home?element=DE.CM-1	1580/82-2022-01 Section: III.D.1.a.-e. (Continuous Monitoring and Prompt Detection)
NIST CSF 1.1 DE.CM-2	Detect (DE) Security Continuous monitoring (CM)	The physical environment is monitored to detect potential cybersecurity events	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/CSF_1_1_0/home?element=DE.CM-2	1580/82-2022-01 Section: III.D.1.a.-e. (Continuous Monitoring and Prompt Detection)
NIST CSF 1.1 DE.CM-3	Detect (DE) Security Continuous monitoring (CM)	Personnel activity is monitored to detect potential cybersecurity events	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/CSF_1_1_0/home?element=DE.CM-3	1580/82-2022-01 Section: III.D.1.a.-e. (Continuous Monitoring and Prompt Detection)
NIST CSF 1.1 DE.CM-4	Detect (DE) Security Continuous monitoring (CM)	Malicious code is detected	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/CSF_1_1_0/home?element=DE.CM-4	1580/82-2022-01 Section: III.D.1.a.-e. (Continuous Monitoring and Prompt Detection)
NIST CSF 1.1 DE.CM-5	Detect (DE) Security Continuous monitoring (CM)	Unauthorized mobile code is detected	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/CSF_1_1_0/home?element=DE.CM-5	1580/82-2022-01 Section: III.D.1.a.-e. (Continuous Monitoring and Prompt Detection)
NIST CSF 1.1 DE.CM-6	Detect (DE) Security Continuous monitoring (CM)	External service provider activity is monitored to detect potential cybersecurity events	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/CSF_1_1_0/home?element=DE.CM-6	1580/82-2022-01 Section: III.D.1.a.-e. (Continuous Monitoring and Prompt Detection)

Resource	Resource Reference/ Framework Category	Applicability	URL	Section
NIST CSF 1.1 DE.CM-7	Detect (DE) Security Continuous monitoring (CM)	Monitoring for unauthorized personnel, connections, devices, and software is performed	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/CSF_1_1_0/home?element=DE.CM-7	1580/82-2022-01 Section: III.D.1.a.-e. (Continuous Monitoring and Prompt Detection)
NIST CSF 1.1 DE.CM-8	Detect (DE) Security Continuous monitoring (CM)	Vulnerability scans are performed	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/CSF_1_1_0/home?element=DE.CM-8	1580/82-2022-01 Section: III.D.1.a.-e. (Continuous Monitoring and Prompt Detection)
NIST CSF 1.1 DE.AE-1	Detect (DE).Anomalies and Events (AE)	A baseline of network operations and expected data flows for users and systems is established and managed	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/CSF_1_1_0/home?element=DE.AE-1	1580/82-2022-01 Section: III.D.1.a.-e. (Continuous Monitoring and Prompt Detection)
NIST CSF 1.1 DE.AE-2	Detect (DE).Anomalies and Events (AE)	Detected events are analyzed to understand attack targets and methods	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/CSF_1_1_0/home?element=DE.AE-2	1580/82-2022-01 Section: III.D.1.a.-e. (Continuous Monitoring and Prompt Detection)
NIST CSF 1.1 DE.AE-3	Detect (DE).Anomalies and Events (AE)	Event data are collected and correlated from multiple sources and sensors	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/CSF_1_1_0/home?element=DE.AE-3	1580/82-2022-01 Section: III.D.1.a.-e. (Continuous Monitoring and Prompt Detection)
NIST CSF 1.1 DE.AE-4	Detect (DE).Anomalies and Events (AE)	Impact of events is determined	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/CSF_1_1_0/home?element=DE.AE-4	1580/82-2022-01 Section: III.D.1.a.-e. (Continuous Monitoring and Prompt Detection)
NIST CSF 1.1 DE.AE-5	Detect (DE).Anomalies and Events (AE)	Incident alert thresholds are established	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/CSF_1_1_0/home?element=DE.AE-5	1580/82-2022-01 Section: III.D.1.a.-e. (Continuous Monitoring and Prompt Detection)
NIST SP 800-53 Rev. 5 IA-1	Identification and Authentication (IA)	Identification and authentication policy and procedures	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_0/home?element=IA-1	1580/82-2022-01 Section III.C.2 (Preventing unauthorized access)
NIST SP 800-53 Rev. 5 IA-2	Identification and Authentication (IA)	Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_0/home?element=IA-2	1580/82-2022-01 Section III.C.1 (Preventing unauthorized access)
NIST SP 800-53 Rev. 5 IA-3	Identification and Authentication (IA)	Device Identification and Authentication -- Uniquely identify and authenticate [Assignment: organization-defined devices and/or types of devices] before establishing a [Assignment (one or more): local, remote, network] connection	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_0/home?element=IA-3	1580/82-2022-01 Section III.C.1 (Preventing unauthorized access)

Resource	Resource Reference/ Framework Category	Applicability	URL	Section
NIST SP 800-53 Rev. 5 IA-4	Identification and Authentication (IA)	Identifier Management -- Manage system identifiers by: Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, service, or device identifier; Selecting an identifier that identifies an individual, group, role, service, or device; Assigning the identifier to the intended individual, group, role, service, or device; and Preventing reuse of identifiers for [Assignment: organization-defined time	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_0/home?element=IA-4	1580/82-2022-01 Section III.C.1 (Preventing unauthorized access)
NIST SP 800-53 Rev. 5 IA-5	Identification and Authentication (IA)	Authenticator Management: Manage system authenticators by: Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator; Establishing initial authenticator content for any authenticators issued by the organization; Ensuring that authenticators have sufficient strength of mechanism for their intended use.	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_0/home?element=IA-5	1580/82-2022-01 Section III.C.1 (Preventing unauthorized access)
NIST SP 800-53 Rev. 5 IA-7	Identification and Authentication (IA)	Cryptographic Module Authentication -- Implement mechanisms for authentications to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_0/home?element=IA-7	1580/82-2022-01 Section III.C.1 (Preventing unauthorized access)
NIST SP 800-53 Rev. 5 IA-8	Identification and Authentication (IA)	Identification and Authentication (non-organizational Users) -- Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_0/home?element=IA-8	1580/82-2022-01 Section III.C.1 (Preventing unauthorized access)
NIST SP 800-53 Rev. 5 IA-9	Identification and Authentication (IA)	Service Identification and Authentication - Uniquely identify and authenticate [Assignment: organization-defined system services and applications] before establishing communications with devices, users, or other services or applications.	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_0/home?element=IA-9	1580/82-2022-01 Section III.C.1 (Preventing unauthorized access)
NIST SP 800-53 Rev. 5 IA-10	Identification and Authentication (IA)	Adaptive Authentication -- Require individuals accessing the system to employ [Assignment: organization-defined supplemental authentication techniques or mechanisms] under specific.	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_0/home?element=IA-10	1580/82-2022-01 Section III.C.1 (Preventing unauthorized access)
NIST SP 800-53 Rev. 5 IA-11	Identification and Authentication (IA)	Re-authentication -- Require users to re-authenticate when [Assignment: organization-defined circumstances or situations requiring re-authentication].	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_0/home?element=IA-11	1580/82-2022-01 Section III.C.1 (Preventing unauthorized access)

Resource	Resource Reference/ Framework Category	Applicability	URL	Section
NIST SP 800-53 Rev. 5 IA-12	Identification and Authentication (IA)	Identity Proofing - Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines; Resolve user identities to a unique individual; and collect, validate, and verify identity evidence	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_0/home?element=IA-12	1580/82-2022-01 Section III.C.1 (Preventing unauthorized access)
NIST CSF 1.1 ID.RA-1	Identify (ID) Risk Assessment (RA)	Asset vulnerabilities are identified and documented	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/CSF_1_1_0/home?element=ID.RA-1	1580/82-2022-01 Section: III.E. (Applying security patches and updates)
NIST CSF 1.1 ID.RA-6	Identify (ID) Risk Assessment (RA)	Risk responses are identified and prioritized	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/CSF_1_1_0/home?element=ID.RA-6	1580/82-2022-01 Section: III.E. (Applying security patches and updates)
NIST 800 – 82 – 5 – ICS	National Institute of Standards and Technology (NIST)	Industrial Control Systems (ICS) Security	https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final	1580/82-2022-01 Section: III.D.4: (Isolation of Industrial Control Systems)
NIST SP 800-207	National Institute of Standards and Technology (NIST)	Zero Trust Architecture	https://csrc.nist.gov/publications/detail/sp/800-207/final	1580/82-2022-01 Section: III.C.5. (Domain trust relationships)
NIST SP 800-53 Rev. 5	National Institute of Standards and Technology (NIST)	Catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets	https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final	1580/82-2022-01 Section III.B. (Network segmentation)
NIST SP 800-63B	National Institute of Standards and Technology (NIST)	Digital Identity Guidelines	https://pages.nist.gov/800-63-3/sp800-63b.html	1580/82-2022-01 Section III.C.2. (Multi-factor authentication or other controls)
NISTIR 8179	National Institute of Standards and Technology Interagency/Intemal Report (NISTIR) 8179	Criticality Analysis Process Model Prioritizing Systems and Components	https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8179.pdf	1580/82-2022-01 Section III.A. (Identifying Critical Cyber Systems)
NIST CSF 1.1 PR.AC-1	Protect (PR).Identity Management, Authentication and Access Contro1(AC)	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes,	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/CSF_1_1_0/home?element=PR.AC-1	1580/82-2022-01 Sections III.C.1. (Preventing unauthorized access)

Resource	Resource Reference/ Framework Category	Applicability	URL	Section
NIST CSF 1.1 PR.AC-4	Protect (PR).Identity Management, Authentication and Access Contro1(AC)	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/CSF_1_1_0/home?element=PR.AC-4	1580/82-2022-01 Section III.C.4 (Limit availability and use of shared accounts)
NIST CSF 1.1 PR.AC-5	Protect (PR).Identity Management, Authentication and Access Contro1(AC)	Network integrity is protected (e.g., network segregation, network segmentation	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/CSF_1_1_0/home?element=PR.AC-5	1580/82-2022-01 Section III.B. (Network segmentation)
NIST CSF 1.1 PR.AC-7	Protect (PR).Identity Management, Authentication and Access Contro1(AC)	Users, devices, and other assets are authenticated commensurate with risk of the transaction security and privacy risks and other organizational risk	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/CSF_1_1_0/home?element=PR.AC-7	1580/82-2022-01 Section III.C.2. (Multi-factor authentication or other controls)
NIST CSF 1.1 PR.PT-1	Protect(PR).Protecti ve Technology (PT)	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/CSF_1_1_0/home?element=PR.PT-1	1580/82-2022-01 Section: III.D.2.a.-d. (Auditing and responding to incidents)
NIST CSF 1.1 PR.PT-4	Protect(PR).Protecti ve Technology (PT)	Communications and control networks are protected	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/CSF_1_1_0/home?element=PR.PT-4	1580/82-2022-01 Section: III.D.2.a.-d. (Auditing and responding to incidents)
NIST CSF 1.1 RS.AN-5	Respond (RS) Analysis (AN)	Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/CSF_1_1_0/home?element=RS.AN-5	1580/82-2022-01 Section: III.E. (Applying security patches and updates)
NIST CSF 1.1 RS.MI-3	Respond (RS) Mitigation (MI)	Newly identified vulnerabilities are mitigated or documented as accepted risks	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/CSF_1_1_0/home?element=RS.MI-3	1580/82-2022-01 Section: III.E. (Applying security patches and updates)
NIST SP 800-53 Rev. 5 SC-1	System and Communication Protection (SC)	System and communications protection policy and procedures	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_0/home?element=SC-1	1580/82-2022-01 Section: III.C.5. (Domain trust relationships)
NIST SP 800-53 Rev. 5 SC-2	System and Communication Protection (SC)	Separation of system and user functionality	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_0/home?element=SC-2	1580/82-2022-01 Section: III.C.5. (Domain trust relationships)
NIST SP 800-53 Rev. 5 SC-3	System and Communication Protection (SC)	Security function isolation	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_0/home?element=SC-3	1580/82-2022-01 Section: III.C.5. (Domain trust relationships)

Resource	Resource Reference/ Framework Category	Applicability	URL	Section
NIST SP 800-53 Rev. 5 SC-4	System and Communication Protection (SC)	Information on shared system resources	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_0/home?element=SC-4	1580/82-2022-01 Section: III.C.5. (Domain trust relationships)
NIST SP 800-53 Rev. 5 SC-7	System and Communication Protection (SC)	Boundary Protection	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_0/home?element=SC-7	1580/82-2022-01 Section III.B. (Network segmentation)
NIST SP 800-53 Rev. 5 SC-10	System and Communication Protection (SC)	Network Disconnect	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_0/home?element=SC-10	1580/82-2022-01 Section III.B. (Network segmentation)
NIST SP 800-53 Rev. 5 SC-20	System and Communication Protection (SC)	Secure/Name/Address Resolution Service	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_0/home?element=SC-20	1580/82-2022-01 Section III.B. (Network segmentation)
NIST SP 800-53 Rev. 5 SA-9 (3)	System and Services Acquisition (SA)	Establish and Maintain Trust Relationship with Providers --establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions	https://csrc.nist.gov/Projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_0/home?element=SA-9	1580/82-2022-01 Section: III.C.5. (Domain trust relationships)

For an additional resource that crosswalks appropriate references to the NIST Cybersecurity Framework – See CISA *Cyber Resilience Review (CRR): NIST Cybersecurity Framework Crosswalks* pages 2-13. https://www.cisa.gov/sites/default/files/publications/4_CRR_4.0_Self_Assessment-NIST_CSF_v1.1_Crosswalk-April_2020.pdf

Appendix B

Suggested Format for Cybersecurity Implementation Plan (CIP)
TSA Security Directive 1580/82-2022-01

Purpose

The purpose of this document is to provide a suggested format for rail Owner/Operators covered under Security Directive (SD) 1580/82-2022-01 to consider when organizing materials for their required Cybersecurity Implementation Plan (CIP). Utilizing this suggested format will assist TSA in reviewing the CIPs and expediting the review process. Furthermore, this format will allow the Owner/Operator and TSA to have a mutual understanding of the CIP's content. Upon approval, the CIP becomes the enforceable document against which an individual Owner/Operator will be inspected to establish compliance with the SD.

This suggested format should be used in conjunction with the Informational Supplement provided by TSA to support the Owner/Operator's development of their CIP.

General Background on CIP Requirements

- Owner/Operators must submit their CIP to TSA no later than February 21, 2023 (120 days from the October 24, 2022 effective date of SD 1580/82-2022-01).
- The CIP must provide all information required by Sections III.A. through III.E. of the SD and describe in detail the Owner/Operator's defense-in-depth plan, including physical and logical security controls, for meeting each of the requirements in the SD.
- Owner/Operators may submit their CIP by one of three methods:
    - By email to SurfOpsRail-SD@tsa.dhs.gov with a password-protected document. The password to the document must be provided to TSA in a separate and unlinked email to the CIP document.
    - Uploaded to the secure Homeland Security Information Network (HSIN) portal (instructions provided separately). If uploading via the HSIN portal, password protection is not required.
    - By an Owner/Operator encrypted means after obtaining approval from TSA.
- The CIP must be marked and handled as "SENSITIVE SECURITY INFORMATION" (SSI) under 49 CFR part 1520. *See* best practices and other resources on TSA's website at https://www.tsa.gov/for-industry/sensitive-security-information. A sample page with appropriate SSI markings is attached for reference.

- Once approved by TSA, the Owner/Operator must implement and maintain all measures in the TSA-approved CIP within the schedule as stipulated in the plan.

- Owner/Operators may submit their CIP in separate sections (as separate documents) to TSA. The CIP does not have to be all in one document or follow the format provided in this document. If submitted in separate documents or a different format, the Owner/Operator must provide an index that clearly identifies which pages or files address specific requirements in the SD.

- If your designated Cybersecurity Coordinator is not the primary POC for TSA to contact regarding submission and/or contents of the CIP, please ensure your submission clearly identifies and provides contact information (name, title, telephone number, and email address) for the CIP POC. If a POC is not identified, TSA will direct any follow-on correspondences to the primary and alternate cybersecurity coordinators.

Plan Organization

Sections III.A. through III.E. of SD 1580/82-2022-01 provide the security outcomes the Owner/Operator's defense-in-depth plan must address. To meet these security outcomes, the defense-in-depth plan must include both physical and logical security controls. In general, there should be five primary sections within your CIP: (1) identification of critical cyber systems; (2) network segmentation; (3) access controls; (4) continuous monitoring, detection, and auditing; and (5) patch management. Within each of these sections, Owner/Operators must provide detailed and specific information on how they address the requirements in the SD, including processes, procedures, analysis, timelines, and oversight mechanisms, as applicable. For additional support, refer to the Informational Supplement for issues to consider when developing and providing details on current actions that meet the required security outcomes.

Owner/Operator:
Date:
POC Name/Contact Info (if not the current cybersecurity coordinator):

Section A (Identification of Critical Cyber Systems)

In this section the Owner/Operator identifies their Critical Cyber Systems in accordance with the definition provided in the Security Directive. Identifying Critical Cyber Systems, including both OT and IT systems, enables Owner/Operators to ensure they have adequately identified risks, including potential vulnerabilities and consequences, if that system is the target of a cyber-attack.

Section B (Network Segmentation)

In this section the Owner/Operator describes how they have implemented network segmentation policies and controls designed to prevent operational disruptions to the Operational Technology system if the Information Technology system is compromised or vice versa.

Section C (Access Controls)

In this section, the Owner/Operator describes how they have implemented access control measures, including for local and/or remote access, to secure and prevent unauthorized access to Critical Cyber Systems.

Section D (Continuous Monitoring, Detection and Auditing)

In this section, the Owner/Operator describes how they have implemented continuous monitoring and detection policies and procedures that are designed to prevent, detect, and respond to cybersecurity threats and anomalies affecting Critical Cyber System operations.

Section E (Patch Management)

In this section, the Owner/Operator describes how they have reduced the risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers, and firmware on Critical Cyber Systems consistent with the Owner/Operator's risk-based methodology.