# Cybersecurity Implementation Plan (CIP) Template

For Owner/Operators of Critical Cyber Systems subject to SD02C

**Background:**

TSA issued a Memorandum dated July 21, 2022, that directed all covered pipeline owner/operators (O/O) to meet the requirements of Security Directive Pipeline-2021-02C (SD02C). The memorandum specifically directed that each O/O: 1) Establish and implement a TSA-approved Cybersecurity Implementation Plan; 2) Develop and maintain a Cybersecurity Incident Response Plan to reduce the risk of operational disruption; and 3) Establish a Cybersecurity Assessment Program and submit an annual plan that describes how the O/O will assess the effectiveness of cybersecurity measures.

The Cybersecurity Implementation Plan (CIP) must provide the information required by Sections III.A. through III.E. of SD02C and describe in detail the O/O's defense-in-depth plan, including physical and logical security controls, for meeting each of the requirements in Sections III.A. through III.E.

This CIP was required to be submitted by each O/O within 90 days of the effective date of SD02C which was July 27, 2022. The plan required review and approval by TSA and once approved, the O/O must implement and maintain all measures contained in the CIP:

1. No later than 90 days after the effective date of this Security Directive, Owner/Operators must submit a Cybersecurity Implementation Plan to SurfOpsSD@ tsa.dhs.gov for TSA approval.

2. The Cybersecurity Implementation Plan must provide the information required by Sections III.A. through III.E. of this Security Directive 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 Sections III.A. through III.E.

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

4. Unless and until TSA approves the Owner/Operator's Cybersecurity Implementation Plan, the Owner/Operator must implement the requirements in the Attachment to this Security Directive, as amended by any TSA-approved alternative measures and/or action plan requirements. Any approved alternative measures or action plan requirements remain in force and effect until completed or rescinded by TSA.

**Update:** In July 2023, TSA issued Security Directive Pipeline-2021-02D. The revised Security Directive was issued due to the ongoing cybersecurity threat to pipeline systems, under the authority of 49U.S.C.

114(/)(2)(A). This Security Directive continues to require performance-based regulatory cybersecurity measures first issued by TSA on July 26, 2021 under the Security Directive Pipeline-2021-02 series. In general, this Security Directive is applicable to the same pipeline and liquefied natural gas facilities subject to the requirements of the Security Directive Pipeline-2021-01 series, which fast went into effect on May 28, 2021.

# Cybersecurity Implementation Plan (CIP) Template

**Owner/Operator: ACME Railways, Inc.**
**Business Headquarters: Anytown, USA**
**Contact: J. Smith**
**Contact Email: jsmith@email**
**Contact Phone: 555-555-5555**

A. **ACME Railways, Inc.** list of Critical Cyber Systems as defined in Section VII of this Security Directive include:

1. **List of ACME Railways, Inc. Critical Cyber Systems (CCS)** (*include a detailed list of all systems/devices, software and data that are determined to be CCS and are subject to the requirements of this CIP).*

B. **ACME Railways, Inc.** implements 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 include:

1. A list and description of:

a. Information and Operational Technology system interdependencies;

b. All external connections to the Operational Technology system; and

c. Zone boundaries, including a description of how Information and Operational Technology systems are defined and organized into logical zones based on criticality, consequence, and operational necessity.

2. **ACME Railways, Inc.** identifies and describes measures that include security controls for securing and defending zone boundaries -

a. To prevent unauthorized communications between zones; and

b. To prohibit Operational Technology system services from traversing the Information Technology system, unless the content of the Operational Technology system is encrypted while in transit.

C. **ACME Railways, Inc.** implements access control measures, including for local and remote access, to secure and prevent unauthorized access to Critical Cyber Systems. These measures 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 schedule for memorized secret authenticator resets; and

b. Documented and defined mitigation measures for components of Critical Cyber Systems that will not have passwords reset in accordance with the schedule required by the preceding subparagraph (III.C. l .a.) and a timeframe to complete these mitigations.

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 industrial control workstations in control rooms regulated under 49 CFR Section parts 192 or 195, the Owner/Operator shall specify what compensating controls are used to manage access.*

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.*

4. Enforcement of standards that limit 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.

5. Schedule for review of existing domain trust relationships to ensure their necessity and policies to manage domain trusts.

D. **ACME Railways, Inc.** implements 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 include:

1. Capabilities to-

a. Prevent malicious email, such as spam and phishing emails, from adversely impacting operations;

b. Prohibit 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).

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.

3. Logging policies that-

    a. Require continuous collection and analyzing of data for potential intrusions and anomalous behavior; and

    b. Ensure data is maintained for sufficient periods to allow for effective investigation of cybersecurity incidents.

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.

E. **ACME Railways, Inc.** reduces 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 include-

1. A patch management strategy that ensures all critical security patches and updates on Critical Cyber Systems are current.

2. This strategy required by paragraph III.E. l. 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 CISA'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.