



MEMORANDUM

To: Covered Pipeline Owner/Operators

Date: July 26, 2023

Subject: Renewal with revision to the Security Directive (SD) Pipeline-2021-02 series: *Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing*

Attached to this memorandum is SD Pipeline-2021-02D: *Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing*. SD-Pipeline-2021-02D is a continuation of the SD Pipeline-2021-02 series and cancels and supersedes SD Pipeline-2021-02C.

The SD applies to Owner/Operators of TSA-designated hazardous liquid and natural gas pipelines or liquefied natural gas facilities. All Owner/Operators subject to these requirements have been previously notified by TSA. This revision maintains the requirement for Owner/Operators to enhance cyber resilience through implementation of a TSA-approved Cybersecurity Implementation Plan (CIP). If TSA identifies additional Owner/Operators with critical pipeline systems or facilities who were not previously subject to the SD Pipeline-2021-02 series, TSA will notify these Owner/Operators and provide specific compliance deadlines for the requirements of this SD.

Revisions to the text of the SD are highlighted in **bold**.

The following table summarizes the changes to the SD.

Section II.A.3.
This section includes new language that requires owner/operators without Critical Cyber Systems to reevaluate whether or not they have Critical Cyber Systems in the event that they change their method of operations. If these methods changed the owner/operator must notify TSA and determine a schedule for complying with the SD’s measures to protect those systems.
Section II.B.3.
This is a new section added to clarify that if an Owner/Operator needs to amend their TSA-approved Cybersecurity Implementation Plan (CIP) based on revisions to this Security Directive (SD) they must follow the procedures in Section VI. (Amendments).
Section II.B.4. (Alternative Measures) Removed
This section and the Attachment from SD Pipeline 2021-02C are no longer applicable because TSA approved all critical Owner/Operators' CIPs.
Section III.A.
This section includes new language informing Owner/Operators that, following consultation, TSA may notify an Owner/Operator that they must include additional Critical Cyber Systems identified by TSA that the Owner/Operator has not previously identified in their CIP.



Section III.F.1.e. This section includes new requirements for the Cybersecurity Incident Response Plan (CIRP) exercises, to include the following: (1) Owner/Operators are required to test at least two CIRP objectives (e.g., containment, segregation, security and integrity of back-up data; and isolation of Information Technology/ Operational Technology) no less than annually ; and (2) include employees identified (by position) as active participants in CIRP exercises.
Section III.G. This section replaces "Cybersecurity Assessment Program" with "Cybersecurity Assessment Plan" (CAP), which more accurately reflects the following changes.
This section includes a new requirement that Owner/Operators must continue to submit an annual CAP update not only for TSA review, but also for TSA approval. Subsequent annual CAP updates will also require TSA approval.
This section includes a new requirement for a CAP schedule for assessing and auditing specific cybersecurity measures and/or actions. The schedule must ensure at least 30 percent of the policies, procedures, measures, and capabilities in the TSA-approved CIP are assessed each year so that 100 percent will be assessed every three years.
This section includes a new requirement for an annual CAP Report that must be submitted to TSA for review. The report must include the results of assessments conducted in accordance with the CAP and indicate, which assessment method(s) were used to determine if the policies, procedures, and capabilities described by the Owner/Operator in its CIP are effective.
Section IV.A. This section includes revised language requiring that previously developed plans, assessments, tests, and evaluations used to meet the requirements of this SD and previously listed in an index must now be explicitly incorporated by reference in the CIP and be made available to TSA upon request. This clarification is being added in response to questions raised during TSA's review of pipeline CIPs.
Section V.C. This section includes a new requirement that Owner/Operators must submit documents in a manner prescribed by TSA. The language is being provided to provide flexibility for future capabilities.

Please submit all queries concerning the attached SD to TSA at: TSA-Surface@tsa.dhs.gov.

Stacey Fitzmaurice
Executive Assistant Administrator
Operations Support

Attachment: Security Directive Pipeline-2021-02D



SECURITY DIRECTIVE

<u>NUMBER</u>	Security Directive Pipeline-2021-02D
<u>SUBJECT</u>	Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing
<u>EFFECTIVE DATE</u>	July 27, 2023
<u>EXPIRATION DATE</u>	July 27, 2024
<u>CANCELS AND SUPERSEDES</u>	Security Directive Pipeline-2021-02C
<u>APPLICABILITY</u>	Owners and Operators of a hazardous liquid and natural gas pipeline or a liquefied natural gas facility notified by TSA that their pipeline system or facility is critical
<u>AUTHORITY</u>	49 U.S.C. 114(d), (f), (l) and (m)
<u>LOCATION</u>	All locations within the United States

I. PURPOSE AND GENERAL INFORMATION

The Transportation Security Administration (TSA) is issuing this Security Directive due to the ongoing cybersecurity threat to pipeline systems, under the authority of 49 U.S.C. 114(l)(2)(A).¹ 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.**² 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 first went into effect on May 28, 2021.³ **All revisions to this Security Directive series from the most recent version, SD Pipeline-2021-02C, are highlighted in bold.**

This Security Directive requires actions necessary to protect the national security, economy, and public health and safety of the United States and its citizens from the impact of malicious

¹ This Security Directive series is issued under the authority of 49 U.S.C. 114(l)(2)(A), which states: "Notwithstanding any other provision of law or executive order (including an executive order requiring a cost-benefit analysis), if the Administrator determines that a regulation or security directive must be issued immediately in order to protect transportation security, the Administrator shall issue the regulation or security directive without providing notice or an opportunity for comment and without prior approval of the Secretary."

² As noted in the Office of Management and Budget's Unified Agenda, TSA intends to more permanently codify these requirements through notice-and-comment rulemaking.

³ See Section II.A. for applicability.

cyber intrusions affecting the nation's most critical gas and liquid pipelines. Even minor disruptions in critical pipeline systems may result in temporary product shortages that can cause significant harm to national security. Prolonged disruptions in the flow of commodities could lead to widespread energy shortfalls, with ripple effects across the economy. Disruptions and delays may affect other domestic critical infrastructure and industries that depend on the commodities transported by the nation's pipeline systems.

The goal of this Security Directive is to reduce the risk that cybersecurity threats pose to critical pipeline systems and facilities by implementing layered cybersecurity measures that demonstrate a defense-in-depth approach against such threats. Recent and evolving intelligence emphasizes the growing sophistication of nefarious persons, organizations, and governments, highlights vulnerabilities, and intensifies the urgency of implementing and sustaining the requirements in this Security Directive series.⁴

To protect against the ongoing threat to the United States' national and economic security, this Security Directive mandates that TSA-specified Owners/Operators of pipeline and liquefied natural gas facilities implement the following cybersecurity measures to prevent disruption and degradation to their infrastructure. Specifically, Owner/Operators must do the following:

1. Establish and implement a TSA-approved Cybersecurity Implementation Plan that describes the specific cybersecurity measures employed and the schedule for achieving the outcomes described in Section III.A. through III.E.
2. Develop and maintain an up-to-date Cybersecurity Incident Response Plan to reduce the risk of operational disruption, or the risk of other significant impacts on necessary capacity, as defined in this Security Directive, should the Information and/or Operational Technology systems of a gas or liquid pipeline be affected by a cybersecurity incident. *See* Section III.F.
3. Develop a Cybersecurity Assessment **Plan** and submit **(a) an annual update, for approval**, that describes how the Owner/Operator will proactively and regularly assess the effectiveness of cybersecurity measures and identify and resolve device, network, and/or system vulnerabilities, and **(b) an annual report that provides Cybersecurity Assessment Plan results from the previous year.** *See* Section III.G.

TSA significantly revised the Security Directive Pipeline 2021-02 series, initially issued in July 2021, to provide Owner/Operators with more flexibility to meet the intended security outcomes while ensuring sustainment of the cybersecurity enhancements accomplished through this Security Directive series. Cybersecurity experts from TSA and the Cybersecurity and Infrastructure Security Agency (CISA) contributed to the development of

⁴ *See, e.g.,* Joint Cybersecurity Advisory (AA22-110A), *Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure* (dated April 20, 2022), available at https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf. *See also* additional information regarding current threats posted at <https://www.cisa.gov/shields-up>.

the measures in this Security Directive series to ensure the efficacy of the requirements in mitigating system vulnerabilities.

This revision retains the transition to a more flexible, performance-based approach requiring all Owner/Operators to submit a Cybersecurity Implementation Plan for TSA approval. All currently identified critical Owner/Operators have a TSA-approved Cybersecurity Implementation Plan in place. This plan sets the security measures and requirements against which TSA inspects for compliance.⁵ See Section II.B. Pursuant to 49 U.S.C. 114(f), the TSA Administrator is authorized to “enforce security-related regulations and requirements”; “inspect, maintain, and test security facilities, equipment, and systems”; and “oversee the implementation, and ensure the adequacy of security measures at ... transportation facilities.” Given this authority, TSA may require Owner/Operators to provide specific documentation and access to TSA as necessary to establish compliance. See Section IV of this Security Directive for examples of the type of records to which TSA may require access.

Although TSA has determined that this document is not sensitive security information, all information that must be reported or submitted to TSA pursuant to this Security Directive is sensitive security information subject to the protections of part 1520 of title 49, Code of Federal Regulations (CFR). DHS may use the information, with company-specific data redacted, for DHS’s intelligence-derived reports. DHS also may use information submitted for vulnerability identification, trend analysis, or to generate anonymized indicators of compromise or other cybersecurity products to prevent other cybersecurity incidents.⁶ Information provided to DHS pursuant to this Security Directive may also be shared with other agencies as appropriate.⁷ The distribution, disclosure, and availability of information will be restricted to persons with a need to know, and safeguarding, protecting, and marking methods for sensitive/critical information will be utilized.⁸ The Office of Management and Budget **has approved this collection under OMB Control No. 1652-0056**

TSA will seek review and ratification of this Security Directive by the Transportation Security Oversight Board (TSOB). The TSOB is statutorily required to “review and ratify or disapprove” emergency regulations and security directives issued by TSA under 49 U.S.C. 114(d)(2). See 49 U.S.C. 114(d)(2)(B) and 115(c)(1). If, for whatever reason, the TSOB fails to ratify any section or subsection of this Security Directive, or deems any section or subsection inapplicable, the remainder of this Security Directive shall not be affected, provided the remaining sections do not rely on the stricken provision for effect.

⁵ See also 49 U.S.C. 114(f); 49 CFR part 1503.

⁶ See OMB Control No. 1652-0056.

⁷ Presidential Policy Directive (PPD) 41 requires Federal agencies to rapidly share incident information with each other to achieve unity of governmental effort. See PPD-41 § III.D (“Whichever Federal agency first becomes aware of a cyber incident will rapidly notify other relevant Federal agencies in order to facilitate a unified Federal response and ensure that the right combination of agencies responds to a particular incident”). Furthermore, for purposes of information shared with DHS pursuant to this directive, cyber incident responders with responsibilities under PPD-41 are “covered” persons with a “need to know,” as provided by 49 CFR 1520.7 and 1520.11, respectively.

⁸ See 49 CFR 1520.5(b)(5) and <https://www.tsa.gov/for-industry/sensitive-security-information>.

II. ACTIONS REQUIRED

A. Applicability, Deadlines for Compliance, and Scope

1. *Covered Pipeline Owner/Operators:* This Security Directive applies to Owner/Operators of TSA-designated critical pipeline systems or facilities notified before July 26, 2022, that they are required to comply with the Security Directive Pipeline-2021-02 series.⁹
2. *Additional Critical Pipeline Systems or Facilities:* If TSA identifies additional Owner/Operators with critical pipeline systems or facilities who were not already subject to the Security Directive Pipeline-2021-02 series, TSA will notify the Owner/Operator and provide specific compliance deadlines for the requirements in this Security Directive.
3. *Scope:* The requirements in this Security Directive apply to the covered Owner/Operators' Critical Cyber Systems.

Note: If an Owner/Operator determines they have no Critical Cyber Systems, as defined in Section VII., they must notify TSA in writing within 60 days of the effective date of this Security Directive. TSA will notify the Owner/Operator if the agency disagrees with the Owner/Operator's determination and may require the Owner/Operator to provide additional information regarding the methodologies or rationale used to identify Critical Cyber Systems. In the event that an Owner/Operator who does not have Critical Cyber Systems changes their method of operations, they must reevaluate whether they have a Critical Cyber System, and if so, notify TSA within 60 days of the change in operations to determine the schedule for complying with the requirements of this Security Directive.

B. Cybersecurity Implementation Plan

1. 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.
2. Once approved by TSA, the Owner/Operator must implement and maintain all measures in the TSA-approved Cybersecurity Implementation Plan and meet any schedule stipulated in the plan.

⁹ See § 1557(b) of the *Implementing Recommendations of the 9/11 Commission Act of 2007*, (Pub. L. 110-53; 121 Stat. 266; Aug. 3, 2007) (9/11 Act) (codified at 6 U.S.C. 1207(b) (requiring TSA to review pipeline security plans and inspect critical facilities of the 100 most critical pipeline operators). Applicability for this Security Directive is the same as the Security Directive Pipeline-2021-01 series and the Security Directive Pipeline-2021-02 series.

3. **If an Owner/Operator needs to amend their TSA-approved Cybersecurity Implementation Plan based on revisions to this Security Directive (highlighted in bold), they must follow the procedures in Section VI.**

III. CYBERSECURITY MEASURES

The Owner/Operator must:

- A. Identify the Owner/Operator's Critical Cyber Systems as defined in Section VII. of this Security Directive. **TSA will notify the Owner/Operator if the agency disagrees with the Owner/Operator's determination and may require the Owner/Operator to provide additional information regarding the methodologies or rationale used to identify Critical Cyber Systems. After consultation with Owner/Operators, TSA may notify an Owner/Operator that it must include additional Critical Cyber Systems identified by TSA not previously identified by the Owner/Operator in their Cybersecurity Implementation Plan.**
- 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 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. 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, unless the content of the Operational Technology system is encrypted while in transit.
- 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 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.1.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 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. 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. 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. 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. This 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 CISA's Known Exploited Vulnerabilities Catalog.¹⁰
 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.
- F. Develop and maintain a Cybersecurity Incident Response Plan.
 1. Owner/Operators must have an up-to-date Cybersecurity Incident Response Plan for the Critical Cyber Systems that include measures to reduce the risk of operational disruption, or the risk of other significant impacts on necessary capacity, should their pipeline or facility experience a cybersecurity incident. The Cybersecurity Incident Response Plan must provide specific measures sufficient to ensure the following objectives, as applicable:
 - a. Prompt containment of the infected server or device.
 - b. Segregation of the infected network (or devices) to ensure malicious code does not spread by, as necessary —
 - i. Segregating (removing from the network) the infected device(s);
 - ii. Segregating any other devices that shared a network with the infected device(s);
 - iii. Preserving volatile memory by collecting a forensic memory image of affected device(s) before powering off or moving; and
 - iv. Isolating and securing all infected and potentially infected devices, making sure to clearly label any equipment that has been affected by malicious code.
 - c. Security and integrity of backed-up data, including measures to secure backups, store backup data separate from the system, and procedures to ensure that the backup data is free of known malicious code when the backup is made and when tested for restoral.
 - d. Established capability and governance for isolating the Information and Operational Technology systems in the event of a cybersecurity incident that results or could result in operational disruption.

¹⁰ Available at: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>.

- e. Exercises to test the effectiveness of procedures, and personnel responsible for implementing measures, in this Cybersecurity Incident Response Plan, no less than annually. **These exercises must—**
 - i. **Test at least two objectives of the Owner/Operator’s Cybersecurity Incident Response Plan required by subparagraphs F.1.a. through F.1.d. of this section, no less than annually; and**
 - ii. **Include the employees identified (by position) in paragraph F.2 of this section as active participants in the exercises.**
 - 2. The Cybersecurity Incident Response Plan must identify who (by position) is responsible for implementing the specific measures in the Incident Response Plan and any necessary resources needed to implement the measures.
- G. Develop a Cybersecurity Assessment **Plan** for proactively assessing and auditing cybersecurity measures.
- 1. The Owner/Operator must develop a Cybersecurity Assessment **Plan** for proactively assessing Critical Cyber Systems to ascertain the effectiveness of cybersecurity measures and to identify and resolve device, network, and/or system vulnerabilities.
 - 2. The Cybersecurity Assessment **Plan** required by Section III.G.1. must –
 - a. Assess the effectiveness of the Owner/Operator’s TSA-approved Cybersecurity Implementation Plan;
 - b. Include a **cybersecurity** architecture design review at least once every two years that includes verification and validation of network traffic and system log review and analysis to identify cybersecurity vulnerabilities related to network design, configuration, and inter-connectivity to internal and external systems;
 - c. Incorporate other assessment capabilities, such as penetration testing of Information Technology systems and the use of “red” and “purple” team (adversarial perspective) testing;
 - d. **Include a schedule for assessing and auditing specific cybersecurity measures and/or actions required by subparagraphs G.2.a. through G.2.c of this section. The schedule must ensure at least 30 percent of the policies, procedures, measures, and capabilities in the TSA-approved Cybersecurity Implementation Plan are assessed each year, with 100 percent assessed over any three-year period; and**
 - e. **Ensure a Cybersecurity Assessment Plan annual report of the results of assessments conducted in accordance with the Cybersecurity Assessment Plan is submitted to TSA as described in paragraph G.4. of this section. The required report must indicate—**

- i. Which assessment method(s) were used to determine whether the policies, procedures, and capabilities described by the Owner/Operator in its Cybersecurity Implementation Plan are effective; and
 - ii. Results of the individual assessments conducted.
3. The Owner/Operator must review and update their Cybersecurity Assessment Plan on an annual basis and submit it to TSA for approval no later than 12 months from the date of the previous Cybersecurity Assessment Plan submission or TSA's approval of the previous plan.
4. The Cybersecurity Assessment Plan report required by subparagraph G.2.e. of this section must be submitted on an annual basis to TSA no later than 12 months from the date of the previous Cybersecurity Assessment Plan submission or TSA's approval of the previous plan. The annual report covers assessments conducted in the previous 12 months.

IV. RECORDS

- A. *Use of previous plans, assessments, tests, and evaluations.* As applicable, Owner/Operators may use previously developed plans, assessments, tests, and evaluations to meet the requirements of this Security Directive. If the Owner/Operator relies on these materials, they must include an index of the records and their location organized in the same sequence as the requirements in this Security Directive. **In addition, these materials must be explicitly incorporated by reference into the Cybersecurity Implementation Plan and made available to TSA upon request.**
- B. *Protection of sensitive security information.* The Owner/Operator must, at a minimum, store and transmit the following information required by this Security Directive consistent with the requirements in 49 CFR part 1520:¹¹
 1. Plans and reports; and
 2. Audit, testing, or assessment results.
- C. *Documentation to Establish Compliance*
 1. The Owner/Operator must make records necessary to establish compliance with the requirements of this Security Directive available to TSA upon request for inspection and/or copying.
 2. TSA may request to inspect or copy the following documents to establish compliance with this Security Directive:

¹¹ Owner/Operators may contact SSI@tsa.dhs.gov for more information on how to comply with requirements for the protection of Sensitive Security Information.

- a. Hardware/software asset inventory, including supervisory control, and data acquisition systems.
- b. Firewall rules.
- c. Network diagrams, switch and router configurations, architecture diagrams, publicly routable internet protocol addresses, and Virtual Local Area Networks.
- d. Policy, procedural, and other documents that informed the development, and documented implementation of, the Owner/Operator's Cybersecurity Implementation Plan, Cybersecurity Incident Response Plan, Cybersecurity Assessment Plan, and assessment or audit results.
- e. Data providing a "snapshot" of activity on and between Information and Operational Technology systems, such as—
 - i. Log files;
 - ii. A capture of network traffic (i.e., packet capture (PCAPs)), not to exceed a period of twenty-four hours, as identified and directed by TSA;
 - iii. "East-West Traffic" of Operational Technology systems/sites/environments within the scope of this Security Directive's requirements; and
 - iv. "North-South Traffic" between Information and Operational Technology systems, and the perimeter boundaries between them.
- f. Any other records or documents necessary to establish compliance with this Security Directive.

V. PROCEDURES FOR SECURITY DIRECTIVES

A. General Procedures

1. *Confirm Receipt.* Immediately provide written confirmation of receipt of this Security Directive via e-mail to TSA at SurfOps-SD@tsa.dhs.gov;
 2. *Dissemination.* Immediately disseminate the information and measures in this Security Directive to corporate senior management and security management representatives. The Owner/Operator must provide the applicable security measures in this Security Directive to the Owner/Operator's direct employees and authorized representatives responsible for implementing applicable security measures as necessary to ensure compliance.
- B. *Comments.* Owner/Operators may comment on this Security Directive by submitting data, views, or arguments in writing to TSA via e-mail at TSA-Surface@tsa.dhs.gov. Any comments referring to specific measures in this Security Directive must be protected in accordance with the requirements in 49 CFR part 1520. TSA may amend the Security

Directive based on comments received. Submission of a comment does not delay the effective date of the Security Directive or requirement to comply with the provisions of the Security Directive.

- C. *Submission of Documentation to TSA: Owner/Operators are required to submit documents in a manner prescribed by TSA. TSA will provide Owner/Operators specific instructions for submission of required documents.***

VI. AMENDMENTS TO CYBERSECURITY IMPLEMENTATION PLAN

- A. *Changes to ownership or control of operations.* An Owner/Operator required to submit a Cybersecurity Implementation Plan under Section II.B. of this Security Directive must submit a request to amend its Cybersecurity Implementation Plan if, after approval, there are any changes to the ownership or control of the operation.
- B. *Changes to conditions affecting security.* An Owner/Operator required to submit a Cybersecurity Implementation Plan under Section II.B. of this Security Directive must submit a request to amend its Cybersecurity Implementation Plan if, after approval, the Owner/Operator makes, or intends to make, permanent changes to the policies, procedures, or measures approved by TSA, including, but not limited to, changes to address:
1. Determinations that a specific policy, procedure, or measure in the Cybersecurity Implementation Plan is ineffective based on results of the audits and assessments required under Section III.G. of this Security Directive; or
 2. The Owner/Operator has identified or obtained new or additional capabilities for meeting the requirements in the Security Directive that have not been previously approved by TSA.
- C. *Permanent change.* For purposes of this section, a “permanent change” is one intended to be in effect for 45 or more calendar days.
- D. *Schedule for requesting amendment.* The Owner/Operator must file the request for an amendment to its Cybersecurity Implementation Plan with TSA no later than 50 calendar days after the permanent change takes effect, unless TSA allows a longer time period.
- E. *TSA approval.*
1. TSA may approve a requested amendment to a Cybersecurity Implementation Plan if TSA determines that it is in the interest of the public and transportation security and the proposed amendment provides the level of security required under this Security Directive.
 2. TSA may request additional information from the Owner/Operator before rendering a decision.

- F. *Petition for reconsideration*. No later than 30 calendar days after receiving a denial of an amendment to a Cybersecurity Implementation Plan, the Owner/Operator may file a petition for reconsideration following the procedures in 49 CFR 1570.119.

VII. DEFINITIONS


In addition to the terms defined in 49 CFR 1500.3, the following terms apply to this Security Directive:

- A. *Critical Cyber System* means any Information or Operational Technology system or data that, if compromised or exploited, could result in operational disruption. Critical Cyber Systems include business services that, if compromised or exploited, could result in operational disruption.
- B. *Cybersecurity architecture design review* means a technical assessment based on government and industry-recognized standards, guidelines, and best practices that evaluates systems, networks, and security services to determine if they are designed, built, and operated in a reliable and resilient manner. These reviews must be designed to be applicable to the Owner/Operator's Information and Operational Technology systems.
- C. *Cybersecurity incident* means an event that, without lawful authority, jeopardizes, disrupts or otherwise impacts, or is reasonably likely to jeopardize, disrupt or otherwise impact, the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident on the system. This definition includes an event that is under investigation or evaluation by the Owner/Operator as a possible cybersecurity incident without final determination of the event's root cause or nature (such as malicious, suspicious, benign).
- D. *Days* means calendar days unless otherwise indicated. As used for compliance deadlines, if a requirement must be met on a date that is a national holiday, the compliance deadline will be the next federal business day after the holiday.
- E. *Demilitarized Zone (DMZ) or perimeter network*, means a network area (a subnetwork) that sits between an internal network and an external network. The security demilitarized zone is used for providing external controlled access to services used by external personnel to the control system network to ensure secure application of system updates and upgrades. For someone on the external network who does not have authorization to connect to the internal network, the demilitarized zone is a dead end.
- F. *East-West Traffic* means, in a networking context, the lateral movement of network traffic within a trust zone or local area network.
- G. *Information Technology System* means any services, equipment, or interconnected systems or subsystems of equipment that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching,

interchange, transmission, or reception of data or information that fall within the responsibility of the Owner/Operator to operate and/or maintain.

- H. *Interdependencies* means relationships of reliance within and among Information and Operational Technology systems that must be maintained for those systems to operate and provide services.
- I. *Memorized secret authenticator* means a type of authenticator comprised of a character string intended to be memorized by, or memorable to, the subscriber, permitting the subscriber to demonstrate something they know as part of an authentication process.
- J. *Necessary capacity* means the Owner/Operator's determination of capacity to support its business-critical functions required for pipeline operations and market expectations.
- K. *North-South Traffic* means network traffic that moves through a perimeter boundary into another trust level.
- L. *Operational disruption*, for purposes of this Security Directive, means a deviation from or interruption of necessary capacity that results from a compromise or loss of data, system availability, system reliability, or control of a TSA-designated critical pipeline system or facility.
- M. *Operational Technology System* is a general term that encompasses several types of control systems, including industrial control systems, supervisory control and data acquisition systems, distributed control systems, and other control system configurations, such as programmable logic controllers, fire control systems, and physical access control systems, often found in the industrial sector and critical infrastructure. Such systems consist of combinations of programmable electrical, mechanical, hydraulic, pneumatic devices or systems that interact with the physical environment or manage devices that interact with the physical environment.
- N. *Owner/Operator* means a person who owns or maintains operational control over pipeline facilities or engages in the transportation of hazardous liquids or natural gases and who has been identified by TSA as one of the most critical interstate and intrastate natural gas and hazardous liquid transmission pipeline infrastructure and operations.
- O. *Phishing* means tricking individuals into disclosing sensitive personal information through deceptive computer-based means (such as internet web sites or e-mails using social engineering or counterfeit identifying information).
- P. *Security, Orchestration, Automation, and Response* means capabilities that enable Owner/Operators to collect inputs monitored by the security operations team. For example, alerts from the security information and event management system and other security technologies – where incident analysis and triage can be performed by leveraging a combination of human and machine power – help define, prioritize and drive standardized incident response activities. These capabilities allow an Owner/Operator to define incident analysis and response procedures in a digital workflow format.

- Q. *Shared Account* means an account that is used by multiple users with a common authenticator to access systems or data. A shared account is distinct from a group account, which is a collection of user accounts that allows administrators to group similar user accounts together in order to grant them the same rights and permissions. Group accounts do not have common authenticators.
- R. *Spam* means electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.
- S. *Tor*, also known as *The Onion Router*, means software that allows users to browse the web anonymously by encrypting and routing requests through multiple relay layers or nodes. Tor software obfuscates a user's identity from anyone seeking to monitor online activity (such as nation states, surveillance organizations, information security tools). This deception is possible because the online activity of someone using Tor software appears to originate from the Internet Protocol address of a Tor exit node, as opposed to the address of the user's computer.
- T. *Trust relationship* means an agreed-upon relationship between two or more system elements that is governed by criteria for secure interaction, behavior, and outcomes relative to the protection of assets. This term refers to trust relationships between system elements implemented by hardware, firmware, and software.
- U. *Unauthorized Access of an Information Technology or Operational Technology System* means access from an unknown source, access by a third party or former employee; an employee accessing systems for which he or she is not authorized; and may include a non-malicious Owner/Operator's policy violation such as the use of shared credential by an employee otherwise authorized to access it.



Stacey Fitzmaurice
Executive Assistant Administrator
Operations Support