U.S. Department of Homeland Security
**Transportation Security Administration**
6595 Springfield Center Drive
Springfield, Virginia 20598

# MEMORANDUM

To: Covered Pipeline Owner/Operators

Date: July 21, 2022

Subject: Revision to the Security Directive Pipeline-2021-02 series: *Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing*

Attached to this memorandum is Security Directive Pipeline-2021-02C (SD02C). SD02C is a continuation of the SD-02 series, and supersedes and replaces SD Pipeline-2021-02B.

SD02C is effective on July 27, 2022, and applies to Owner/Operators of hazardous liquid and natural gas pipelines or a liquefied natural gas facility notified by TSA that their pipeline system or facility is critical.

SD02C includes requirements for covered Owner/Operators to 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 Owner/Operator will assess the effectiveness of cybersecurity measures.

Owner/Operators must continue to implement the specific measures from Security Directive Pipeline 2021-02B, as identified in the Attachment to SD02C, and modified by any TSA-approved alternative measures and/or action plans, until a Cybersecurity Implementation Plan issued pursuant to this Directive is approved by TSA.

Although TSA has not designated this SD as Sensitive Security Information (SSI), the information submitted by the Owner/Operator to TSA as a result of these requirements is protected as SSI per 49 CFR parts 15 and 1520.

All queries concerning the attached SD should be submitted to TSA at TSA-Surface@tsa.dhs.gov.

David P. Pekoske
Administrator

Attachments:

Security Directive Pipeline-2021-02C

U.S. Department of Homeland Security
**Transportation Security Administration**
6595 Springfield Center Drive
Springfield, Virginia 20598

| | |
|---|---|
| NUMBER | Security Directive Pipeline-2021-02C |
| SUBJECT | Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing |
| EFFECTIVE DATE | July 27, 2022 |
| EXPIRATION DATE | July 27, 2023 |
| CANCELS AND SUPERSEDES | Security Directive Pipeline-2021-02B |
| APPLICABILITY | 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 |
| AUTHORITY | 49 U.S.C. 114(d), (f), (*l*) and (m) |
| LOCATION | 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, under a new performance-based regulatory model, mandatory cybersecurity measures first implemented by TSA in July 2021, as part of what is known as the Security Directive Pipeline-2021-02 series, which first went into effect on July 26, 2021. 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.[2]

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 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

[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] *See* Section II.A. for applicability.

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.[3]

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. Establish a Cybersecurity Assessment Program and submit an annual plan 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. *See* Section III.G.

TSA has significantly revised the Security Directive 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 the measures in this Security Directive series to ensure the efficacy of the requirements in mitigating system vulnerabilities. This revision also reflects industry feedback along with both industry and general congressional support for TSA's transition to this performance-based, security outcome model. In addition, the directive incorporates knowledge gained from TSA's

[3] *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*.

processing and consideration of alternative measure[4] requests submitted by pipeline Owner/Operators in response to the Security Directive Pipeline-2021-02 series.

The transition to a more flexible, performance-based approach requires all Owner/Operators to submit a Cybersecurity Implementation Plan for TSA approval. This plan, once approved by TSA, will set the security measures and requirements against which TSA will inspect for compliance.[5] *See* Section II.B. TSA may also require Owner/Operators to provide specific documentation and access to TSA as necessary to establish compliance. *See* Section IV for examples of the type of records to which TSA may require access.

To ensure ongoing cybersecurity, Owner/Operators must continue to implement the specific measures from Security Directive Pipeline-2021-02B, as identified in the Attachment, and modified by any TSA-approved alternative measures and/or action plans,[6] until a Cybersecurity Implementation Plan issued pursuant to this Directive is approved by TSA.

The Attachment is annotated to identify how the prescriptive requirements in Security Directive Pipeline-2021-02B align with the performance-based requirements in this Security Directive. This annotation supports Owner/Operators who choose to use the actions they have already taken in compliance with this Security Directive series to incorporate these actions into their Cybersecurity Implementation Plan.

Finally, TSA recognizes that, in response to this performance-based revision to the Security Directive, Owner/Operators may incorporate measures or a schedule for implementation into their proposed Cybersecurity Implementation Plan that is different than those in their previously issued action plans. As Owner/Operators work with TSA to obtain approval of Cybersecurity Implementation Plans, TSA will also work with the Owner/Operator on appropriate modifications to any previously issued action plans.

While 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.[7] Information provided to DHS pursuant to this Security Directive may also be shared with

---

[4] The previous versions of this Security Directives series provided procedures for Owner/Operators to request alternative measures to the prescriptive requirements in the directive. TSA could grant these requests if the proposed alternative measures provided a commensurate level of security to the requirements in the directive.

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

[6] Action plans reflect an agreement between TSA and Owner/Operators on corrective actions to resolve security vulnerabilities before they become noncompliant and/or noncompliant with a specific requirement. The process allows Owner/Operators to either avoid penalties by addressing the issue before it becomes an instance of noncompliance or offset potential civil penalties with investment.

[7] *See* OMB Control No. 1652-0056.

other agencies as appropriate.[8] 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.[9] As required, TSA sought approval from the Office of Management and Budget for a revision to OMB Control No. 1652-0056 for the collection of information under this Security Directive.

TSA is issuing this Security Directive in consultation with the CISA, the United States Coast Guard, the Department of Energy (including the Federal Energy Regulatory Commission), and the Department of Transportation (including the Pipeline and Hazardous Materials Safety Administration). 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(*l*)(2). *See* 49 U.S.C. 114(*l*)(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.

## 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.[10]

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.

---

[8] 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.

[9] *See* 49 CFR 1520.5(b)(5) and *https://www.tsa.gov/for-industry/sensitive-security-information.*

[10] *See* § 1557(b) of the *Implementing Recommendations of the 9/11 Commission Act* 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 Security Directive Pipeline-2021-02 Series.

B. Cybersecurity Implementation Plan

1. No later than 90 days after the effective date of this Security Directive, Owner/Operators must submit a Cybersecurity Implementation Plan to SurfOps-SD@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.

## 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.

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 paragraph 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.[11]

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 System that includes 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

[11] Available at: *https://www.cisa.gov/known-exploited-vulnerabilities-catalog.*

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.

e. Exercises to test the effectiveness of procedures, and personnel responsible for implementing measures, in this Cybersecurity Incident Response Plan, no less than annually.

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 Program for proactively assessing and auditing cybersecurity measures.

1. The Owner/Operator must develop a Cybersecurity Assessment Program 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 Program required by Section III.G.1. must—

a. Assess the effectiveness of the Owner/Operator's TSA-approved Cybersecurity Implementation Plan;

b. Include an architectural 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; and

c. Incorporate other assessment capabilities, such as penetration testing of Information Technology systems and the use of "red" and "purple" team (adversarial perspective) testing.

3. No later than 60 days after TSA's approval of the Owner/Operator's Cybersecurity Implementation Plan, the Owner/Operator must submit the annual plan for their Cybersecurity Assessment Program to SurfOps-SD@tsa.dhs.gov. This plan must describe the Cybersecurity Assessment Program required by Section III.G.1., including the schedule for specific actions. The Owner/Operator must update this plan on an annual basis and submit it no later than one year from the date of the previous plan's submission.

## 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.

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[12]:

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:

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 Program, 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;

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

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.

## 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. *Application allowlisting* means a security capability that reduces harmful security attacks by allowing only trusted files, applications, and processes to be run.

B. *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.

C. *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.

D. *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).

E. *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.

F. *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.

G. *East-West Traffic* means, in a networking context, the lateral movement of network traffic within a trust zone or local area network.

H. *Group policy* means a centralized place for administrators to manage and configure operating systems, applications, and users' settings that can be used to increase the security of users' computers and help defend against both insider threats and external attacks.

I. *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 maintain.

J. *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.

K. *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.

L. *Necessary capacity* means the Owner/Operator's determination of capacity to support its business-critical functions required for pipeline operations and market expectations.

M. *North-South Traffic* means network traffic that moves through a perimeter boundary into another trust level.

N. *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.

O. *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.

P. *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.

Q. *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).

R. *Post-exploitation tool* means a capability used after a cybersecurity incident to determine the sensitivity or value of data stored on a machine and the extent to which the machine can be used to further compromise the network.

S. *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.

T. *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.

U. *Service accounts* means accounts used by system services, such as web servers, mail transport agents, databases, etc. Service accounts are generally created to provide a security context for services running on the operating system without a real user.

V. *Software Restriction Policies* means a Group Policy-based feature that identifies software programs running on computers in a domain and control the ability of those programs to run.

W. *Spam* means electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

X. *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.

Y. *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.

Z. *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. It may include a non-malicious Owner/Operator policy violation such as the use of shared credential by an employee otherwise authorized to access it.

David P. Pekoske
Administrator

## ATTACHMENT

*This attachment has been annotated to identify corresponding sections between Pipeline SD 2021-02B and Pipeline SD 2021-02C (SD2C).*

A. Until the Owner/Operator's Cybersecurity Implementation Plan required by Section II.B. of this Security Directive is approved by TSA, the Owner/Operator must apply the following cybersecurity measures, as modified by any TSA-approved alternative measures, and/or action plans, previously issued to the requirements in the Security Directive Pipeline-2021-02 series.

B. The following requirements must be applied to any Information and/or Operational Technology system connected to a critical pipeline system or facility identified by TSA.

1. In a manner compliant with the most current versions of the National Institute of Standards and Technology (NIST) Digital Identity Guidelines,[13] the Owner/Operator must:

*See* § III.C.1. of SD2C.

   a. Implement and complete a mandatory password reset of all passwords within Information Technology systems (such as corporate remote access, and Virtual Private Networks).

   b. Implement and complete a mandatory password reset(s) of all equipment within Operational Technology systems, to include Programmable Logic Controllers. The Owner/Operator must continue to comply with any TSA-approved alternative measures previously approved for systems where implementing a mandatory password reset is not technically feasible.

   c. For equipment within Information and Operational Technology systems that do not permit password resets, update or develop a plan that identifies the equipment and provides a timeline for replacing the designated equipment. This plan must be approved by TSA.

   d. Require supervisors of individuals with elevated privilege accounts/permission[14] to verbally confirm and document with users of all such accounts their account ownership and continued

*See* § III.C.3 of SD2C.

[13] These actions must be consistent with industry standards, such as those in NIST Special Publication 800-63, Digital Identity Guidelines (available at *https://pages.nist.gov/800-63-3/*) and CISA's Emergency Directive 21-01 (December 13, 2020) (available at *https://cyber.dhs.gov/ed/21-01/*).

[14] *See* National Security Agency's Cybersecurity Information Bulletin: Defend Privileges and Accounts (defense.gov), PP-19-1039 (August 2019) for information on privileges, available at: *https://media.defense.gov/2019/Sep/09/2002180330/-1/-1/0/DEFEND%20PRIVILEGES%20AND%20ACCOUNTS.PDF#:~:text=NSA%20%7C%20Defend%20Privileges%20and%20Accounts%20Traditionally%2C%20administrative,user%20accounts%20may%20have%20access%20to%20valuable%20data.*

need for access to Information and Operational Technology systems.

e. Implement a schedule for verification of continued need at least every 90 days after the verbal confirmation required by B.1.d., and maintain documentation establishing the date of last verification.

2. Continue to apply and/or implement the following additional cybersecurity measures to Information and Operational Technology systems.

a. Apply Multi-factor authentication for non-service accounts accessing Information and Operational Technology systems in a manner compliant with the most current version of NIST Special Publication 800-63B, Digital Identify Guidelines, Authentication and Lifecycle Management standards for use of multifactor cryptographic device authenticators.[15] — *See* § III.C.2. of SD2C.

b. Implement network segmentation sufficient to ensure the Operational Technology system can operate at necessary capacity even if the Information Technology system is compromised by, at a minimum— — *See* § III.B. of SD2C.

i. Identifying Information and Operational Technology network inter-dependencies; — *See* § III.B.1.a. of SD2C.

ii. Implementing and maintaining capability for network physical and logical segmentation between Information and the Operational Technology systems sufficient to ensure the Operational Technology system can continue to operate even if the Information Technology system is taken offline because it has been compromised; — *See* § III.D.4. of SD2C.

iii. Defining a demilitarized zone and using firewall rules, physical separation, and other tools to eliminate unrestricted communication between the Information and Operational Technology systems; — *See* § III.B.2.a. of SD2C.

iv. Organizing Operational Technology system assets into logical zones, such as isolating unrelated sub-processes, by taking into account criticality, consequence, and operational necessity; — *See* § III.B.1.c. of SD2C.

v. Monitoring and filtering traffic between networks of different trust levels, for example, between the Information and — *See* § III.B.2.a. of SD2C.

[15] As stated in NIST Special Publication 800-63B, multifactor cryptographic device authenticators or validators must not leverage Short Message Service. *See supra* n. 1313, at section 5.1,

| | |
|---|---|
| Operational Technology systems, by defining appropriate communication conduits between the logical zones and deploying security controls to monitor and filter network traffic and communications between logical zones; | |
| vi. Prohibiting Operational Technology system protocols from traversing the Information Technology system unless expressly through an encrypted point-to-point tunnel; and | *See* § III.B.2.b. of SD2C. |
| vii. Developing workarounds or manual controls to ensure industrial control system networks can be physically isolated when the Information Technology system creates risk to the safe and reliable Operational Technology system processes. | *See* § III.D.4. of SD2C. |
| c. Review and update (or develop, if necessary) log retention policies to ensure that they include policies and procedures consistent with NIST standards[16] for— | *See* § III.D.3 of SD2C. |
| i. Log management; | |
| ii. Secure log management infrastructure; and | |
| iii. How long log data must be maintained. | |
| d. Employ filters sufficient to— | *See* § III.D1. of SD22C. |
| i. Identify malicious email traffic, spam and phishing emails and inhibit them from reaching end users; | *See* § III.D.1.a. of SD2C. |
| ii. Prohibit ingress and egress of communications with known malicious Internet Protocol addresses for Information Technology systems and all Operational Technology systems with external connectivity; | *See* § III.D.1.b. of SD2C. |
| iii. Prevent users and devices from accessing malicious websites by implementing Uniform Resource Locator block lists and/or allowlists; | *See* §§ III.D.1.a. and III.D.2.a. of SD2C. |
| iv. Control access from the Operational Technology system to external internet access using an allowlist; and | |
| v. Investigate any communication between the Operational Technology system and an outside system that deviates from | *See* § III.D.2.b. of SD2C. |

[16] *See* NIST Special Publication 800-92, Guide to Computer Security Log Management (available at *https://csrc.nist.gov/publications/detail/sp/800-92/final*).

the identified baseline of communications and ensure it is necessary for operations.

e. Set antivirus/anti-malware programs to conduct weekly scans, with on-access and on-demand scans, of Information and Operational Technology systems and other network assets using current signatures.

*See* § III.D.1. of SD2C.

f. Establish passive Domain Name System capabilities that are consistent with currently recognized standards[17] and, at a minimum, include the following actions:

*See* §§ III.D.1.c. and III.D.2.a. of SD2C.

i. Implement software analytics that allow Owner/Operators to rapidly determine which host sourced each Domain Name System-query.

ii. Maintain a current list of domains that are frequently visited or searched for by legitimate users within their systems that are not already included in commercially available top one million domain lists; and

iii. Develop and/or update policies and procedures requiring investigation of the reputation of the domains that are only rarely queried for and/or accessed by legitimate users within their organization, to determine if the communication with these domains carries an inappropriate level of risk to the organization.

g. Ensure, with respect to all security software updates and patches—

*See* § III.E. of SD2C.

i. For operating systems, applications, drivers, and firmware on Information Technology systems:

a) For patches and updates that are listed on CISA's Known Exploited Vulnerabilities Catalog (*https://www.cisa.gov/known-exploited-vulnerabilities-catalog*) and have a NIST Base Score of "Critical" (under the Common Vulnerability Scoring System), the patch/update must be installed within 15 days of its availability.

[17] *See* Passive DNS-Common Output Format, available at *https://datatracker.ietf.org/doc/html/draft-dulaunoy-dnsop-passive-dns-cof.*

b) If the Owner/Operator is unable to install the patch/update for a "Critical" vulnerability within 15 days, it must do the following:

1. Include it on a cumulative list that includes operational and other risk-based considerations to justify not meeting the 15-day deadline, and

2. Install the patch/update within 30 days of its listing on the Known Exploited Vulnerabilities Catalog.

c) All other updates and patches must be installed within 30 days of availability.

ii. For operating systems, applications, drivers, and firmware on Operational Technology systems, software updates and patches must be tested within 35 days of update patch availability and implemented within 35 days of testing validation. Patches not implemented must be included on a cumulative list that includes operational and other risk-based considerations justifying the determination not to apply the patch.

*See* § III.E.3. of SD2C.

h. Implement a "zero trust" policy that provides layers of defense to prevent unauthorized execution by taking the following actions, as applicable, to the Owner/Operator's Information and Operational Technology systems:

i. If using Microsoft Office, fully disable macro use and user-based approval across the organization for Microsoft Office products (such as Word, Excel) using Group Policy. Macros determined necessary for business functionality may be enabled on a case-by-case basis only after implementing additional host-based security controls and network monitoring;

*See* §§ III.D.1.d. and III.D.2.c. of SD2C.

ii. Apply application allowlisting to Information and Operational Technology systems and then implement software restriction policies, or other controls providing the same security benefits, to prevent unauthorized programs from executing;

*See* § III.D.2.a. of SD2C.

iii. If not already incorporated into system-change management, update application allowlisting no less frequently than quarterly to remove applications no longer in use;

iv. Monitor and/or block connections from known malicious command and control servers (such as Tor exit nodes, and other anonymization services) to Internet Protocol addresses

*See* § III.D.1.e. of SD2C.

and ports for which external connections are not expected (such as ports other than virtual private network gateways, mail ports, or web ports);

v. Implement Security, Orchestration, Automation, and Response, as applicable. If the Owner/Operator determines these capabilities are not applicable, they must document which aspects of the system do not apply the capability and their justification for excluding these operations; and — *See* § III.D.2.d. of SD2C.

vi. Require implementation of signatures to detect and/or block connection from post-exploitation tools. — *See* § III.D.1.e. of SD2C.

i. Organize access rights based on the principles of least privilege and separation of duties, such as user and process accounts limited through account use policies, user account control, and privileged account management, compliant with the most current version of NIST Special Publication 800-53, Security and Privacy Controls for Information Systems and Organizations.[18] — *See* § III.C.3. of SD2C.

j. For any group accounts, establish a written process to review operational need for the account, document justification, maintain a list, ensure memorized secret authenticators are compliant with NIST SP 800-63B, maintain a list of personnel who have or had access to group accounts, and maintain a list of dates for last password resets. Within no more than seven (7) days after a user of a group account leaves the Owner/Operator's employment, the Owner/Operator must rotate memorized secret authenticators for the group account.[19] — *See* § III.C.4. of SD2C.

3. Remove all trust relationships, such as identity stores, between the Information and Operational Technology systems. Separate and dedicated identity providers must be implemented for the Information and Operational Technology systems, if they do not already exist. — *See* § III.C.5 of SD2C.

[18] Available at *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.*
[19] *See* section 5.1.1.1 of NIST SP 800-63B, *supra*, at n. 15.