



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

INFORMATION

MEMORANDUM FOR: The Record

SUBJECT: SD-Pipeline-2021-02B

DATE: June 6, 2022

The Transportation Security Administration has made a determination that the Security Directive, SD Pipeline-2021-02B, is no longer considered to contain Sensitive Security Information (SSI) and the markings denoting the document as SSI have been removed from the attached copy of the Security Directive.

Previous copies of the Security Directive marked as SSI may be disposed of and replaced with the unmarked (attached) version.

For instructions on the proper disposal of documents marked as SSI please refer to <https://www.tsa.gov/sites/default/files/ssi-best-practices-guide-for-non-dhs-employees.pdf>

Attachments:

1. Final Signed_SD Pipeline-2021-02B Non-SSI Version



<u>NUMBER</u>	Security Directive Pipeline-2021-02B
<u>SUBJECT</u>	Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing
<u>EFFECTIVE DATE</u>	December 17, 2021
<u>EXPIRATION DATE</u>	July 26, 2022
<u>CANCELS AND SUPERSEDES</u>	Not Applicable
<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 ¹
<u>AUTHORITY</u>	49 U.S.C. 114(d), (f), (l) and (m)
<u>LOCATION</u>	United States

I. PURPOSE AND GENERAL INFORMATION

Due to the ongoing cybersecurity threat to pipeline systems, the Transportation Security Administration (TSA) is issuing this Security Directive to complement the initial set of actions outlined in Security Directive Pipeline-2021-01, which went into effect on May 28, 2021.²

This Security Directive requires urgently needed steps to protect the national security, economy, and public health and safety of the United States and its citizens from the impact of

¹ 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). Scope of applicability for this Security Directive is the same as Security Directive Pipeline-2021-01.

² This directive was 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.”

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, including economic security, particularly if consumer reactions lead to longer-term shortages. 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.

Reducing the vulnerability of critical pipeline operations and facilities to cybersecurity threats is fundamental to securing our national and economic security. Recent events have emphasized the growing sophistication of nefarious persons and organizations, highlighted vulnerabilities, and intensified the urgency of implementing the requirements in this security directive. To protect against the ongoing threat to the United States' national and economic security posed by this threat, this Security Directive mandates that TSA-specified Owners/Operators of gas and liquid pipelines implement an array of cybersecurity measures to prevent disruption and degradation to their infrastructure.³ Specifically, Owner/Operators must do the following:

1. Implement critically important mitigation measures to reduce the risk of compromise from a cyberattack. *See* Section II.B.
2. Develop a Cybersecurity Contingency/Response Plan to reduce the risk of operational disruption or significant business or functional degradation of 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 II.C.
3. Test the effectiveness of the Owner/Operator's cybersecurity practices through an annual cybersecurity architecture design review. *See* Section II.D.

The requirements in this Security Directive are consistent with the recommended security measures in Section 7 of TSA's 2018 Pipeline Security Guidelines (with Change 1 (April 2021)),⁴ and the Joint Cybersecurity Advisory - Alert (AA21-131A), *DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks*, released by the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation on May 11, 2021 (as revised on May 20, 2021).⁵

³ See Attachment 1 for a summary of compliance deadlines

⁴ Available at https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf.

⁵ Available at <https://us-cert.cisa.gov/ncas/alerts/aa21-131a>.

Information provided to TSA pursuant to this Security Directive will be shared by TSA with CISA and may also be shared with the National Response Center and other agencies as appropriate.⁶

All information that must be reported 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). TSA may use the information, with company-specific data redacted, for TSA's intelligence-derived reports. TSA and CISA 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. The Office of Information and Regulatory Affairs has approved the collection of information required by this Security Directive in accordance with the Paperwork Reduction Act. *See* OMB Control No. 1652-0056.

TSA is issuing this Security Directive to protect pipeline security, in consultation with CISA, the United States Coast Guard, the Department of Energy, and the Pipeline and Hazardous Materials Safety Administration of the Department of Transportation. TSA, in consultation with CISA, has determined that each action required by this security directive must be implemented within the prescribed deadlines in order to protect transportation security.

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 if any section or subsection is otherwise deemed inapplicable, the remainder of this Security Directive shall not be affected.

II. ACTIONS REQUIRED

- A. The following actions must be applied to all Information and Operational Technology systems connected to critical pipeline systems or facilities identified by TSA.
- B. Implementing Critically Important Mitigation Measures

⁶ 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 TSA 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.

1. Owner/Operators must implement the following mitigation measures in a manner compliant with the most current versions of the National Institute of Standards and Technology (NIST) Digital Identity Guidelines.⁷
 - a. No later than **August 25, 2021**, implement and complete a mandatory password reset of all passwords within Information Technology systems (such as corporate remote access, and Virtual Private Networks).
 - b. No later than **November 23, 2021**, implement and complete a mandatory password reset(s) of all equipment within Operational Technology systems, to include Programmable Logic Controllers. If it is not technically feasible **by November 23, 2021**, an alternative procedure under Section 5 must be approved by TSA.
 - c. For equipment within Information and Operational Technology systems that do not permit password resets, **no later than November 23, 2021**, develop and submit a plan to TSA that identifies the equipment and provides a timeline for replacing the designated equipment.
 - d. **No later than August 25, 2021**, require supervisors of individuals with elevated privilege accounts/permission⁸ to verbally confirm and document with users of all such accounts their account ownership and continued 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 II.B.1.d., and maintain documentation establishing the date of last verification.
 - f. Within 7 days of completing each requirement in this subsection, ensure that the Cybersecurity Coordinator or other accountable executive submits a statement to TSA at SurfOps-SD@tsa.dhs.gov certifying that the Owner/Operator has met the requirement. Documentation of compliance must be provided to TSA upon request.
2. Owner/Operators must begin implementing the following cybersecurity measures without delay. Recognizing that applying these measures on Operational Technology systems may require additional planning in order to avoid unnecessary operational

⁷ 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/>).

⁸ See National Security Agency's Cybersecurity Information Bulletin: [Defend Privileges and Accounts](https://www.defense.gov) ([defense.gov](https://www.defense.gov)), PP-19-1039 (August 2019) for information on privileges.

consequences, unless otherwise directed, requirements applicable to Information Technology systems must be fully implemented **no later than October 24, 2021**. Requirements applicable to Operational Technology systems must be fully implemented **no later than January 22, 2022**. The requirements in paragraph II.B.2.b. (network segmentation) that involve both Information and Operational Technology systems must be fully implemented **no later than January 22, 2022**.

- 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.⁹
- 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—
 - i. Identifying Information and Operational Technology network inter-dependencies;
 - 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;
 - 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;
 - iv. Organizing Operational Technology system assets into logical zones, such as isolating unrelated sub-processes, by taking into account criticality, consequence, and operational necessity;
 - v. Monitoring and filtering traffic between networks of different trust levels, for example, between the Information and Operational Technology systems, by defining appropriate communication conduits between the

⁹ As stated in NIST Special Publication 800-63B, multifactor cryptographic device authenticators or validators must not leverage Short Message Service. *See supra* n. 77, at section 5.1,

- logical zones and deploying security controls to monitor and filter network traffic and communications between logical zones;¹⁰
- vi. Prohibiting Operational Technology system protocols from traversing the Information Technology system unless expressly through an encrypted point-to-point tunnel; and
 - 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.
- c. Review and update (or develop, if necessary) log retention policies to ensure that they include policies and procedures consistent with NIST standards¹¹ for (i) log management; (ii) secure log management infrastructure; and (iii) how long log data must be maintained.
- d. Employ filters sufficient to—
- i. Identify malicious email traffic, spam and phishing emails and inhibit them from reaching end users;
 - 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;
 - iii. Prevent users and devices from accessing malicious websites by implementing Uniform Resource Locator block lists and/or allowlists;
 - 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 the identified baseline of communications and ensure it is necessary for operations.

¹⁰ For additional guidance on sufficient monitors and filters, see the Purdue Enterprise Reference Architecture (PERA) model for industrial control system architecture.

¹¹ See NIST Special Publication 800-92, Guide to Computer Security Log Management (available at <https://csrc.nist.gov/publications/detail/sp/800-92/final>).

- 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.
- f. Establish passive Domain Name System capabilities that are consistent with currently recognized standards¹² and, at a minimum, include the following actions:
 - 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 —
 - 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.
 - 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

¹² See Passive DNS-Common Output Format, available at <https://datatracker.ietf.org/doc/html/draft-dulaunoy-dnsop-passive-dns-cof>.

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.
 - 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;
 - 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;
 - 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 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

- vi. Require implementation of signatures to detect and/or block connection from post-exploitation tools.
 - 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.¹³
 - 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 list of personnel who have or had access to group accounts, and maintain list of dates for last password resets. Within no more than 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.¹⁴
3. **No later than January 22, 2022**, 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.
 4. Within 7 days of completing the requirements in II.B.1., II.B.2., and II.B.3., including specific deadlines in certain sections, Owner/Operators must ensure that their Cybersecurity Coordinator or other accountable executive submits a statement to TSA at SurfOps-SD@tsa.dhs.gov certifying that the Owner/Operator has met the requirements. Documentation of compliance must be provided to TSA upon request.

C. Implementing a Cybersecurity Contingency/Response Plan

1. **No later than August 25, 2021**, unless otherwise directed, Owner/Operators must develop and adopt a Cybersecurity Contingency/Response Plan that includes measures to reduce the risk of operational disruption, or other significant business or functional degradation to necessary capacity, should their pipeline or facility experience a cybersecurity incident. The Cybersecurity Contingency/Response Plan

¹³ Available at <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>.

¹⁴ See section 5.1.1.1 of NIST SP 800-63B, *supra*, at n. 9.

must provide specific measures sufficient to ensure the following objectives, as applicable and feasible.

- a. Prompt isolation of the infected system by—
 - i. Removing the infected system from all networks, and disabling the system's wireless, Bluetooth, and any other potential networking capabilities; and
 - ii. Ensuring all shared and networked drives are disconnected, whether wired or wireless.
- b. Segregation of the infected computer from other computers and devices by—
 - i. Segregating (removing from the network) the infected computer(s);
 - ii. Segregating any other computers or devices that shared a network with the infected computer(s);¹⁵
 - iii. Preserving volatile memory by collecting forensic memory image of affected device(s) before powering off or moving; and
 - iv. Isolating and securing all infected and potentially infected computers and devices, making sure to clearly label any equipment that has been encrypted by malware.
- c. Security and integrity of backed-up data, including measures to secure backups, store backup data offline, and procedures requiring scanning of stored backup data with an antivirus program to check that it is free of known malware when the backup is made and when tested for restoration.
- d. Established capability and governance for isolating the Information Technology and Operational Technology systems in the event of a cybersecurity incident that arises to the level of potential operational disruption while maintaining operational standards and limits.

¹⁵ The Plan must provide measures sufficient to manage a ransomware event, including segregating computers that have been fully encrypted by such an attack and powering-off and segregating infected computers and computers that have not been fully encrypted so as to allow for the recovery of partially encrypted files by specialists.

- e. Situational exercises to test the effectiveness of procedures, and personnel responsible for implementing measures, in the Cybersecurity Contingency/Response Plan, no less than annually.
 2. The Cybersecurity Contingency/Response Plan must, at a minimum, identify who (by position) is responsible for implementing the specific measures and any necessary resources needed to implement these measures.
 3. Within 7 days of completing the requirements in this section, Owner/Operators must ensure that their Cybersecurity Coordinator or other accountable executive submits a statement to TSA at SurfOps-SD@tsa.dhs.gov certifying the Owner/Operator has met the requirement. Documentation of compliance must be provided to TSA upon request.
- D. Conduct Operational Technology System Cybersecurity Architecture Design Reviews
1. **No later than January 22, 2022**, unless otherwise directed, Owner/Operators must schedule a third-party evaluation of the Owner/Operator's Operational Technology system design and architecture, to be conducted **no later than July 26, 2022**, which 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. This evaluation must —
 - a. Be conducted by an independent third-party, unless otherwise approved by TSA, that has demonstrated capability to perform the cybersecurity architecture design review required by this Security Directive.
 - b. Be completed annually thereafter for the duration of this Security Directive, as revised and renewed.
 - c. Include a written report detailing the results of the evaluation and the acceptance or rejection of any recommendations provided by the evaluator to address vulnerabilities. This written report must be made available to TSA upon request and retained for no less than two (2) years from the date of completion.
 2. A Validated Architecture Design Review (VADR) conducted by the Department of Homeland Security (DHS) satisfies this requirement. If not a VADR conducted by DHS, the evaluation required by paragraph II.D.1. must be completed using a standard that, at a minimum, evaluates the extent to which the Owner/Operator's system architecture and design is compliant with the most current version of NIST Special Publication 800.82, *Guide to Industrial Control Systems (ICS) Security*, and

also encompasses an architecture and design review; system configuration; log file review; an analysis of network traffic to develop a detailed representation of the communications, flows, and relationships between devices; and identifies anomalous (and potentially suspicious) communication flows.

3. The deadline for the testing required by paragraphs II.D.1. does not apply to Owner/Operators who have had a DHS-conducted VADR between **July 26, 2020, and July 26, 2021**. The anniversary date for annual testing required by this section is one year from the date of the DHS VADR report.
4. Within 7 days of completing the requirements in this section, Owner/Operators must ensure that their Cybersecurity Coordinator or other accountable executive submits a statement to TSA at SurfOps-SD@tsa.dhs.gov certifying that the Owner/Operator has met the requirement. Documentation of compliance must be provided to TSA upon request.

III. RECORDS

- A. Owner/Operators may use previously developed plans, assessments, tests, and evaluations to meet the requirements in this Security Directive. If the Owner/Operator is relying on these materials, the Owner/Operator must notify TSA no later than the deadline identified in each section and ensure that the relevant records include an index, organized in the same sequence as the requirements in this Security Directive, of where the requirements of this Security Directive may be found.
- B. Plans and results of tests or evaluations created and maintained pursuant to this Security Directive must be stored and transmitted consistent with the requirements in 49 CFR part 1520.¹⁶

IV. PROCEDURES FOR SECURITY DIRECTIVES

- A. Owner/Operators must:
 1. Immediately provide written confirmation of receipt of this Security Directive via e-mail to TSA at SurfOps-SD@tsa.dhs.gov; and
 2. 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

¹⁶ Owner/Operators may contact SSI@tsa.dhs.gov for more information on how to comply with requirements for the protection of Sensitive Security Information.

Directive only to the Owner/Operator's direct employees and authorized representatives responsible for implementing applicable security measures as necessary to ensure compliance.

3. TSA's regulations prohibit unauthorized dissemination of this Security Directive or information contained herein. *See* 49 CFR part 1520. The Owner/Operator must—
 - a. Brief all individuals receiving Sensitive Security Information on the restrictions governing dissemination.
 - b. Restrict the availability of the Security Directive, and information contained in the document, to those persons with a need-to-know.
 - c. Refuse to release the Security Directive, and any information contained in this document, to persons other than those who have an operational need to know without the prior written consent of TSA.
 4. TSA recognizes that Owner/Operators must ensure the safety of their operations at all times. To the extent that an Owner/Operator determines that implementation of any requirement in this Security Directive could jeopardize safe operations or cause an operational disruption, the Owner/Operator must promptly, no later than seven days of their determination, notify TSA at SurfOps-SD@tsa.dhs.gov, including a written justification for their inability to comply. TSA will review and consider all information provided in consultation with CISA, the Department of Energy, and the Pipeline and Hazardous Materials Safety Administration before deciding whether to concur with the Owner/Operator's determination. TSA may require the Owner/Operator to provide additional information or request an alternative measure consistent with Section V. of this Security Directive. Notification to TSA under this section does not stay the effective date for any requirement in this Security Directive unless otherwise notified by TSA.
- B. 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 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.

V. APPROVAL OF ALTERNATIVE MEASURES

Owner/Operators may submit their proposed alternative measures to TSA via e-mail to SurfOps-SD@tsa.dhs.gov, including the basis for submitting the alternative measures. TSA may grant a request for an alternative measure if the designated official determines that safety and the public interest will allow it, and the proposed alternative provides the level of security required by this Security Directive. The Owner/Operator must implement any alternative measures approved by TSA. Any communications referring to specific measures in this Security Directive must be protected in accordance with the requirements in 49 CFR part 1520

VI. DEFINITIONS

In addition to the terms defined in TSA's section 1500.3 of title 49, Code of Federal Regulations, and Security Directive Pipeline-2021-01, 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. *Cybersecurity Architecture Design Review* means a technical assessment based on federal and industry 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. *Days* means calendar days unless otherwise indicated.
- D. *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.
- E. *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.

- F. *Industrial Control System Protocols* means network and host communication methods and standards which are specifically implemented by Operational Technology systems and applications.
- G. *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
- H. *Necessary capacity* means the owner/operators determination of capacity to support their business critical functions required for pipeline operations and market expectations.
- I. *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).
- J. *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.
- K. *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.
- L. *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.
- M. *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.
- N. *Spam* means electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.
- O. *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.

- P. *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.
- Q. *Trusted network* means a system in which there exists a level of confidence (based on rigorous analysis and testing) that the security principals and mechanisms (*e.g.*, separation, isolation, least privilege, discretionary and non-discretionary access control, trusted path, authentication, and security policy enforcement) are correctly implemented and operate as intended even in the presence of adversarial activity.
- R. *Validated Architecture Design Review* means an evaluation conducted by the Cybersecurity and Infrastructure Security Agency, with other federal government agencies and resources, of an Owner/Operator's systems, networks, and security services to determine if they are designed, built, and operated in a reliable and resilient manner. These reviews are based on federal government standards, guidelines, and best practices and are designed for Information and Operational Technology systems. For more information on Validated Architecture Design Reviews, see [Pipeline Cybersecurity Initiative Fact Sheet 20181115_CISA.indd](#).

THOMAS L
BUSH

Digitally signed by
THOMAS L BUSH
Date: 2021.12.17
12:30:43 -05'00'

Thomas L. Bush
Acting Executive Assistant Administrator
Operations Support

Attachment 1: (SSI) Table of Implementation Timeframes