



SECURITY DIRECTIVE

<u>NUMBER</u>	Security Directive Pipeline-2021-01B
<u>SUBJECT</u>	Enhancing Pipeline Cybersecurity
<u>EFFECTIVE DATE</u>	May 29, 2022
<u>EXPIRATION DATE</u>	May 29, 2023
<u>CANCELS AND SUPERSEDES</u>	Security Directive Pipeline-2021-01A
<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

PURPOSE AND GENERAL INFORMATION

Due to the ongoing cybersecurity threat to pipeline systems and associated infrastructure, the Transportation Security Administration (TSA) is issuing this Security Directive.²

This Security Directive requires three critical actions. First, it requires TSA-specified Owner/Operators to report cybersecurity incidents to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). Second, it requires Owner/Operators to designate a Cybersecurity Coordinator who is required to be available to TSA and CISA 24/7 to coordinate cybersecurity practices and address any incidents that arise. Third, it requires Owner/Operators to review their current activities against TSA's recommendations for pipeline cybersecurity to assess cyber risks, identify any gaps, develop remediation measures, and report the results to TSA and CISA.

¹ See section 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). Section 1557(b) requires TSA to review pipeline security plans and inspect critical facilities of the 100 most critical pipeline operators. In general, criticality is determined based on factors such as the volume of product transported, service to other critical sectors, *etc.*

² This Security Directive is being 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."

To avoid duplicate reporting, information provided to CISA pursuant to this Security Directive will be shared with TSA and may also be shared with the National Response Center and other agencies as appropriate. Similarly, information provided to TSA pursuant to this Security Directive will be shared with CISA and may also be shared with the National Response Center and other agencies as appropriate.³ All information that must be reported to TSA or CISA pursuant to this Security Directive is sensitive security information subject to the protections of part 1520 of title 49, Code of Federal Regulations.

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.⁴

ACTIONS REQUIRED

- A. Owner/Operators must designate and use a primary and at least one alternate Cybersecurity Coordinator at the corporate level.
 1. Owner/Operators must provide in writing to TSA the names, titles, phone number(s), and email address(es) of the Cybersecurity Coordinator and alternate Cybersecurity Coordinator(s) within seven days of the commencement of new operations or change in any of the information required by this section.
 2. The Cybersecurity Coordinator shall—
 - a. Be a U.S. citizen who is eligible for a security clearance;
 - b. Serve as the primary contact for cyber-related intelligence information and cybersecurity-related activities and communications with TSA and CISA;
 - c. Be accessible to TSA and CISA 24 hours a day, seven days a week;
 - d. Coordinate cyber and related security practices and procedures internally; and
 - e. Work with appropriate law enforcement and emergency response agencies.
- B. Owner/Operators must report to the CISA cybersecurity incidents involving systems that the Owner/Operator has responsibility to operate and maintain including:
 1. Unauthorized access of an Information or Operational Technology system;
 2. Discovery of malicious software on an Information or Operational Technology system;

³Presidential Policy Directive (PPD) 41 calls for Federal cyber incident response agencies to share incident information with each other to achieve unity of governmental effort. *See* PPD-41 § III.D.

⁴ *See* Information Collection Request, OMB No. 1652-0050 for TSA's identification of the Most Critical Pipelines, as required by sec. 1557(b) of the 9/11 Act and OMB No. 1652-0055 for assessment data.

3. Activity resulting in a denial of service to any Information or Operational Technology system;
 4. A physical attack against the Owner/Operator's network infrastructure, such as deliberate damage to communication lines; and
 5. Any other cybersecurity incident that results in operational disruption to the Owner/Operator's Information or Operational Technology systems or other aspects of the Owner/Operator's pipeline systems or facilities, or otherwise has the potential to cause operational disruption that adversely affects the safe and efficient transportation of liquids and gases including, but not limited to impacts to a large number of customers, critical infrastructure or core government functions, or impacts national security, economic security or public health and safety.
- C. Owner/Operators must report the information required by Section B. as soon as practicable, but no later than **24** hours after a cybersecurity incident is identified. Reports must be made to CISA Central using CISA's Reporting System form at: <https://us-cert.cisa.gov/forms/report> or by calling (888) 282-0870.⁵ If the required information is not available at the time of reporting, Owner/Operators must submit an initial report within the specified timeframe and supplement as additional information becomes available. All reported information will be protected in a manner appropriate for the sensitivity and criticality of the information.
- D. In the report to CISA required by Section B., Owner/Operators must include the following information:
1. The name of the reporting individual and contact information, including a telephone number or email address. The report must also explicitly specify that the information is being reported in order to satisfy the reporting requirements in Security Directive-Pipeline-2021-01.
 2. The affected hazardous liquid and natural gas pipeline(s) and/or facilities, including identifying information and location.
 3. Description of the threat, incident, or activity, to include:
 - a. Information about who has been notified and what action has been taken;
 - b. Any relevant information observed or collected by the Owner/Operator, such as malicious IP addresses, malicious domains, malware, or the abuse of legitimate software or accounts; and

⁵ CISA's Incident Reporting System provides a secure web-enabled means of reporting computer security incidents to CISA. This system assists analysts in providing timely handling of the security incidents Owner/Operators must report pursuant to this Security Directive as well as the ability to conduct improved analysis.

- c. Any known threat information, to include information about the source of the threat or attack, if available.
4. A description of the incident's impact or potential impact on Information or Operational Technology systems and operations. This information must also include an assessment of actual, imminent or potential service operations, operational delays, and/or data theft that have or are likely to be incurred, as well as any other information that would be informative in understanding the impact or potential impact of the cybersecurity incident.
5. A description of all responses that are planned or under consideration, to include, for example, a reversion to manual backups, if applicable.
6. Any additional relevant information.

E. Vulnerability Assessment

1. Owner/Operators must review Section 7 of TSA's 2018 Pipeline Security Guidelines (with Change 1 (April 2021)),⁶ and—
 - a. Assess whether current practices and activities to address cyber risks to Owner/Operators Information and Operational Technology systems align with the Guidelines;
 - b. Identify any gaps; and
 - c. Identify remediation measures that will be taken to fill those gaps and a timeline for implementing these remediation measures.
2. The assessment and identification of gaps must be completed using the form provided by TSA.⁷
3. Owner/Operators who have not previously submitted a vulnerability assessment to TSA must provide a report containing all information required by this section to TSA and CISA within 30 days of the effective date of this SD.

PROCEDURES FOR SECURITY DIRECTIVES

A. Owner/Operators must:

1. Immediately provide written confirmation of receipt of this Security Directive via email to TSA at SurfOps-SD@tsa.dhs.gov.

⁶ See https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf

⁷ The assessment form is not sensitive security information before it is completed. Once any question is answered on the form, however, it becomes sensitive security information subject to the protections of 49 CFR part 1520.

2. Immediately disseminate the information and measures in this Security Directive to corporate senior management, security management representatives, and any personnel having responsibilities in implementing the provisions in this Security Directive. The Owner/Operator also should share this Security Directive with anyone subject to the provisions of this Security Directive to include, but not limited to, Federal, state, and local government personnel, tenants, and contractors.
 3. Brief all individuals responsible for implementing this Security Directive.
- B. Owner/Operators may comment on this Security Directive by submitting data, views, or arguments in writing to TSA via email at SurfOps-SD@tsa.dhs.gov. TSA may amend the Security Directive based on comments received. Submission of a comment does not delay the effective date of the Security Directive.

DEFINITIONS

- A. *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).
- B. *Days* means calendar days unless otherwise indicated.
- C. *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.
- D. *Operational disruption* means a deviation from or interruption of normal activities or operations that results in a loss of data, system availability, system reliability, or control of systems, or indicates unauthorized access to, or malicious software present on, critical information technology systems.
- E. *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.

- F. *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.
- G. *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 policy violation such as the use of shared credential by an employee otherwise authorized to access it.

APPROVAL OF ALTERNATIVE MEASURES

Owner/Operators must immediately notify TSA via email at TSA-Surface@tsa.dhs.gov if unable to implement any of the measures in this Security Directive. Owner/Operators may submit proposed alternative measures and the basis for submitting the alternative measures to TSA for approval to the email address above.

Austin Gould
Acting Executive Assistant Administrator
Operations Support