[9110-9M]

DEPARTMENT OF HOMELAND SECURITY

6 CFR Chapter I

49 CFR Chapter XII

Ratification of Security Directives

AGENCY: Office of Strategy, Policy, and Plans, Department of Homeland Security (DHS).

ACTION: Notice of ratification of security directives.

SUMMARY: The Department of Homeland Security (DHS) is publishing official notice that the Transportation Security Oversight Board (TSOB) ratified Transportation Security Administration (TSA) Security Directive Pipeline-2021-01D and Security Directive Pipeline-2021-02E, applicable to owners and operators of critical hazardous liquid and natural gas pipeline infrastructure (owner/operators). Security Directive Pipeline-2021-01D, issued on May 29, 2024, extended the requirements of the Security Directive Pipeline-2021-01 series for an additional year, with minor revisions. Security Directive Pipeline-2021-02E, issued on July 26, 2024, extended the requirements of the Security Directive Pipeline-2021-02 series for an additional year, with amendments to strengthen their effectiveness and provide additional clarity.

DATES: The TSOB ratified Security Directive Pipeline-2021-01D on June 28, 2024 and Security Directive Pipeline-2021-02E on August 23, 2024.

FOR FURTHER INFORMATION CONTACT: Thomas McDermott, Deputy Assistant Secretary for Cyber, Infrastructure, Risk and Resilience Policy, at 202-834-5803 or thomas.mcdermott@hq.dhs.gov.

SUPPLEMENTARY INFORMATION:

I. Background

A. Cybersecurity Threat

The cyber threat to the country's critical infrastructure has only increased in the time since TSA issued its initial cybersecurity-related security directives to pipeline entities in 2021 in response to the Colonial Pipeline incident. Cyber threats to surface transportation systems, including hazardous liquid and natural gas pipelines and facilities, continue to proliferate, as both nation-states and criminal cyber groups target critical infrastructure in order to cause operational disruption and economic harm.[1] In addition to the Colonial Pipeline incident, cyber attackers have maliciously targeted surface transportation modes in the United States, including freight railroads, passenger railroads, and rail transit systems, with multiple cyberattack and cyber espionage campaigns.[2] Cyber incidents, particularly ransomware attacks, are likely to increase in the near and long term, due in part to vulnerabilities identified by threat actors in U.S. networks.[3] Especially in light of the ongoing Russia-Ukraine conflict,[4] these threats remain elevated and pose a risk to the national and economic security of the United States.

In its 2023 annual assessment, the Intelligence Community noted that "China almost certainly is capable of launching cyber attacks that could disrupt critical infrastructure services within the United States, including against oil and gas pipelines,

---

[1] Annual Threat Assessment of the U.S. Intelligence Community, Office of the Director of National Intelligence (2024 Intelligence Community Assessment), 11, 16 (dated Feb. 5, 2024) (last accessed July 23, 2024, at https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf).

[2] These activities include the January 2023 breach of the Washington Metropolitan Area Transit Authority; the January 2023 breach of San Francisco's Bay Area Rapid Transit System; and the April 2021 breach of New York City's Metropolitan Transportation Authority (the nation's largest mass transit agency) by hackers linked to the Chinese government. This threat is ongoing: on February 7, 2024, CISA published an advisory warning of the threat posed by PRC state-sponsored actors. *See* Cybersecurity Advisory (AA24-038A), *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*.

[3] Alert (AA22-040A), *2021 Trends Show Increased Globalized Threat of Ransomware*, released by CISA on February 10, 2022 (as revised).

[4] Joint Cybersecurity Alert – Alert (AA22-110A), *Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, released cybersecurity authorities of the United States, Australia, Canada, New Zealand, and the United Kingdom on April 20, 2022 (as revised).

and rail systems."[5] And the 2024 annual assessment notes that, "[i]f Beijing believed that a major conflict with the United States were imminent, it would consider aggressive cyber operations against U.S. critical infrastructure and military assets. Such a strike would be designed to deter U.S. military action by impeding U.S. decision-making, inducing societal panic, and interfering with the deployment of U.S. forces."[6] In addition, "Russia maintains its ability to target critical infrastructure…in the United States as well as in allied and partner countries" and "Tehran's opportunistic approach to cyber-attacks puts U.S. infrastructure at risk for being targeted."[7] Furthermore, "malicious cyber actors have begun testing the capabilities of AI-developed malware and AI-assisted software development—technologies that have the potential to enable larger scale, faster, efficient, and more evasive cyber-attacks—against targets, including pipelines, railways, and other US critical infrastructure."[8]

B. Regulatory History

Following the Colonial Pipeline incident in May 2021, TSA issued two security directives requiring owners and operators of critical hazardous liquid and natural gas pipelines or liquefied natural gas facilities (owner/operators) to implement cybersecurity measures necessary to prevent disruption and degradation to their critical infrastructure. On May 27, 2021, TSA issued the first directive (Security Directive Pipeline-2021-01), which required covered owner/operators to: (1) report cybersecurity incidents to CISA; (2) designate a cybersecurity coordinator to be available 24/7 to coordinate with TSA and CISA; and (3) conduct a vulnerability assessment of cybersecurity practices, identify any

---

[5] Annual Threat Assessment of the U.S. Intelligence Community, Office of the Director of National Intelligence (2023) (2023 Intelligence Community Assessment), 10 (dated February 6, 2023) (last accessed July 23 2024, at https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.

[6] 2024 Intelligence Community Assessment at 11.

[7] 2024 Intelligence Community Assessment at 16, 20.

[8] DHS Intelligence and Analysis (I&A), Homeland Threat Assessment (2024) at 18 (last accessed July 23, 2024, at https://www.dhs.gov/sites/default/files/2023-09/23_0913_ia_23-333-ia_u_homeland-threat-assessment-2024_508C_V6_13Sep23.pdf).

gaps, and develop a plan and timeline for remediation. TSA issued the second directive (Security Directive Pipeline-2021-02) on July 19, 2021, which required owner/operators to implement additional specific cybersecurity measures to prevent disruption and degradation to their infrastructure.

Due to the continuing cyber threat to pipeline infrastructure, the requirements of both Security Directive Pipeline-2021-01 and Security Directive Pipeline-2021-02 have been renewed and extended beyond their original expiration dates by subsequent directives, creating two security directive "series" (the Security Directive Pipeline-2021-01 series and the Security Directive Pipeline-2021-02 series). In several instances, as TSA renewed each of these security directive series, TSA also amended their requirements to strengthen their effectiveness and address emerging cyber threats. Most significantly, TSA transitioned the requirements of the Security Directive Pipeline-2021-02 series to be more performance-based and less prescriptive. The performance-based approach enhances security by mandating that critical security outcomes are achieved while allowing owner/operators to choose the most appropriate security measures for their specific systems and operations. Under the performance-based framework of the Security Directive Pipeline-2021-02 series, TSA identified critical security outcomes that covered parties must achieve. To ensure that these outcomes are met, the directives in this series now require owner/operators to:

- Establish and implement a TSA-approved Cybersecurity Implementation Plan (CIP) that describes the specific cybersecurity measures employed and the schedule for achieving the security outcomes identified;
- Develop and maintain an up-to-date Cybersecurity Incident Response Plan (CIRP) to reduce the risk of operational disruption, or the risk of other significant impacts on business critical functions, as defined in the directive,

should the Information and/or Operational Technology systems of a gas or liquid pipeline be affected by a cybersecurity incident; and

- Establish a Cybersecurity Assessment Program (CAP) 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.

The table below provides a list of each the security directives issued within the Security Directive Pipeline-2021-01 and Security Directive Pipeline-2021-02 series. All of the security directives in both series are available online in TSA's Surface Transportation Cybersecurity Toolkit.[9]

[9] TSA Surface Transportation Cybersecurity Toolkit, *available at* https://www.tsa.gov/for-industry/surface-transportation-cybersecurity-toolkit.

Table 1: TSA Security Directives Applicable to Critical Pipeline Systems					
Security Directive	**Date Issued**	**Effective Date**	**Date Ratified by TSOB**	**Set Expiration Date**	**Federal Register Citation of Ratification**
Pipeline-2021-01	May 27, 2021	May 28, 2021	July 3, 2021	May 28, 2022	86 FR 38209
Pipeline-2021-01A	Dec. 2, 2021	Dec. 2, 2021	Dec. 29, 2021	May 28, 2022	87 FR 31093
Pipeline-2021-01B	May 27, 2022	May 29, 2022	June 24, 2021	May 29, 2023	88 FR 36919[10]
Pipeline-2021-01C	May 22, 2023	May 29, 2023	June 21, 2023	May 29, 2024	89 FR 28570
Pipeline-2021-01D	May 29, 2024	May 29, 2024	June 28, 2024	May 29, 2025	*Current
Pipeline-2021-02	Jul. 19, 2021	Jul. 26, 2021	Aug. 17, 2021	Jul. 26, 2022	86 FR 52953
Pipeline-2021-02B	Dec. 17, 2021	Dec. 17, 2021	Jan. 13, 2022	Jul. 26, 2022	87 FR 31093
Pipeline-2021-02C	Jul. 21, 2022	Jul. 27, 2022	Aug. 19, 2022	Jul. 27, 2023	88 FR 36919
Pipeline-2021-02D	Jul. 26, 2023	Jul. 27, 2023	Aug. 24, 2023	Jul. 27, 2024	89 FR 28570
Pipeline-2021-02E	Jul. 26, 2024	Jul. 27, 2024	Aug. 23, 2024	Jul. 27, 2025	*Current

C. Security Directive Pipeline-2021-01D

In light of the continuing threat, TSA determined that the cybersecurity measures required by the Security Directive-Pipeline-2021-01 series, as amended and extended, remain necessary to protect the Nation's critical pipeline infrastructure beyond Security Directive Pipeline-2021-01C's expiration date of May 29, 2024. On May 29, 2024, TSA issued Security Directive Pipeline-2021-01D to extend the requirements of Security Directive Pipeline-2021-01 series for an additional year. Security Directive Pipeline-2021-01D became effective May 29, 2024, and expires on May 29, 2025. Security

[10] Security Directive Pipeline-2021-01B also extended the deadline by which cybersecurity incidents must be reported to CISA from 12 hours to 24 hours after an incident is identified. This change aligned the reporting timeline for critical pipeline entities to mirror the reporting requirements applicable to other surface transportation entities and aviation entities.

Directive Pipeline-2021-01D contains minor revisions refining existing requirements to clarify applicability, compliance timelines, and reporting requirements, as well as updated definitions to ensure standardization across TSA's cybersecurity requirements applicable to different transportation modes.

D. Security Directive Pipeline-2021-02E

Considering the continuing threat, TSA also determined that the measures required by the Security Directive-Pipeline-2021-02 series, as amended and extended, remain necessary to protect the Nation's critical pipeline infrastructure beyond Security Directive Pipeline-2021-02D's expiration date of July 27, 2024. On July 26, 2024, TSA issued Security Directive Pipeline-2021-02E to extend the requirements of Security Directive Pipeline-2021-02 series for an additional year. Security Directive Pipeline-2021-02E became effective July 27, 2024, and expires on July 27, 2025.

In addition to extending the existing requirements, Security Directive Pipeline-2022-02E contains several amendments to strengthen the effectiveness of certain requirements and provide further clarity. The revisions include new and modified definitions clarifying certain terms and harmonizing terminology across TSA's cybersecurity requirements applicable to different transportation modes; clarifying when responsibility for compliance with the directive's requirements is shared between an owner/operator and a third party; and clarifying requirements regarding submission of CAP and related annual reports.

II. TSOB Ratification

TSA has broad statutory responsibility and authority to safeguard the nation's transportation system.[11] The TSOB—a body consisting of the Secretary of Homeland Security, the Secretary of Transportation, the Attorney General, the Secretary of Defense, the Secretary of the Treasury, the Director of National Intelligence, or their designees,

[11] *See, e.g.*, 49 U.S.C. 114(d), (f), (*l*), (m).

and a representative of the National Security Council—reviews certain TSA regulations and security directives as consistent with law.[12] TSA issued Security Directive Pipeline-2021-01D and Security Directive Pipeline-2021-02E under 49 U.S.C. § 114(*l*)(2)(A), which authorizes TSA to issue emergency regulations or security directives without providing notice or the opportunity for public comment where "the Administrator determines that a regulation or security directive must be issued immediately in order to protect transportation security . . .." Security directives issued pursuant to the procedures in 49 U.S.C. § 114(*l*)(2) "shall remain effective for a period not to exceed 90 days unless ratified or disapproved by the Board or rescinded by the Administrator."[13]

Following the issuance of Security Directive Pipeline-2021-01D on May 29, 2024, and Security Directive Pipeline-2021-02E on July 26, 2024, the chair of the TSOB convened the board to review the directives.[14] In reviewing each Security Directive, the TSOB reviewed the required measures extended and amended by the directives and the continuing need for TSA to maintain these requirements pursuant to its emergency authority under 49 U.S.C. 114(*l*)(2) to prevent the disruption and degradation of the country's critical transportation infrastructure. The TSOB also considered whether to authorize TSA to extend each security directive beyond their current expiration dates subject to certain conditions, should the TSA Administrator believe such an extension is necessary to address the evolving threat that may continue beyond the original expiration date.

Following its review, the TSOB ratified Security Directive Pipeline-2021-01D on June 28, 2024, and Security Directive Pipeline-2021-02E on August 23, 2024. The TSOB also authorized TSA to extend each of the security directives beyond their current

---

[12] *See, e.g.*, 49 U.S.C. 115; 49 U.S.C. 114(*l*)(2)(B).
[13] 49 U.S.C. 114(*l*)(2)(B).
[14] The Secretary of Homeland Security serves as the TSOB Chairperson, 49 U.S.C. 115(b)(2), and has further delegated that responsibility to the Deputy Secretary of Homeland Secretary. DHS Delegation No. 7071.1.

expiration dates, should the TSA Administrator determine such an extension is necessary to address the evolving threat that may continue beyond the original expiration date. Such an extension is subject to the following conditions: (1) there are no changes to the security directive other than an extended expiration date; (2) the TSA Administrator makes an affirmative determination that conditions warrant the extension of the directive's requirements; and (3) the TSA Administrator documents such a determination and notifies the TSOB.

Kristie Canegallo

Senior Official Performing the Duties of the Deputy Secretary of Homeland Security & Chairman of the Transportation Security Oversight Board.

[FR Doc. 2025-01243 Filed: 1/15/2025 11:15 am; Publication Date: 1/17/2025]