[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: Notification of ratification of security directives.

SUMMARY: The Department of Homeland Security (DHS) is publishing official notice that the Transportation Security Oversight Board (TSOB) has ratified Transportation Security Administration (TSA) Security Directive 1580-21-01B, Security Directive 1582-21-01B, Security Directive 1580/82-2022-01A, and Security Directive 1580/82-2022-01C applicable to owners and operators of critical rail entities (owners/operators). Security Directive 1580-21-01B and Security Directive 1582-21-01B extended the requirements of 1580-21-01 and 1582-21-01 series for an additional year, with minor revisions. Security Directive 1580/82-2022-01A and Security Directive 1580/82-2022-01C extend the performance-based requirements of the 1580/82-2022-01 series for an additional year and amends them to strengthen their effectiveness and address emerging cyber threats.

DATES: The TSOB ratified Security Directive 1580-21-01B, Security Directive 1582-21-01B, and Security Directive 1580/82-2022-01A on November 22, 2023. The TSOB ratified Security Directive 1580/82-2022-01C on July 29, 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 faced by the nation's critical rail infrastructure has only increased in the time since TSA issued its initial security directives addressing cybersecurity in rail and mass transit in December 2021.[1] Cyber threats to surface transportation systems, including railroads and transit systems, continue to proliferate, as both nation-states and criminal cyber groups target critical infrastructure in order to cause operational disruption and economic harm.[2] In recent years, 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.[3] 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.[4] Especially in light of the ongoing Russia-Ukraine conflict,[5] these threats remain elevated and pose a risk to the national and economic security of the United States.

---

[1] Transportation Security Administration, SD 1580-21-01 Enhancing Rail Cybersecurity (Dec. 31, 2021), https://www.tsa.gov/sites/default/files/sd-1580-21-01_signed.pdf; Transportation Security Administration, SD 1582-21-01 Enhancing public Transportation and Passenger Railroad Cybersecurity (Dec. 31, 2021), https://www.tsa.gov/sites/default/files/sd-1582-21-01_signed.pdf.

[2] 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).

[3] 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 government of the People's Republic of China. 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*.

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

[5] 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).

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, and rail systems."[6] 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."[7] 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."[8] Furthermore, "malicious cyber actors have begun testing the capabilities of [artificial intelligence (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."[9]

B. Regulatory History

To counter the threat to rail infrastructure, in December 2021, TSA issued two security directives to owners and operators of certain higher risk rail entities (owner/operators) requiring them to implement cybersecurity measures necessary to prevent disruption and degradation to their critical infrastructure. Security Directive 1580-21-01 (applicable to freight rail entities) and Security Directive 1582-21-01

---

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

[7] 2024 Intelligence Community Assessment at 11.

[8] 2024 Intelligence Community Assessment at 16, 20.

[9] DHS Intelligence and Analysis (I&A), Homeland Threat Assessment (2024) at 18 (last accessed July 23, 2024, *available 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).

(applicable to passenger rail and mass transit entities) required covered owner operators to: (1) report cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency (CISA); (2) designate a cybersecurity coordinator to be available 24/7 to coordinate with TSA and CISA; (3) conduct a vulnerability assessment of cybersecurity practices, identify any gaps, and develop a plan and timeline for remediation; and (4) develop a Cybersecurity Incident Response Plan to reduce the risk of operational disruption in the event of a cybersecurity incident.

Due to the evolving threat to freight and passenger rail, TSA issued Security Directive 1580/82-2022-01 on October 18, 2022, which built on the requirements of the initial directives and required covered owner/operators to implement additional performance-based cybersecurity measures.[10] Under the performance-based framework of Security Directive 1580/82-2022-01, TSA identified critical security outcomes that covered parties must achieve. To ensure that these outcomes are met, the directive required 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; 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 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.

---

[10] 88 FR 36921 (June 6, 2023).

In response to the continuing cyber threat to rail infrastructure, the requirements of Security Directive 1580-21-01, Security Directive 1582-21-01, and Security Directive 1580/82-2022-01 have been renewed and extended beyond their original expiration dates by subsequent directives, creating three security directive series (the 1580-21-01 series, the 1582-21-01 series, and 1580/82-2022-01 series). As TSA has renewed these directives series, it has also amended their requirements to strengthen their effectiveness and address emerging cyber threats.

The table below provides a list of each of the security directives within the 1580-21-01, 1582-21-01, and 1580/82-2022-01 series. All of the security directives provided in the table are available online in TSA's Surface Transportation Cybersecurity Toolkit.[11]

Table 1: TSA Security Directives
Applicable to Freight Rail, Passenger Rail, and Rail Transit Systems

Security Directive	Date Issued	Effective Date	Date Ratified by TSOB	Set Expiration Date	Federal Register Notice of Ratification
1580-21-01	Dec. 2, 2021	Dec. 31, 2021	Dec. 29, 2021	Dec. 31, 2022	87 FR 31093
1580-21-01A	Oct. 18, 2022	Oct. 24, 2022	Nov. 16, 2022	Oct. 24, 2023	88 FR 36921
1580-21-01B	Oct. 23, 2023	Oct. 24, 2023	Nov. 22, 2023	Oct. 24, 2024	*Current
1582-21-01	Dec. 2, 2021	Dec. 31, 2021	Dec. 29, 2021	Dec. 31, 2022	87 FR 31093
1582-21-01A	Oct. 18, 2022	Oct. 24, 2022	Nov. 16, 2022	Oct. 24, 2023	88 FR 36921
1582-21-01B	Oct. 23, 2023	Oct. 24, 2023	Nov. 22, 2023	Oct. 24, 2024	*Current
1580/82-2022-01	Oct. 18, 2022	Oct. 24, 2022	Nov. 16, 2022	Oct. 24, 2023	88 FR 36921
1580/82-2022-01A	Oct. 23, 2023	Oct. 24, 2023	Nov. 22, 2023	Oct. 24, 2024	*Current

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

1580/82-2022-01C	Jul. 1, 2024	Jul. 1, 2024	July 29, 2024	May 2, 2025	*Current

C. Security Directive 1580-21-01B and Security Directive 1582-21-01B

In light of the continuing threat, TSA determined that the cybersecurity measures required by the 1580-21-01 and 1582-21-01 security directive series remain necessary to protect the nation's critical rail infrastructure beyond the October 24, 2023, expiration date of Security Directive 1580-21-01A and Security Directive 1582-21-01A. On October 23, 2023, TSA issued Security Directive 1580-21-01B and Security Directive 1582-21-01B, extending the requirements of the 1580-21-01 (applicable to freight rail) and 1582-21-01 (applicable to passenger rail and rail transit systems) security directive series for an additional year. Security Directive 1580-21-01B and Security Directive 1582-21-01B contained minor revisions to provide further clarity regarding the applicability of the directives and their compliance deadlines. Additionally, the directives included revisions to improve the effectiveness of the required Cyber Incident Response Plans (CIRPs) by specifying certain requirements for testing exercises. The directives became effective on October 24, 2023, and expired on October 24, 2024.[12]

D. Security Directive 1580/82-2022-01A

Considering the continuing threat, TSA also determined that the measures required by the 1580/82-2022-01 series remained necessary to protect the Nation's critical rail infrastructure beyond Security Directive 1580/82-2022-01's expiration date of October 24, 2023. On October 23, 2023, TSA issued Security Directive 1580/82-2022-01A, extending the requirements of the 1580/82-2022-01 series for an additional year. The directive became effective on October 24, 2023, and was set to expire on October 24, 2024.

[12] On October 23, 2024, TSA issued Security Directive 1580-21-01C and Security Directive 1582-21-01C. These Security Directives superseded the respective -01B directives. Security Directive 1580-21-01C and Security Directive 1582-21-01C each went into effect on October 24, 2024.

In addition to extending the performance-based requirements of the initial directive in this series, Security Directive 1580/82-2022-01A included revisions to strengthen the effectiveness of these requirements and allow greater ability to respond to changing threats. Specifically, the revisions improved the effectiveness of the requirements related to Cybersecurity Assessment Plans (referred to as Cybersecurity Assessment Programs in prior versions); ensured the provisions related to defining Critical Cyber Systems allow flexibility to respond to emerging and evolving threats; and provided greater clarity regarding the role of "Managed Security Service Providers" and "Authorized Representatives."

E. Security Directive 1580/82-2022-01C

To address ongoing cyber threats to rail transportation infrastructure, TSA determined that further amendments to the 1580/82-2022-01 series were necessary prior to the expiration of Security Directive 1580/82-2022-01A. On July 1, 2024, TSA issued Security Directive 1580/82-2022-01C, revising and extending the requirements of Security Directive 1580/82-2022-01A.[13] The directive became effective on July 1, 2024, 2024, and is set to expire on May 2, 2025.

Security Directive 1580/82-2022-01C specifically requires Positive Train Control (PTC) systems be included in owner/operators' list of Critical Cyber Systems, subjecting them to the applicable performance-based cybersecurity measures. The designation of PTC systems as a Critical Cyber System ensures that PTC systems are protected by the performance-based cybersecurity measures of the Security Directive 1580/82-2022-01 series.

II. TSOB Ratification

[13] TSA first issued these revisions as Security Directive 1580/82-2022-01B on May 1, 2024. Due to two oversights in the original directive that may have created confusion, TSA issued a corrected version of the amended directive (Security Directive 1580/82-2022-01C) on July 1, 2024. TSA sought TSOB review and ratification of the reissued directive, currently in effect.

TSA issued Security Directive 1580-21-01B, Security Directive 1582-21-01B, Security Directive 1580/82-2022-01A, and Security Directive 1580/82-2022-01C 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 when "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 [Transportation Security Oversight Board] or rescinded by the Administrator."[14]

The Transportation Security Oversight Board (TSOB) is 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, and a representative of the National Security Council.[15] Among its statutory duties, the TSOB must "review and ratify or disapprove" security directives issued under 49 U.S.C. 114(*l*)(2) within 30 days of the action's issuance.[16]

Following the issuance of Security Directive 1580-21-01B, Security Directive 1582-21-01B, Security Directive 1580/82-2022-01A, and Security Directive 1580/82-2022-01C, the chair of the TSOB convened the board to review the directives.[17] In reviewing each 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

---

[14] 49 U.S.C. 114(*l*)(2)(B).
[15] 49 U.S.C. 115(a), (b).
[16] 49 U.S.C. 115(c)(1); 49 U.S.C. 114(*l*)(2)(B).
[17] 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.

their 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 1580-21-01B, Security Directive 1582-21-01B, and Security Directive 1580/82-2022-01A on November 22, 2023; and ratified Security Directive 1580/82-2022-01C on July 29, 2024. The TSOB also authorized TSA to extend each of the security directives beyond their current 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. 2025-01422 Filed: 1/16/2025 4:15 pm; Publication Date: 1/21/2025]