[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: DHS is publishing official notification that the Transportation Security Oversight Board (TSOB) has ratified Transportation Security Administration (TSA) Security Directive 1580-21-01A, Security Directive 1582-21-01A, and Security Directive 1580/82-2022-01 applicable to owners and operators of critical railroad infrastructure (owner/operators). Security Directive 1580-21-01A and Security Directive 1582-21-01A amend and extend previously ratified security directives issued to critical rail entities to maintain the cybersecurity measures required by those directives. Security Directive 1580/82-2022-01 requires owner/operators to implement performance-based cybersecurity measures necessary to prevent the disruption and degradation of critical rail infrastructure.

DATES: The TSOB ratified Security Directive 1580-21-01A, Security Directive 1582-21-01A, and Security Directive 1580/82-2022-01 on November 16, 2022.

FOR FURTHER INFORMATION CONTACT: Thomas McDermott, Acting 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, including freight and passenger rail, remains elevated and poses a risk to the national and economic security of the United States. Malicious actors have increasingly demonstrated the capability to conduct cyber-attacks exploiting the vulnerabilities of the Internet-accessible Operational Technology (OT) assets and Information Technology (IT) systems of the surface transportation sector. In recent years, cyber attackers have maliciously targeted surface transportation modes in the U.S., including freight railroads, passenger railroads, and rail transit systems, with multiple cyberattack and cyber espionage campaigns.[1] By targeting the integrated cyber and physical infrastructure of surface transportation entities, these actions threaten the safe, secure, and uninterrupted daily operation of surface transportation systems relied upon by the U.S. economy with potential to cause nation-wide impact.

The cyber threat posed by both criminal enterprises and nation-state actors continues to expand and become more complex. Ransomware tactics and techniques continue to evolve, exhibiting threat actors' growing technological sophistication and an increased ransomware threat to organizations globally.[2] The intelligence community has assessed that both the People's Republic of China and the Russian Federation have the capability to target critical infrastructure with cyber operations.[3] In particular, the

---

[1] These activities include 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; the December 2020 "Sunburst" attack on transit agencies; the August 2020 attack on the Southeastern Pennsylvania Transportation Authority; the 2017 ransomware attack on the Sacramento Regional Transit District; and the November 2016 ransomware attack on the San Francisco Municipal Transportation agency. This threat is ongoing: on November 17, 2021 the Federal Bureau of Investigation, the Cybersecurity and Infrastructure Security Agency (CISA), the Australian Cyber Security Centre, and the United Kingdom's National Cyber Security Centre issued a joint cybersecurity advisory highlighting ongoing malicious cyber activity by an advanced persistent threat group (APT) that these agencies associated with the government of Iran. The advisory states that "The Iranian government-sponsored APT actors are actively targeting a broad range of victims across multiple U.S. critical infrastructure sectors, including the Transportation Sector and the Healthcare and Public Health Sector, as well as Australian organizations." Alert AA21-321A (November 17, 2021).

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

[3] Annual Threat Assessment of the U.S. Intelligence Community, Office of the Director of National Intelligence, 8, 12 (February 2022).

intelligence assessment is that China presents the most active and persistent cyber threat to the U.S. with the capability to launch attacks that would disrupt critical rail systems.[4]

In 2022, the threat was heightened further in light of the Russian Federation's attack on Ukraine.[5] Throughout the ongoing Russia-Ukraine conflict there has been an increase in activity by politically or ideologically-motivated cyber groups and criminal cyber groups, who may act independently and without official support from a nation-state government, to target critical infrastructure, including the transportation sector.[6] Illustrating the threat, on March 24, 2022, the U.S. Department of Justice unsealed indictments of three Russian Federal Security Service (FSB) officers and employees of a State Research Center of the Russian Federation FGUP Central Scientific Research Institute of Chemistry and Mechanics (also known as "TsNIIKhM") for their involvement in intrusion campaigns against U.S. and international oil refineries, nuclear facilities, and energy companies. Documents revealed that the FSB conducted a multi-stage campaign in which they gained remote access to U.S. and international energy sector networks, deployed industrial control systems (ICS)-focused malware, and collected and exfiltrated enterprise and ICS-related data.[7] Since April 15, 2022, a pro-Russian hacking group known as "Killnet" has targeted a number of transportation entities, including U.S. and European airports and a U.S. oil and natural gas company. Killnet claimed responsibility for an October 10, 2022, cyber incident targeting the

---

[4] *Id*. at 12.
[5] Joint Cybersecurity Alert – Alert (AA22-011A), *Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure*, released by CISA, the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA) on January 11, 2022 (as revised); 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).
[6] 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).
[7] Press Release 22-285, *Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide*, Department of Justice, issued on March 24, 2022, available at https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical.

public-facing website of 48 airports across the United States, resulting in a number of these websites being unavailable for a period of time.

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

To counter the threat to critical rail infrastructure, on December 2, 2021, TSA issued Security Directive 1580-21-01 and Security Directive 1582-21-01. These two materially identical security directives—one applicable to specified freight railroad carriers and the other applicable to specified passenger railroad carriers and rail transit systems—required covered owner/operators to implement the following four measures:

- Designate a Cybersecurity Coordinator who is required to be available to TSA and CISA at all times (all hours/all days) to coordinate implementation of cybersecurity practices, manage cybersecurity incidents, and serve as a principal point of contact with TSA and CISA for cybersecurity-related matters;
- Report cybersecurity incidents to CISA;
- Conduct a Cybersecurity Vulnerability Assessment to identify gaps in current cybersecurity measures, identify remediation measures, and develop a plan for the owner/operator to implement the remediation measures to address any identified vulnerabilities and gaps; and
- Develop a Cybersecurity Incident Response Plan to reduce the risk of operational disruption should their Information and/or Operational Technology systems be affected by a cybersecurity incident.

These directives became effective on December 31, 2021 and were set to expire on December 31, 2022. The TSOB ratified both directives on December 29. 2021.[8]

In light of the continuing and evolving threat to critical rail infrastructure, as reflected in recent and ongoing intelligence, TSA determined that it remains necessary for owner/operators of the most critical rail entities to implement cybersecurity measures

[8] *See* 87 FR 31093 (May 23, 2022).

to prevent disruption and degradation to their infrastructure. TSA issued Security Directive 1580-21-01A and Security Directive 1582-21-01A on October 18, 2022 to extend the expiration date for the initial requirements from December 31, 2022 to October 24, 2023. The directives are available online in TSA's Surface Transportation Cybersecurity Toolkit.[9]

The amended directives contain two additional changes from the original directives. First, both amended directives modify the requirement to develop a Cybersecurity Incident Response Plan to require covered entities to continuously update and maintain these plans, once developed. The original directive only required owner/operators to develop a plan by a specific date, but did not provide for ongoing updating and maintenance. Second, Security Directive 1580-21-01A, which applies to freight railroads, broadens the entities covered by the directive to include a small number of additional owner/operators designated and notified by TSA based on a risk determination. Security Directive 1580-21-01A and Security Directive 1582-21-01A became effective on October 24, 2022 and are set to expire on October 24, 2023.

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

Along with extending the requirements of the previously issued security directives, as amended, TSA determined that additional cybersecurity measures must be implemented due to the extent of the threat reflected by current intelligence. Security Directive 1580/82-2022-01, also issued on October 18, 2022, requires owner/operators to implement additional performance-based cybersecurity measures to prevent disruption and degradation to their critical cyber systems. This approach ensures that the mandated critical security outcomes are achieved while allowing covered owner/operators options

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

to implement security measures for their specific systems and operations. The directive became effective on October 24, 2022, and is set to expire on October 24, 2023.

The performance-based cybersecurity measures required by Security Directive 1580/82-22-01 closely model those required by Security Directive Pipeline-2021-02C[10] issued on July 21, 2022 to owner/operators of critical oil and natural gas pipelines. This framework enhances security by allowing owner/operators to choose the most appropriate methods to protect their specific systems, while mandating that certain security outcomes are achieved. It also provides owner/operators the ability to be agile and adaptive in leveraging innovative technologies in a changing threat environment.

Security Directive 1580/82-2022-01 identifies four critical security outcomes that covered owner/operators would be required to achieve:

- Implement network segmentation policies and controls to ensure that the Operational Technology (OT) system can continue to safely operate in the event that an Information Technology (IT) system has been compromised;
- Implement access control measures to secure and prevent unauthorized access to critical cyber systems;
- Implement continuous monitoring and detection policies and procedures to detect cybersecurity threats and correct anomalies that affect critical cyber system operations; and
- Reduce the risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers,

[10] Security Directive Pipeline-2021-02C replaced an earlier security directive (Security Directive Pipeline-2021-02) issued to critical pipeline entities on July 26, 2021, which required owner/operators to implement more prescriptive cybersecurity measures. Security Directive Pipeline-2021-02C maintained the security objectives of the previous directive but implemented them through performance-based standards rather than requiring prescriptive specific measures. Cybersecurity experts from TSA and the CISA contributed to the development of the requirements and performance-based standards in Security Directive Pipeline-2021-02C to ensure the efficacy of the requirements in mitigating vulnerabilities. The revised directive also reflected input from stakeholders and general congressional support for a transition to this performance-based, security outcome-focused model.

and firmware on critical cyber systems in a timely manner using a risk-based methodology.

For each of these performance outcomes, the directive includes specific issues that must be addressed and provides options for achieving the required outcomes.

To ensure that the critical security outcomes identified are achieved under this performance-based framework, Security Directive 1580/82-2022-01 requires that owner/operators:

- Establish and implement a TSA-approved Cybersecurity Implementation Plan that describes the specific cybersecurity measures employed and the schedule for achieving the security outcomes identified; and
- 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.[11]

Security Directive 1580/82-2022-01 applies to the same TSA-designated higher risk rail entities covered by Security Directive 1580-21-01A and Security Directive 1582-21-01A,[12] including the small number of additional railroads that Security Directive 1580-21-01A was broadened to include. The covered entities are those that the nation depends on to move passengers and transport freight in support of critical sectors, including national defense. Security Directive 1580/82-2022-01 is available online in TSA's Surface Transportation Cybersecurity Toolkit.[13]

---

[11] Security Directive Pipeline-2021-02C also required owner/operators of critical pipeline entities to 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, in the event of cybersecurity incident. Security Directive 1580/82-2022-01 does not contain this requirement because covered owner/operators must maintain an up-to-date Cybersecurity Incident Response Plan under amended Security Directive 1580-21-01A and Security Directive 1582-21-01A.

[12] *See* 49 CFR §§ 1580.101 and 1582.101.

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

II. TSOB Ratification

TSA has broad statutory responsibility and authority to safeguard the nation's transportation system.[14] 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, and a representative of the National Security Council—reviews certain TSA regulations and security directives consistent with law.[15] TSA issued each of these security directives under 49 U.S.C. 114(*l*)(2)(A), which authorizes TSA to issue emergency regulations or security directives without providing notice or 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."[16]

Following the issuance of Security Directive 1580-21-01A, Security Directive 1582-21-01, and Security Directive 1580/82-2022-01 on October 18, 2022, the chairman of the TSOB convened the board for the purpose of reviewing each directive. In reviewing Security Directive 1580-21-01A, Security Directive 1582-21-01, the TSOB considered the need for owner/operators to maintain the cybersecurity measures required by the amended directives. In reviewing Security Directive 1580/82-2022-01, the TSOB considered its performance-based requirements, including the security outcomes that covered owner/operators must achieve. For all of the directives, the TSOB reviewed the need for TSA to issue the security directives pursuant to its emergency authority under 49 U.S.C. § 114(/)(2)(A) to require necessary cybersecurity measures in order to prevent the

---

[14] *See, e.g.*, 49 U.S.C. 114(d), (f), (*l*), (m).
[15] *See, e.g.*, 49 U.S.C. 115; 49 U.S.C. 114(*l*)(2)(B).
[16] 49 U.S.C. 114(*l*)(2)(B).

disruption and degradation of the country's critical rail infrastructure. The TSOB also considered whether to authorize TSA to extend the security directives beyond their current expiration date of October 24, 2023, 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 1580-21-01A, Security Directive 1582-21-01, and Security Directive 1580/82-2022-01 on November 16, 2022. The TSOB also authorized TSA to extend each of the security directives beyond their current expiration date, 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 directives other than an extended expiration date; (2) the TSA Administrator makes an affirmative determination that conditions warrant the extension of the directives' requirements; and (3) the TSA Administrator documents such a determination and notifies the TSOB.

John K. Tien

Deputy Secretary of Homeland Security & Chairman of the Transportation Security Oversight Board.

[FR Doc. 2023-11942 Filed: 6/5/2023 8:45 am; Publication Date: 6/6/2023]