Rules and Regulations

Federal Register
Vol. 88, No. 108
Tuesday, June 6, 2023

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 Pipeline–2021–01B and Security Directive Pipeline–2021–02C applicable to owners and operators of critical oil and natural gas pipeline infrastructure (owner/operators). Security Directive Pipeline–2021–01B extended the expiration date of cybersecurity measures initially required by Security Directive Pipeline–2021–01, issued on May 27, 2022, for an additional year. Security Directive Pipeline–2021–02C revised the cybersecurity measures originally required by Security Directive Pipeline–2021–02, issued on July 19, 2021, to be more performance-based and less prescriptive than the original requirements. This performance-based approach ensures the mandated critical security outcomes are achieved while allowing covered owner/operators options to implement security measures for their specific systems and operations.

DATES: The TSOB ratified Security Directive Pipeline–2021–01B on June 24, 2021 and ratified Security Directive Pipeline–2021–02C on August 19, 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 pipelines, has remained elevated since the ransomware attack on the Colonial Pipeline Company on May 8, 2021. That attack temporarily disrupted critical supplies of gasoline and other refined petroleum products throughout the East Coast and demonstrated the significant threat such attacks pose to the country's infrastructure and economic well-being. 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.[1] 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.[2]

In 2022, the threat was heightened further in light of the Russian Federation's attack on Ukraine.[3] 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. 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.[4] 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 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 Pipeline–2021–01B

On May 27, 2021, TSA issued Security Directive Pipeline–2021–01, which was the first of two security directives issued by TSA to enhance the cybersecurity of critical pipeline systems in response to the attack on Colonial Pipeline. Security Directive Pipeline–2021–01, and the subsequent amendments in this series, required covered owner/operators to: (1) report cybersecurity incidents to CISA; (2) appoint a cybersecurity coordinator to be available 24/7 to coordinate with TSA and CISA; and (3) conduct a self-assessment of cybersecurity practices, identify any gaps, and develop a plan and timeline for remediation.[5] This first security directive went into effect on May 28, 2021 and was ratified by the TSOB on July 3, 2021.[6]

On December 1, 2021, TSA amended Security Directive Pipeline–2021–01 to update the definition of cybersecurity incident to ensure the consistent identification of incidents that must be reported to CISA across all modes of

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

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

[3] 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).

[4] 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.*

[5] Security Directive Pipeline–2021–01: Enhancing Pipeline Cybersecurity.

[6] *See* 86 FR 38209 (July 20, 2021).

transportation.[7] This amended directive, Security Directive Pipeline–2021–01A, was ratified by the TSOB on December 29, 2021.[8]

In light of the continuing and evolving threat, as reflected in recent and ongoing intelligence, TSA determined that the measures required by the Security Directive Pipeline–2021–01 series remain necessary to protect the Nation's critical pipeline infrastructure beyond Security Directive Pipeline–2021–01A's expiration date of May 28, 2022. On May 27, 2022, TSA issued Security Directive Pipeline–2021–01B to extend the requirements of Security Directive Pipeline–2021–01A for an additional year. Security Directive Pipeline–2021–01B became effective May 29, 2022 and expires on May 29, 2023. Security Directive Pipeline 2021–01B is available online in TSA's Surface Transportation Cybersecurity Toolkit.[9]

The only substantive change in Security Directive Pipeline–2021–01B to the prior requirements is an increase in the amount of time covered entities have to report cybersecurity incidents 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. TSA reached the determination to extend the reporting deadline to 24 hours following engagement with industry stakeholders and in consultation with CISA.

C. Security Directive Pipeline–2021–02C

Due to the extent of the threat to pipeline cybersecurity reflected by intelligence, and the need for widespread best practices to be mandated within the industry, TSA issued Security Directive Pipeline–2021–02 on July 19, 2021. This directive required owner/operators to implement additional cybersecurity measures to prevent disruption and degradation to their infrastructure in response to the ongoing threat. Specifically, Security Directive Pipeline–2021–02, which became effective on July 26, 2021, and was set to expire on July 26, 2022, required owner/operators to take the following additional actions:

- Implement an array of specified mitigation measures to reduce the risk of compromise from a cyberattack;
- Develop a Cybersecurity Contingency/Response Plan to reduce the risk of operational disruption or functional degradation of information technology and operational technology systems in the event of a malicious cyber intrusion; and
- Test the effectiveness their cybersecurity practices through an annual cybersecurity architecture design review conducted by a third party.

Security Directive Pipeline–2021–02 was ratified by the TSOB on August 17, 2021.[10]

On December 17, 2021, TSA issued Security Directive Pipeline–2021–02B, amending Security Directive Pipeline–2021–02 in response to industry input. Specifically, the amended directive revised the time limits for owner/operators to install security software updates and patches for operating systems, applications, drivers, and firmware on Information Technology systems. The TSOB ratified Security Directive Pipeline–2021–02B on January 13, 2022.[11]

In response to the persistent threat to critical oil and natural gas pipelines, TSA determined that it remains necessary for owner/operators of the most critical oil and natural pipelines to implement and maintain cybersecurity measures to prevent disruption and degradation to their infrastructure. On July 21, 2022, TSA issued Security Directive Pipeline–2021–02C requiring owner/operators of the most critical oil and natural gas pipelines to continue to implement necessary cybersecurity measures. The directive became effective on July 27, 2022, and is set to expire on July 27, 2023.

In order to best achieve the critical security outcomes necessary to counter the threat, Security Directive Pipeline–2021–02C transitioned the original requirements to a performance-based model. The directive maintains the security objectives of the previous versions, but implements them through performance-based standards rather than requiring specific prescriptive measures. This approach enhances security by allowing owner/operators to choose the most appropriate cybersecurity measures to protect their specific systems, while mandating that certain security outcomes are achieved. It also provides owner/operators greater ability to be agile and adaptive in leveraging innovative technologies in a changing threat environment.

Security Directive Pipeline–2021–02C identifies four critical security outcomes that covered entities are 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 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 Pipeline–2021–02C 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;
- 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 on necessary capacity, 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 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.

Cybersecurity experts from TSA and the Cybersecurity and Infrastructure Security Agency (CISA) contributed to the development of the requirements and performance-based standards in Security Directive Pipeline–2021–02C to

[7] To counter the persistent and growing cyber threat to critical transportation infrastructure, TSA took action over the course of 2021 to require entities across the modes of transportation regulated by TSA to institute the same critical measures Security Directive Pipeline–2021–01 required in the pipeline context. To date, TSA has issued security directives to high-risk freight railroad carriers, passenger railroad carriers, and rail transit systems and, in the aviation sector, issued security program amendments to airports and aircraft operators.

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

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

[10] *See* 86 FR 52953 (September 24, 2021).

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

ensure the efficacy of the requirements in mitigating vulnerabilities. The directive also reflects input from stakeholders and for a transition to a performance-based, security outcome-focused model. Security Directive Pipeline–2021–02C is available online in TSA's Surface Transportation Cybersecurity Toolkit.[12]

II. TSOB Ratification

TSA has broad statutory responsibility and authority to safeguard the nation's transportation system.[13] 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.[14] TSA issued both 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.'' [15]

Following the issuance of Security Directive Pipeline–2021–01B on May 27, 2022, the chairman of the TSOB convened the board for the purpose of reviewing the directive. In reviewing Security Directive Pipeline–2021–01B, the TSOB considered the continuing need for TSA to maintain the directive's requirements pursuant to its emergency authority under 49 U.S.C. 114(*1*)(2) to prevent the disruption and degradation of the country's critical transportation infrastructure and the change in the deadline for reporting cybersecurity incidents to CISA from 12 hours to 24 hours. Following its review, the TSOB ratified Security Directive Pipeline–2021–01B on June 24, 2022.

Following the issuance of Security Directive Pipeline–2021–02C on July 21, 2022, the chairman again convened the board for the purpose of reviewing that directive. In reviewing Security Directive Pipeline–2021–02C, the TSOB considered its transition to a performance-based approach to requiring owner/operators of critical oil and natural gas pipelines to address persistent and evolving cyber threats that threaten the country's critical pipeline infrastructure as well as the need for TSA to issue the directive's requirements using its emergency authority under 49 U.S.C. ll4(*l*)(2)(A). The TSOB also considered whether to authorize TSA to extend the security directive beyond its current expiration date of July 27, 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 Pipeline–2021–02C on August 19, 2022. The TSOB also authorized TSA to extend the security directive beyond its 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 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.

John K. Tien,

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

[FR Doc. 2023–11941 Filed 6–5–23; 8:45 am]

BILLING CODE 9110–9M–P

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

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

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

[15] 49 U.S.C. 114(*l*)(2)(B).

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

[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

Continued