Rules and Regulations

Federal Register

Vol. 89, No. 77

Friday, April 19, 2024

DEPARTMENT OF HOMELAND SECURITY

6 CFR Chapter I

49 CFR Chapter XII

Recommendation Regarding Emergency Action in Aviation

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

ACTION: Notice.

SUMMARY: DHS is publishing official notice that the Transportation Security Oversight Board (TSOB) has recommended to the Transportation Security Administration (TSA) that a cybersecurity emergency exists that warrants TSA's determination to expedite the implementation of critical cyber mitigation measures through the exercise of emergency regulatory authority.

DATES: The TSOB provided this recommendation on April 20, 2023.

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

On March 7, 2023, TSA issued Joint Emergency Amendment (EA) 23–01 [1] to certain aviation stakeholders to address the significant cybersecurity threat to the aviation system, evidenced by recent incidents and intelligence. Joint EA 23–01 is part of TSA's and the Government's, more broadly, ongoing plans and efforts to rapidly increase the cybersecurity resilience of critical transportation infrastructure. TSA determined that proceeding with immediate action was warranted under the circumstances to ensure timely implementation of critical mitigation measures by higher risk regulated entities. Joint EA 23–01 amends the security programs [2] for covered owners/operators to require performance-based cybersecurity measures intended to prevent the disruption and degradation of their critical systems. Joint EA 23–01's requirements are similar to performance-based requirements that TSA has already issued to critical pipeline and rail entities.[3]

II. TSOB Recommendation

The TSOB was created by the Aviation and Transportation Security Act (ATSA) to provide guidance regarding transportation security-related matters. TSOB members include the Secretaries of Homeland Security, Transportation, Defense, and the Treasury, the Attorney General, the Director of National Intelligence, or their designees, and one member appointed by the President to represent the National Security Council. The Secretary of Homeland Security serves in the role of TSOB chairman, which has been further delegated within the Department to the Deputy Secretary.[4] As part of its statutory duties, the TSOB is authorized to review plans for transportation security and make recommendations to the TSA Administrator regarding those plans.[5]

Following the issuance of Joint EA 23–01, TSA sought the TSOB's discretionary review under 49 U.S.C. 115(c)(5) and (6) regarding whether a cybersecurity emergency exists that warrants TSA's determination to expedite the implementation of critical cyber mitigation measures through the exercise of its emergency regulatory authority, under which the EA was issued.[6] TSA sought the TSOB's perspective and guidance given the TSOB's role in ratifying TSA's emergency cybersecurity actions applicable in the pipeline and rail sectors as well as the context of the coordinated efforts across the Government to counter the continuing and serious cyber threats.

Under the authority of 49 U.S.C. 115(c)(5) and (6), the chairman of the TSOB convened a meeting of the Board to review TSA's transportation security plans for cybersecurity in the aviation sector and provide a recommendation regarding whether a cybersecurity emergency exists that warrants TSA's determination to expedite the implementation of critical cyber mitigation measures by exercising its emergency regulatory authority to issue Joint EA 23–01. Representatives from the White House Office of the National Cyber Director, the Department of Defense's United States Transportation Command, DHS's Cybersecurity and Infrastructure Security Agency, and the Federal Aviation Administration, as well as the Deputy National Security Advisor for Cyber and Emerging Technology at NSC were also invited to participate in the meeting given their relevant expertise.

During the meeting, the TSOB was briefed on the cyber threat to the aviation transportation system and on TSA's effort to mitigate the threat through Joint EA 23–01. The briefing included presentation of sensitive security information and classified information. Following the briefing, the TSOB discussed the circumstances precipitating TSA's issuance of Joint EA 23–01, including relevant events and intelligence presented during the briefing. At the meeting's conclusion, the TSOB recommended that a cybersecurity emergency exists that warrants TSA's determination to expedite the implementation of a critical cyber mitigation measures through the exercise of its emergency regulatory authority to issue Joint EA 23–01. This action reinforced the need for TSA to proceed with critical

[1] EA 23–01 is Sensitive Security Information (SSI). *See* 49 CFR 1520.5(b).

[2] Under TSA regulations, airport and aircraft operators must adopt and carry out a security program approved by TSA that provides for the safety and security of persons and property engaged in air transportation. 49 CFR part 1542, subpart B; 49 CFR part 1544, subpart B.

[3] The TSOB reviewed and ratified TSA's security directives mandating performance-based cybersecurity requirements in the pipeline and rail sectors. 88 FR 36919; 88 FR 36921.

[4] 49 U.S.C. 115(a), (b)(1), (b)(2), and (c).

[5] 49 U.S.C. 115(c)(5)–(6).

[6] Certain TSA actions issued pursuant to statutory emergency authority, like the security directives mandating cybersecurity measures in the pipeline and rail sectors, must be ratified by the TSOB to remain effective beyond 90 days. 49 U.S.C. 114(*l*)(2)(B). Unlike those directives, EA 23–01 was issued under separate TSA regulatory authority, 49 CFR 1542.105(d); 49 CFR 1544.105(d), which does not require TSOB ratification.

mitigation measures on an emergency basis.

Kristie Canegallo,

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

[FR Doc. 2024–08394 Filed 4–18–24; 8:45 am]

BILLING CODE 9110–9M–P

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–2021–01C and Security Directive Pipeline–2021–02D, applicable to owners and operators of critical hazardous liquid and natural gas pipeline infrastructure (owner/operators). Security Directive Pipeline–2021–01C, issued on May 22, 2023, extended the requirements of the Security Directive Pipeline-2021–01 series for an additional year. Security Directive Pipeline–2021–02D, issued on July 26, 2023, extended the requirements of the Security Directive Pipeline–2021–02 series for an additional year and amended them to strengthen their effectiveness and address emerging cyber threats.

DATES: The TSOB ratified Security Directive Pipeline–2021–01C on June 21, 2023, and Security Directive Pipeline–2021–02D on August 24, 2023.

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 directive (Security Directive Pipeline–2021–01) in response to the Colonial Pipeline incident. Cyber threats to surface transportation systems, including pipelines, continue to proliferate, as both nation-states and criminal cyber groups continue to target critical infrastructure in order to cause operational disruption and economic harm.[1] 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.[2] Particularly in light of the ongoing Russia-Ukraine conflict,[3] these threats remain elevated and pose a risk to the national and economic security of the United States.

B. Security Directive Pipeline–2021–01C

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 Colonial Pipeline attack on May 7, 2021. 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.[4] This first security directive went into effect on May 28, 2021, was ratified by the TSOB on July 3, 2021, and was set to expire on May 28, 2022.[5]

On December 2, 2021, TSA issued Security Directive Pipeline–2021–01A, amending Security Directive Pipeline–2021–01, to update the definition of cybersecurity incident covered by the directive's reporting requirement and align it with the definition applicable to the other modes.[6] The TSOB ratified Security Directive Pipeline–2021–01A on December 29, 2021.[7] Security Directive Pipeline–2021–01, as amended by Security Directive Pipeline–2021–01A, was set to expire 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.[8] Security Directive Pipeline–2021–01B became effective May 29, 2022 and was set to expire on May 29, 2023. The TSOB ratified Security Directive Pipeline–2021–01B on June 24, 2021.[9]

In light of the continuing threat, TSA determined that the measures required by the Security Directive Pipeline–2021–01, as amended and extended by Security Directive Pipeline–2021–01A and Security Directive Pipeline–2021–01B, remain necessary to protect the Nation's critical pipeline infrastructure beyond Security Directive Pipeline–2021–01B's expiration date of May 29, 2023. On May 22, 2023, TSA issued Security Directive Pipeline–2021–01C to extend the requirements of Security Directive Pipeline–2021–01B for an additional year. Security Directive Pipeline–2021–01C became effective May 29, 2023 and expires on May 29, 2024. Security Directive Pipeline–2021–01C contains no substantive changes from Security Directive Pipeline–2021–01B. Security Directive Pipeline–2021–01C is available online in TSA's Surface Transportation Cybersecurity Toolkit.[10]

C. Security Directive Pipeline–2021–02D

On July 19, 2021, TSA issued Security Directive Pipeline-2021–02, the second security directive TSA issued in response to the attack on Colonial Pipeline. This directive required owner/operators to implement additional

[1] Annual Threat Assessment of the U.S. Intelligence Community, Office of the Director of National Intelligence, 10, 15 (February 2023); Press Release 23–530, *Justice Department Announces Court-Authorized Disruption of Snake Malware Network Controlled by Russia's Federal Security Service,* Department of Justice, issued on May 9, 2023, available at *https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-snake-malware-network-controlled;* Joint Cybersecurity Advisory (AA23–144a), *People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection,* released by CISA on May 24, 2023.

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

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

[5] 86 FR 38209.

[6] During TSA's development of cybersecurity actions applicable to other transportation modes, TSA made a determination to modify the definition of cybersecurity incident it had used in the first security directive following industry input and consultation with DHS cybersecurity experts.

[7] 87 FR 31093.

[8] 88 FR 36919. 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.

[9] *Id.*

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