DEPARTMENT OF HOMELAND SECURITY

6 CFR Chapter I

49 CFR Chapter XII

[DHS Docket No. DHS–2021–0039]

Ratification of Security Directive

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

ACTION: Notification of ratification of directive.

SUMMARY: DHS is publishing official notice that the Transportation Security Oversight Board (TSOB) has ratified Transportation Security Administration (TSA) Security Directive Pipeline–2021–02, which is applicable to certain owners and operators of critical pipeline systems and facilities (Owner/Operators) and requires implementation of an array of cybersecurity measures to prevent disruption and degradation to their infrastructure.

DATES: The ratification was executed on August 17, 2021, and took effect on that date.

FOR FURTHER INFORMATION CONTACT: Thomas McDermott, Deputy Assistant Secretary, Cyber Policy, Office of Strategy, Policy, and Plans at 202–834–5803 or *thomas.mcDermott@HQ.DHS.GOV.*

SUPPLEMENTARY INFORMATION:

I. Background

A. Ransomware Attack on the Colonial Pipeline Company and TSA Security Directive Pipeline–2021–01

On May 8, 2021, the Colonial Pipeline Company announced that it had halted its pipeline operations due to a ransomware attack. This 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. In response, TSA issued Security Directive Pipeline–2021–01 on May 26, 2021, which required Owner/Operators to: (1) Report cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency (CISA) within 12 hours; (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.[1] As ratified by the TSOB on July 3, 2021, this first security directive became effective on May 28, 2021, and is set to expire on May 28, 2022.[2]

B. TSA Security Directive Pipeline–2021–02

Due to a continuing active threat to pipeline cybersecurity, TSA issued Security Directive Pipeline–2021–02 on July 19, 2021, which requires Owner/Operators to implement additional and immediately needed cybersecurity measures to prevent disruption and degradation to their infrastructure in response to an ongoing threat. Specifically, Security Directive Pipeline-2021–02 requires Owner/Operators to take the following additional actions:

- Implement specified mitigation measures to reduce the risk of compromise from a cyberattack, drawing on guidelines published by the National Institute of Standards and Technology (NIST) and recommendations from CISA as reflected in a series of recent alerts; [3]
- 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.

TSA issued this Security Directive pursuant to its authority under 49 U.S.C. 114(*l*)(2), which authorizes TSA to issue emergency security directives without providing notice or an opportunity for public comment when the TSA Administrator ''determines that a . . . security directive must be issued immediately in order to protect transportation security . . . ''. Each of the measures have been carefully evaluated and determined critical to protect this critical sector in light of the current threat. The directive became effective on July 26, 2021, and expires on July 26, 2022.

II. TSOB Ratification

TSA has broad statutory responsibility and authority to safeguard the nation's transportation system, including pipelines.[4] 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 regulations and security directives consistent with law.[5] 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.'' [6]

On August 4, 2021, the chairman of the TSOB convened an in-person a meeting of the Board for the purpose of reviewing the security directive. At the meeting, the TSOB discussed the threat to the cybersecurity of the pipeline industry, the actions required by Security Directive Pipeline-2021–02, and the need for TSA to issue the security directive pursuant to its emergency authority under 49 U.S.C. 114(*l*)(2) to prevent the disruption and degradation of the country's critical pipeline infrastructure. There was unanimous consensus that the Security Directive should be in place. Following this review, on August 17, 2021, the TSOB ratified Security Directive–2021–02 in its entirety.

John K. Tien,

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

[FR Doc. 2021–20738 Filed 9–23–21; 8:45 am]

BILLING CODE 9110–9M–P

[1] *See* DHS Press Release, DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators (May 27, 2021), available at: *https://www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators* (accessed Aug. 27, 2021).

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

[3] *See, e.g.,* Joint Cybersecurity Advisory—Alert (AA21–131A), *Darkside Ransomware: Best Practices for Preventing Disruption from Ransomware Attacks,* released by CISA and the Federal Bureau of Investigation (FBI) on May 11, 2021 (as revised); and Alert (AA21–201A), *Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013),* released by CISA and the FBI on July 20, 2021 (as revised).

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

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

[6] 49 U.S.C. 114(*l*)(2)(B).