U.S. Department of Homeland Security
Transportation Security Administration
6595 Springfield Center Drive
Springfield, Virginia 20598

ACTION

MEMORANDUM FOR: Dominic Mancini
Deputy Administrator
Office of Information and Regulatory Affairs (OIRA)
Office of Management and Budget (OMB)

THROUGH: Eric Hysen
Chief Information Officer,
Department of Homeland Security

ERIC N HYSEN
Digitally signed by ERIC N HYSEN
Date: 2022.10.26 08:53:58 -04'00'

FROM: Opeyemi Oshinnaiye
Assistant Administrator
Chief Information Officer
Authorizing Official
Office of Information Technology
Transportation Security Administration (TSA)

OPEYEMI B OSHINNAIYE
Digitally signed by OPEYEMI B OSHINNAIYE
Date: 2022.10.21 14:31:34 -04'00'

SUBJECT: Emergency Information Collection Request: Revision Cybersecurity Measures for Surface Modes (1652-0074)

Purpose

This memorandum seeks the Office of Management and Budget (OMB) approval of the Transportation Security Administration's (TSA's) request for an emergency revision under the Paperwork Reduction Act (PRA) to OMB Control Number 1652-0074, Cybersecurity Measures for Surface Modes, to address cybersecurity risks and the ongoing cybersecurity threat to freight rail and passenger rail systems and associated infrastructure.

To protect against escalating cybersecurity threats, TSA intends to publish a Security Directive (SD) which will be mandatory, titled SD 1580/1582-2022-01 Rail Cybersecurity Mitigation Actions, Contingency Planning, and Testing. The purpose of this SD will be to reduce the vulnerability of critical railroad operations and facilities to cybersecurity threats through implementation of layered cybersecurity measures that provide defense-in-depth. The SD 1580/1582-2022-01 would apply to Owner/Operators of freight and passenger railroads, to include the "Higher Risk" Freight railroads identified in 49 CFR 1580.101 and additional TSA-designated freight and passenger railroads. As this SD requires new information to be submitted to TSA, TSA is requesting emergency approval for a revision of OMB Control Number 1652-0074, Cybersecurity Measures for Surface Modes. TSA would continue to collect information under this

Information Collection Request (ICR) for the previously issued SD-1580-21-01[1], SD -1582-21-01[2] and IC 2021-01[3] issued on December 31, 2021, which remain in effect.

Background

The United States (U.S.) surface transportation system is a complex interconnected and largely open network including freight railroads, public transportation and passenger rail systems, and over-the-road-bus (OTRB) Owner/Operators. Many of these modes employ increasingly integrated cyber and physical systems that operate daily in close coordination with and proximity to each other nationwide. This growing dependence on Operational Technology (OT) and Information Technology (IT) systems and assets puts these operations at risk as malicious cyber actors have demonstrated their willingness to conduct cyber-attacks against critical infrastructure by exploiting the vulnerability of these cyber systems.

In December 2021, OMB issued emergency approval of an ICR for TSA to collect information required by SD-1580-21-01, SD-1582-21-01, and IC 2021-01 in order to address the growing threat to the integrated cyber and physical systems that operate daily in close coordination with and proximity nation-wide, and its uninterrupted secure and safe operation is critical for the U.S. economy. IC 2021-01 is an "information circular (IC)", which contains non-binding recommendations with the same measures for railroad Owner/Operators, public transportation agencies, rail transit system Owner/Operators, and certain OTRB Owner/Operators not specifically covered under SDs 1580-21-01 or 1582-21-02.

TSA's SDs are issued under authority granted by the Aviation and Transportation Security Act (ATSA). Pursuant to ATSA, and delegated authority from the Secretary of Homeland Security, Congress granted the TSA Administrator broad statutory responsibility and authority with respect to the security of the transportation system. *See* 49 U.S.C. § 114(d). Under 49 U.S.C. § 114(f)(3) and (4), TSA may "develop policies, strategies, and plans for dealing with the threats ... including coordinating countermeasures with appropriate departments, agencies, and instrumentalities of the United States." Additionally, TSA may, at the discretion of the Administrator, assist another Federal agency, such as CISA, in carrying out its authority in order to address a threat to transportation.[4] TSA has the authority to issue SDs in order to protect transportation security.

> "Notwithstanding any other provision of law or executive order (including an executive order requiring a cost-benefit analysis), if the Administrator determines that a regulation or security directive must be issued immediately in order to protect transportation security, the Administrator shall issue the regulation or security directive without providing notice or an opportunity for comment and without prior approval of the Secretary." 49 U.S.C. § 114(l)(2).

The SDs and the IC were developed in consultation with the Cybersecurity and Infrastructure Security Agency (CISA) and coordinated with applicable components of the Department of Transportation and Department of Defense.

[1] https://www.tsa.gov/sites/default/files/sd-1580-21-01_signed.pdf

[2] https://www.tsa.gov/sites/default/files/sd-1582-21-01_signed.pdf

[3] https://www.tsa.gov/sites/default/files/20211201_surface-ic-2021-01.pdf

[4] *Id.* §§ 114(m), granting the TSA Administrator the same authority as the FAA Administrator under 49 U.S.C. § 106(m).

Since the issuance of TSA's aforementioned SDs and IC, more information has developed regarding global cybersecurity threats, requiring additional action to ensure the security of U.S. transportation systems. The following highlights some of this new information.

- February 7, 2022: The Office of the Director for National Intelligence released the *Annual Threat Assessment of the U.S. Intelligence Community,* which noted that "China almost certainly is capable of launching cyber-attacks that would disrupt critical infrastructure services within the United States, including against oil and gas freight rail and passenger rails and rail systems."[5]
- April 13, 2022: CISA, FBI, NSA and DOE released Joint Cybersecurity Advisory (AA22-103A), *APT Cyber Tools Targeting ICS/SCADA Devices,* which warned that certain advanced persistent threat (APT) actors have exhibited the capability to gain full system access to multiple industrial control system (ICS)/supervisory control and data acquisition (SCADA) devices.[6]
- On April 20, 2022: CISA, FBI, NSA, and International Partners issued Joint Cybersecurity Advisory (AA 22-110A), *Demonstrated Threats and Capabilities of Russian State-Sponsored and Cyber Criminal Actors.*[7]
- June 7, 2022: CISA and NSA released Joint Cybersecurity Advisory (AA22-158A), *People's Republic of China (PRC) State-Sponsored Cyber Actors Exploit Network Providers and Devices,* which identified the use of publicly known vulnerabilities in order to establish a broad network of compromised infrastructure.[8]

Securing the surface transportation network has become increasingly important to the U.S.
The degradation, destruction, or malfunction of systems that control this infrastructure could cause significant harm to the national and economic security of the U.S. TSA's cybersecurity measures are intended to reduce the vulnerability of IT and OT systems and protect civilian higher-risk infrastructure from being attractive targets for malicious cyber actors or foreign powers attempting to harm U.S. interests or retaliate for perceived U.S. aggression.

To address this threat TSA is issuing an SD that includes the following requirements:

- Implement a TSA-approved Cybersecurity Implementation Plan that describes the specific cybersecurity measures employed by the Owner/Operator and the schedule for achieving the performance outcomes in the SD.
  - Develop 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 and vice versa;
  - Create access control measures to secure and prevent unauthorized access to critical cyber systems;
  - Build 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.
- Annually submit a Cybersecurity Assessment Program to proactively test and regularly audit the effectiveness of cybersecurity measures and identify and resolve device, network and/or system vulnerabilities.

[5] 2022 Annual Threat Assessment of the U.S. Intelligence Community (dni.gov)

[6] https://www.cisa.gov/uscert/ncas/alerts/aa22-103a

[7] https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

[8] https://www.cisa.gov/uscert/ncas/alerts/aa22-158a

- Upon request, provide documentation to establish compliance of records of common IT or OT systems to be reviewed as part of a compliance inspection. In many situations, providing TSA with access to documents and records on site will be sufficient.

Discussion

TSA is addressing this continuous global cyber threat to transportation security and implementing the President's Industrial Control System Cybersecurity Initiative[9] using its ATSA authority. The emergency revision for the SD 1580/1582-2022-01 contains several collections of information to update the current information collection requirements to address emerging cybersecurity concerns. This update requires TSA to request emergency approval for a revision of OMB Control Number 1652-0074, Cybersecurity Measures for Surface Modes[10].

TSA plans to collect the following information:

1) A Cybersecurity Implementation Plan (CIP) submitted to TSA for approval that addresses how the Owner/Operator will achieve each of the following objectives:
   - Identification of the Owner/Operator's Critical Cyber Systems
   - Implementation of network segmentation policies and controls to ensure that the Operational Technology system can continue to safely operate in the event that an Information Technology system has been compromised
   - Implementation of access control measures to secure and prevent unauthorized access to critical cyber systems;
   - Implementation of continuous monitoring and detection policies and procedures to detect cybersecurity threats and correct anomalies that affect Critical Cyber System operations; and;
   - Reduction of 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.

2) 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.

3) Providing documentation as necessary to establish compliance, to be provided to TSA upon request.

The imminent and quickly evolving cybersecurity threats to surface transportation infrastructure necessitate these collections. The information derived from this collection will directly support and facilitate TSA's cybersecurity mission, as well as TSA's responsibility and authority for "security in all modes of

[9] July 28, 2021, the White House issued a National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems stating, "The cybersecurity threats posed to the systems that control and operate the critical infrastructure on which we all depend are among the most significant and growing issues confronting our Nation. The degradation, destruction, or malfunction of systems that control this infrastructure could cause significant harm to the national and economic security of the United States." The President's ICS Cybersecurity Initiative creates a path for Government and industry to collaborate to take immediate action, within their respective spheres of control, to address these serious threats."

[10] The SD-1580-01, SD-1582-01 and IC 2021-01 is being reissued to expand applicability, and is scheduled to expire on September 30, 2023.

transportation … including security responsibilities … over modes of transportation that are exercised by the Department of Transportation." 49 U.S.C. § 114(d).

TSA and federal partner agencies will use the information to respond to and contain emerging cybersecurity threat to make a global assessment of the cyber risk posture of the industry and possibly impose additional security measures as appropriate or necessary. TSA may also use the information, with company-specific data redacted, for TSA's intelligence-derived reports. In addition, TSA and CISA may use information submitted for vulnerability identification, trend analysis, or to generate anonymized indicators of compromise or other cybersecurity products to prevent other cybersecurity incidents. All reported information will be protected in a manner appropriate for the sensitivity and criticality of the information.

Emergency clearance request

Regarding all proposed collections, TSA has explored other options for addressing the existing threat and found it cannot do so without collecting information from covered Owner/Operators. The TSA Administrator has determined that the cybersecurity threat facing the rail industry requires the issuance of a rail SD. This emergency request is based on the information collection requirements in the SD. TSA is pursuing federal cybersecurity rulemaking, but the current threat requires the issuance of this SD. Therefore, TSA is seeking emergency approval of this information collection to require TSA-designated Owner/Operators to comply with the collection requirements discussed above.

Without emergency approval, and instead going through the normal PRA clearance process, TSA will be unable to address this continuous threat of cyberattacks, such as ransomware, to the nation's surface transportation systems. The use of normal PRA clearance procedures is reasonably likely to result in public harm because TSA would not have the foundational cybersecurity posture of the covered Owner/Operators, and thus, hinder TSA's ability to quickly obtain information needed to address imminent, serious, quickly moving and rapidly evolving threats to these systems, which is key to national and economic security and would be impeded if Owner/Operators did not provide the information required by the SD in the near future. In addition, delaying the effective date of the SD would impede the ability of the industry to effectively and efficiently reduce the vulnerability of critical rail operations and facilities to cybersecurity threats, which is fundamental to securing our nation's national and economic security.

It is critical to ensure that SD -1580/1582-2022-01 is issued to address emerging cybersecurity threats. National, state, and other actors with malicious intent could easily take advantage of even a temporary diminution of security that could result without the issuance of this revision. The Department of Homeland Security has determined that it is necessary to mandate these measures on an expedited basis to ensure they are implemented as necessary to protect national security by mitigating the current risk to Rail Owner/Operators from cybersecurity threats. The evolving cybersecurity threats to surface transportation infrastructure necessitate these collections.

Conclusion

As part of the focused and aggressive continuing federal effort to mitigate this continuing cybersecurity threat and reduce the risk across surface transportation, TSA respectfully requests that OMB grant TSA's request for emergency clearance for the revision of TSA's Cybersecurity Surface Mode collection in order to address this emergency need to protect transportation security consistent with TSA's responsibilities and authorities. It is imperative that TSA issue the SD as soon as possible to effectuate these goals.