U.S. Department of Homeland Security
Arlington, VA 20598

Transportation Security Administration

ACTION

MEMORANDUM FOR: Sharon Block
Acting 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: 2021.11.30 09:24:44 -05'00'

FROM: Russell Roberts
Assistant Administrator
Chief Information Officer
Authorizing Official (AO)
Office of Information Technology
Transportation Security Administration (TSA)

RUSSELL A ROBERTS
Digitally signed by RUSSELL A ROBERTS
Date: 2021.11.29 17:04:41 -05'00'

SUBJECT: Emergency Information Collection Request (ICR): Cybersecurity Measures for Surface Modes (1652-NEW)

Purpose

The memorandum seeks the Office of Management and Budget (OMB) approval of the Transportation Security Administration's (TSA's) request for a new OMB control number under the Paperwork Reduction Act (PRA), 1652-NEW, Cybersecurity Measures for Surface Modes. TSA intends to publish Security Directives (SD), which will be mandatory, and Information Circular (IC), which will be non-mandatory recommendations, to various surface transportation mode operators to address the ongoing cybersecurity threat using a risk-based approach to transportation security. The SDs would only apply to "Higher Risk" Railroads and Rail Transit operations and the IC would apply to lower-risk operations to enhance the surface transportation integrated system to include transit bus operations and over-the-road bus (OTRB) owner/operators.[1]

Background

The U.S. surface transportation system is a complex interconnected and largely open network including mass transit systems, passenger and freight railroads, OTRB owner/operators, motor

[1] Agencies that are identified as higher-risk service the regions with the highest surface transportation-specific risk. Risk ranking is based on considerations related to ridership, location of services provided (use of the same stations and stops), and relationship between feeder and primary systems. See https://www.tsa.gov/sites/default/files/guidance-docs/high_threat_urban_area_htua_group_designations_0.pdf

carrier owner/operators, and pipelines. Many of these modes employ increasingly integrated cyber and physical systems that operate daily in close coordination with and proximity to each other nationwide. The uninterrupted secure and safe operation of this interrelated, increasingly cyber-dependent system, is critical for U.S. national, transportation, and economic security.

Earlier this year, OMB approved, two emergency ICR requests from TSA to collect information via similar SDs directed to pipelines in order to address cybersecurity threats. On May 8, 2021, the Colonial Pipeline Company announced that it had halted its pipeline operations due to a ransomware attack. This attack received national attention as it temporarily disrupted critical supplies of gasoline and other refined petroleum products throughout the East Coast. Such attacks pose significant threats to the country's transportation infrastructure and economic security as extensive interdependencies exist among transportation and other critical infrastructure sectors.

During the last few years, cybersecurity incidents affecting surface transportation has become a 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, for example:

- During the Thanksgiving weekend in 2016, the San Francisco Municipal Transportation Agency, sometimes called Muni or SFMTA, was the victim of a ransomware attack that affected internal computer systems including email and ticketing. The attack disrupted ticket-selling systems, causing kiosk screens to display the phrase "You Hacked, ALL Data Encrypted;" the hacker's goal was to extort 100 bitcoins ($73,000) from the SFMTA for the release of its systems.

- A severe cybersecurity attack occurred in 2017 against Sacramento Regional Transit (SaRT) in which SaRT suffered a ransomware attack that crippled its website and destroyed data.

- Another attack on the Southeastern Pennsylvania Transportation Authority occurred in August of 2020 took down its real-time bus and rail information for two full weeks.

- In December 2020, the Sunburst attack on transit agencies is not yet understood, transit agencies have recently been confirmed targets of several other cyberattacks.

- April 2021, Hackers breached several computer systems of the Metropolitan Transportation Authority, the nation's largest mass transit agency that daily carries millions of people in and around New York City. The intrusion was discovered in late April when hackers linked to the Chinese exploited security flaws in Pulse Connect Secure, a VPN that allows employees to connect remotely to their employer's network. The cyberattack impacted three of the transit agency's 18 systems.

- July 2021: A cyberattack began to affect many small and medium-size business across the United States beginning Friday, and the attack was felt in Butte County, specifically on its bus system. The Butte Regional Transit's B-Line bus system serves[2] Chico, Paradise,

[2] http://www.blinetransit.com/Schedules/Bus-Stop-Location-Maps/

Magalia, Oroville, Palermo, Gridley and Biggs. It also has a paratransit offering for those with Americans with Disabilities Act certification or a "dial-a-ride" service for those 70 years and older[3].

- August 14, 2021: Cyberattack on Iran's railroad system last month caused widespread chaos with hundreds of trains delayed or canceled. The message itself was the work of the hackers and, in a sardonic twist, it advised confused travelers to seek more information by calling 64411 (New York Times).

- September 2021: The U.S. Cybersecurity and Infrastructure Security Agency (CISA) issued an alert on the increased use of Conti ransomware in more than 400 attacks on U.S. and international organizations. The alert comes after ransomware attacks on two major farming cooperatives, Crystal Valley Cooperative and New Cooperative — where the hacker asked for $5.9 million in payment.

Malicious cyber actors have demonstrated their willingness to conduct cyber-attacks against critical infrastructure by exploiting the vulnerability of Internet-accessible Operational Technology (OT) and Information Technology (IT) systems and assets. Given the multitude of connected devices already in use by the surface transportation industry and the vast amount of data generated (with more coming online soon), protecting the higher-risk freight rail, passenger rail, and transit industry has become an increasing critically important and complex undertaking to protect critical infrastructure from malicious cyber-attack and other cybersecurity-related threats.

On July 28, 2021, the White House issued a National Security Memorandum (NSM) on Improving Cybersecurity for Critical Infrastructure Control Systems[4] 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 Industrial Control System Cybersecurity (ICS) 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."

TSA is addressing this continuous global threat through its authority under 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." Pursuant to this authority, TSA may, at the discretion of the Administrator, assist another Federal agency, such as CISA, in

[3] https://www.chicoer.com/2021/07/08/butte-county-bus-system-hit-by-weekend-cyberattack/
[4] National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems | The White House

carrying out its authority in order to address a threat to transportation.[5] As noted above, TSA may issue security directives in order to protect transportation security. *See* 49 U.S.C. 114(l)(2).

> 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.

Due to the ongoing cybersecurity threat to surface systems and associated infrastructure, TSA is preparing to issue two new SDs, which are mandatory: SD 1580-2021-01, Enhancing Rail Cybersecurity, and SD 1582-2021-02, Enhancing Public Transportation and Passenger Railroads, to address the threat. These directives were developed in consultation with CISA and coordinated with applicable components of the Department of Transportation. In general, the cybersecurity requirements of the two SDs would apply to Owner/Operators with operations that meet the criteria identified in 49 CFR parts 1580 (Freight Rail), 1582 (Mass Transit and Passenger Rail) required to report security incidents under 49 CFR 1570.203.

In addition, TSA is preparing to issue an IC, which is recommended guidance, IC Surface Transportation IC-2021-01, Enhancing Surface Transportation Cybersecurity. The IC recommendation would apply to owner/operators not specifically covered under Security Directives 1580-2021-01 or 1582-2021-02.

- Each railroad owner/operator identified in 49 CFR 1580.1(a)
- Each passenger railroad, public transportation agency, or rail transit system owner/operator identified in 49 CFR 1582.1
- Each Over-The-Road-Bus owner/operator identified in 49 CFR 1584.1

To protect against the ongoing cybersecurity threat, the two SDs mandate that TSA-specified Owner/Operators of "Higher Risk" Railroads and Rail Transit implement an array of cybersecurity measures to prevent disruption and degradation to their infrastructure. DHS has also determined that the same measures should be provided as recommendations within an IC, which will apply to Owner/Operators of bus systems as they are considered to be lower risk for potential cyber-attacks against their critical infrastructure that would aim to exploit the vulnerability of Internet-accessible OT assets and IT systems.

In order to execute its security responsibilities within the surface transportation industry and its cybersecurity responsibilities, DHS needs to have current awareness of potential security incidents and suspicious activity within the mode. The SDs will require, and in the case of the IC will recommend, railroads Owner/Operators, rail transit system Owner/Operators, and OTRB Owner/Operators to conduct the following security measures:

1. Designate a Cybersecurity Coordinator who is required to be available to TSA 24/7 to coordinate cybersecurity practices and address any incidents that arise.

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

2. Report cybersecurity incidents to CISA.[6]
3. Develop a cybersecurity incident response plan to address cybersecurity gaps.
4. Conduct a cybersecurity vulnerability assessment using the form provided by TSA.

While many of these measures exist in various guidance documents, standards, and best practices and are likely to have been implemented to some degree by many of the Owner/Operators within the scope of TSA's SDs, the DHS 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 "Higher Risk" Railroads and Rail Transit Owner/Operators from cybersecurity threats.

SD Required and IC recommended collections:

Designate a Cybersecurity Coordinator	Owner/Operators will be required or recommended, as applicable, to appoint a U.S. Citizen Cybersecurity Primary and Alternate Coordinator who must submit contact information. The Cybersecurity Coordinator serves as the primary contact for cyber-related intelligence information and cybersecurity-related activities and communications with TSA and CISA; must be accessible to TSA and CISA 24 hours a day, seven days a week; must coordinate cyber and related security practices and procedures internally; and must work with appropriate law enforcement and emergency response agencies.
Cybersecurity Incident Reporting	Owner/Operators Cybersecurity Coordinators will be required or recommended, as applicable, to report actual and potential cybersecurity incidents to CISA within 24 hours of identification of a cybersecurity incident. The information provided to CISA pursuant to the SD is shared with TSA and may also be shared with the National Response Center (NRC) and other agencies as appropriate. Conversely, information provided to TSA pursuant to this directive is shared with CISA and may also be shared with the NRC and other agencies as appropriate. Cybersecurity incident reports are submitted using the CISA Reporting System form at: https://us-cert.cisa.gov/forms/report. Incident reports can also be reported by calling (888) 282-0870. Covered by CISA's approved OMB control number 1670-0037.
Cybersecurity Contingency/Response Plan	Owner/Operators will be required or recommended, as applicable, to develop and adopt a Cybersecurity Contingency/Response Plan to reduce the risk of operational disruption should their Information and/or OT systems be affected by a cybersecurity incident. Owner/operators must provide or recommended to provide, as applicable, evidence of compliance to TSA upon request.
Cybersecurity Assessment	Owner/Operators will be required or recommended, as applicable, to assess their current cybersecurity posture consistent with the

[6] OMB control number 1670-0037 covers voluntary reporting to CISA through the US-CERT website.

	functions and categories found in the NIST Cybersecurity Guidance Framework. The assessment and identification of cybersecurity gaps must be completed using a form provided by TSA. As part of the assessment, owners and operators must/may identify remediation measures to address the vulnerabilities and cybersecurity gaps identified during the assessment and plan for implementing the identified measures if necessary, and report the results to TSA. TSA will use the results of the assessments 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. TSA and CISA may also 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.

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. TSA's cybersecurity measures are aimed at protecting the vulnerability of OT systems and protecting civilian higher-risk infrastructure from being attractive targets for malicious cyber actors or foreign powers attempting to harm to US interests or retaliate for perceived US aggression has become increasingly important to securing the surface transportation network, U.S. national economy. and the way of life of Americans.

TSA is seeking approval for its new ICR "Cybersecurity Measures for Surface Modes" to include the collections to be required under TSA's SDs for "Higher Risk" Railroads and for rail and Rail Transit Owner/Operators and to be recommended under TSA's IC for public transportation bus Owner/Operators and OTRB Owner/Operators.

On October 14, 2021, OMB approved OMB control number 1670-0037, granting CISA approval to collect both voluntary and mandatory information security incidents. TSA will use the CISA Reporting System form approved under OMB control number 1670-0037, as directed by the SDs and IC, to report cybersecurity incidents to CISA.

Discussion

In order to execute its security responsibilities within the surface transportation industry and for to enhance cybersecurity of all critical infrastructure, TSA needs to have current awareness of potential security incidents and suspicious activity within surface transportation operations. TSA is issuing the cybersecurity SDs and IC to further secure the surface transportation sector against evolving and emerging risks and partnering with the private sector partners to secure "Higher-Risk" Railroads, Rail Transit and Rail bus operations, and OTRB Owner/Operators from cyber-attacks. Systems within mass transit, passenger rail, and freight rail rely on monitor and control systems, such as automated rail crossings and signals, staff access, track lighting, and freight

handling. Other systems monitor bridge and tunnel traffic and structural integrity. In addition, cyber risks can impact both data as well as control systems like tunnel-ventilation systems operated by transportation agencies.

There are also extensive interdependencies among transportation and other sectors. For example, bridges, tunnels, and roadways may also house utilities like power and communications, which are used by passenger and freight movement as well as the supply chain. To mitigate the continuing cyber threat and reduce the risk across surface transportation, TSA is issuing two SDs that will require "Higher Risk" Railroads and Rail Transit Owner/Operators to implement cybersecurity measures and issuing one IC that will recommend the implementation of specific cybersecurity measures for owner/operators not specifically covered under Security Directives 1580-2021-01 or 1582-2021-02.

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 transportation … including security responsibilities … over modes of transportation that are exercised by the Department of Transportation.

TSA and federal partner agencies will use the information to respond to and contain emerging cybersecurity attached. TSA will use the results of the assessments 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. TSA and CISA may also 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.

Certification of completion of SD requirements

Within 7 days of the deadlines set forth in the SD, Owner/Operators must ensure that their Cybersecurity Coordinator or other accountable executive submits a statement to TSA via email certifying that the Owner/Operator has met the requirements of the. TSA is not requiring/recommending any specific format for making these notifications, but is requiring them to be made in a timely way. Documentation of compliance must be provided upon request.

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 Owner/Operators. TSA has determined that the most efficient way to obtain the needed information is by issuing the SDs and IC to address cybersecurity concerns highlighted in the September 2021 CISA alerts.

In light of the current security threat to the nation's surface transportation systems, the increased use of Conti ransomware in more than 400 attacks on U.S. and international organizations, and recent global attacks against rail systems, TSA is seeking emergency clearance for approval to

require TSA-designated Owner/Operators to comply with the collection requirements mentioned above.

As is evident from the myriad of attacks mentioned in the timeline in Background section above, there is an immediate need to have the operators have a cybersecurity incident response plan to build resiliency and to conduct a cybersecurity assessment to identify gaps and permit TSA to do a global assessment of the industry risk posture. 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 SDs and IC in the near future. Reducing the vulnerability of "Higher Risk" railroads, rail transit systems, and OTRB operations and infrastructure to cybersecurity threats is fundamental to securing our nation's travelling public and economic security. The cybersecurity incident reporting information is covered under OMB control 1670-0037, as directed in the SDs and IC.

Conclusion

To mitigate this continuing threat and reduce the risk across surface transportation, TSA is issuing the SDs requiring and an IC recommending the implementation of specific cybersecurity measures for "Higher Risk" Railroads, Rail Transit and OTRB Owner/Operators and for the public transportation bus Owner/Operators and OTRB Owner/Operators, respectively, as part of the focused and aggressive continuing federal effort to address these significant threats to our nation. TSA is committed to securing the Transportation Sector against evolving and emerging risks such as cyber-attacks in partnership with the private sector partners.

TSA respectfully requests that OMB grant TSA's request for emergency clearance for TSA's Surface Mode Cybersecurity 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 SDs and IC as soon as possible to effectuate these goals.