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: 2021.07.14 15:57:11 -04'00'

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: 2021.07.14 11:46:27 -04'00'

SUBJECT: Emergency Information Collection Request (ICR): Pipeline Corporate Security Review (1652-0056)

Purpose

The 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 1652-0056, Pipeline Corporate Security Review (PCSR), to address the ongoing cybersecurity threat to pipeline systems and associated infrastructure.

Background

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 infrastructure and economic well-being.

Due to the ongoing cybersecurity threat to pipeline systems and associated infrastructure, TSA issued Security Directive (SD) Pipeline 2021-01[1] to address the threat, in coordination with the

[1] This directive requires TSA-designated Owner/Operators of hazardous liquid and natural gas pipelines and liquefied natural gas (LNG) facilities[1] to report cybersecurity incidents or potential cybersecurity incidents on their

Cybersecurity and Infrastructure Security Agency (CISA). TSA issued this SD under the authority of 49 U.S.C. 114(l)(2), which states:

> 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.

To protect against the ongoing cybersecurity threat, TSA is preparing to issue a second SD under the same authority, which will mandate that TSA-specified Owners/Operators of gas and liquid pipelines implement an array of cybersecurity measures to prevent disruption and degradation to their infrastructure.[2]

This SD will require , Owner/Operators to conduct the following security measures:

1. Implement specific mitigation measures to reduce the risk of compromise from a cyberattack.
2. Develop a Cybersecurity Contingency/Response Plan to reduce the risk of business or functional degradation of the Information and Operational Technology systems should a gas or liquid pipeline be the victim of a malicious cyber intrusion.
3. Test the effectiveness of the Owner/Operator's cybersecurity practices through an annual cybersecurity architecture design review.

While many of these measures exist in various guidance documents, standards, and best practices and are likely to have been implemented in some degree by many of the Owner/Operators within the scope of TSA's SDs, DHS has determined that it is necessary to mandate these measures to on an expedited basis to ensure they are implemented as necessary to protect national security by mitigating the current risk to pipelines from cybersecurity threats.

The SD contains several collections of information that require TSA to amend its currently approved OMB control number 1652-0056, Pipeline Corporate Security Review (PCSR), for which TSA is seeking emergency approval. Section 1557 of the Implementing Recommendations of the 9/11 Commission Act (Pub. L. 110-53; 121 Stat. 475; Aug. 3, 2007)

---

information technology (IT) and operational technology (OT) systems to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). This directive also requires these Owners/Operators to designate a Cybersecurity Coordinator who must submit his or her contact information and who is required to be available to the TSA 24/7 to coordinate cybersecurity practices and address any incidents that arise. TSA also requires owner/operators to assess their current cybersecurity posture against recommendations in TSA's Pipeline Security Guidelines in April 2011 and subsequently update the Guidelines in 2018 and 2021. *See* https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf. The results of the assessment will be used to develop remediation plan to address identified vulnerabilities. The results of the assessment must be reported to TSA within 30 days of issuance of the SD. TSA sought and OMB subsequently granted emergency approval for revision of the above-mentioned OMB control numbers on May 26, 2021.

[2] *See* Attachment 1 for a summary of compliance deadlines [TO BE ADDED ONCE REQUIREMENTS FINALIZED].

(9/11 Act), as codified at 6 U.S.C. 1207, requires TSA to conduct assessments of pipeline security systems. In order to assess current industry security practices, TSA implemented its PCSR program. The PCSR is a voluntary, face-to-face visit with a pipeline owner/operator during which TSA discusses the company's corporate level security planning and also completes the PCSR Form, which includes 210 questions concerning the owner/operator's corporate level security planning, covering security topics such as physical and cyber security, vulnerability assessments, training, and emergency communications. TSA also follows up on results of each PCSR. TSA uses the information to determine baseline security standards and areas of security weakness in the pipeline mode. This data and interaction with stakeholders informs TSA's *Pipeline Security Guidelines* (Guidelines), which were published in December 2010, with an update published in March 2018,[3] and it's Pipeline Security Best Practice Observation documents. TSA is seeking approval to amend this PCSR collection to include the collections to be required under TSA's second pipeline security SD.

Congress granted the TSA Administrator broad statutory responsibility and authority with respect to the security of the transportation system, including pipelines. *See* 49 U.S.C. 114(d). section 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 carrying out its authority in order to address a threat to transportation.[4] As noted above, TSA may issue security directives in order to protect transportation security. *See* 49 U.S.C. 114(l)(2). Congress' recognition of TSA's responsibility for pipeline security is reflected in Sec. 1557 of the 9/11 Act.

Discussion

Cybersecurity incidents affecting surface transportation are a growing threat. The attack on Colonial Pipeline demonstrates how criminal cyber actors are able to take advantage of remote and anonymous connectivity to a system or network to cause disruption or physical damage. TSA is issuing this second SD to address this continued threat to pipeline security demonstrated by the ransomware attack on Colonial Pipeline. Since that date, malicious actors have successfully conducted a ransomware attack with a significant affect across the global supply chain. To mitigate this continuing threat and reduce the risk TSA is issuing an SD that will require implementing of specific security measures.

Cybersecurity Contingency/Response Plan

Owner/Operators will be required to develop and adopt a Cybersecurity Contingency/Response Plan to ensure the resiliency of their operations in the event of a cybersecurity attack. Owners/operators must provide evidence of compliance to TSA upon request.

[3] See https://www.tsa.gov/for-industry/surface-transportation

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

Third Party Evaluation

Owner/Operators are required to have a third-party complete an evaluation of their industrial control system design and architecture to identify previously unrecognized vulnerabilities. This evaluation must include a written report detailing the results of the evaluation and the acceptance or rejection of any recommendations provided by the evaluator to address vulnerabilities. This written report must be made available to TSA upon request and retained for no less than 2 years from the date of completion.

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 SD. TSA is not requiring 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.

TSA will share information provided to TSA pursuant to this SD with CISA and may also share with the National Response Center and other agencies as appropriate. TSA may use the information, with company-specific data redacted, for TSA's intelligence-derived reports. TSA and CISA also 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.

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 this SD. In light of the current security threat to the nation's pipeline systems, TSA is seeking emergency clearance for approval to require TSA-designated owner/operators to comply with the collection requirements mentioned above.

The requirements that necessitate these collections are consistent with TSA's 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.[5] Consistent with this authority, TSA is the federal agency responsible for "assess[ing] the security of each surface transportation mode and evaluat[ing] the effectiveness and efficiency of current federal government surface transportation security initiatives."[6]

Without emergency approval, TSA will be unable to address the critical threat to the nation's pipeline systems. The use of normal PRA clearance procedures is reasonably likely to result in public harm such that DHS would be hindered in their ability to address immediate, continuing, and probable threats to pipeline systems if the SD were not issued in the near future. Reducing the vulnerability of critical pipeline operations and facilities to cybersecurity threats is fundamental to securing our nation's national and economic security.

[5] 49 U.S.C. § 114(d).
[6] EO 13416, section 3(a) (Dec. 5, 2006).

Conclusion

TSA respectfully requests that OMB grant TSA's request for emergency clearance for a revision to TSA's 1652-0056 pipeline security 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 this SD as soon as possible to effectuate these goals.