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: 2021.05.25 18:38:19 -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: 2021.05.25 16:41:10 -04'00'

SUBJECT: Emergency Information Collection Request (ICR): Critical Facility Information of the Top 100 Most Critical Pipelines (1652-0050); Pipeline Operator Security Information (1652-0055)

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 Numbers 1652-0050, Critical Facility Information of the Top 100 Most Critical Pipelines, and 1652-0055, Pipeline Operator Security Information, 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 is issuing a Security Directive (SD) to address the threat, in coordination with the Cybersecurity and Infrastructure Security Agency (CISA). TSA is issuing 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.

This directive will require 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 information technology (IT) and operational technology (OT) systems to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). This directive will also require 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 will also require 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 o 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 currently has two collections approved by OMB under the PRA that concern pipeline security through the voluntary collection of information. OMB control number 1652-0050 covers TSA-conducted voluntary assessments of critical pipeline facilities to facility security policies, procedures, and physical security measures. The operators covered by this collection are the same operators within the applicability of the SD. The approved collection is for TSA to collect the information on a Critical Facility Security Review (CFSR) Form. After TSA receives the CFSR Form, it conducts a facility visit and gets information about the facility's implementation of the security improvements and makes recommendations.to the facility. TSA will be providing the cybersecurity portions of this assessment to owner/operators for their use in conducting the assessment required by the SD. Owner/operators are not required to use the assessment resource provided by TSA. OMB control number 1652-0055 covers the voluntary reporting of suspicious activities or security incident data, as recommended in TSA's *Pipeline Security Guidelines* (Guidelines), which were published in December 2010, with an update published in March 2018.[2]

[1] Under the SD, TSA will also require TSA-specified Owner/Operators to report cybersecurity incidents and potential cybersecurity incidents to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). Second, the SD will require Owner/Operators to designate a Cybersecurity Coordinator who is required to be available to the TSA 24/7 to coordinate cybersecurity practices and address any incidents that arise, and who must submit contact information to TSA.

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

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.[3] As noted above, TSA may issue security directives in order to protect transportation security. *See* 49 U.S.C. 114(l)(2).

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 the SD to address this threat to pipeline security demonstrated by the ransomware attack on Colonial Pipeline.

Reporting of Cybersecurity Incidents

While TSA currently receives reports of security incidents on a voluntary basis, including pipeline cybersecurity incidents, under OMB control number 1652-0055, TSA has determined it is necessary to require reporting of pipeline cybersecurity incidents or potential cybersecurity incidents related to pipeline system and liquid natural gas facility information technology and operational technology systems. The SD requires the information to be reported to CISA within 12 hours of discovery. As CISA also voluntarily collects cybersecurity incidents from all infrastructure sectors, and required cybersecurity information from federal agencies, reporting to CISA will eliminate any confusion regarding where the information should be reported and reduce the burden of duplicate reporting to both agencies.

Security Coordinator

TSA's directive requires the TSA-designated Owner/Operators to designate a U.S. citizen Cybersecurity Coordinator who must submit his or her contact information and who is required to be available to TSA 24/7 to coordinate cybersecurity practices and address any incidents that arise. There is currently no federal requirement to designate a Cybersecurity Coordinator nor a consolidated list of information for the most critical pipeline owner/operators. In light of the current threat, it is critical for the government to have this information readily available.

Reporting Assessment Results

While TSA currently collects information when conducting voluntary assessments of pipeline operations, through its CFSRs approved under OMB control number 1652-0050, TSA has determined it is necessary for the most critical pipeline owner/operators to review Section 7 of TSA's Guidelines and self-assess current activities to address cyber risk. A current assessment

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

of cybersecurity is necessary to ensure the industry is protected from the threat. TSA does not have the resources to conduct an assessment of every system within the time necessary to address the threat. TSA will provide the cyber-related questions from the current assessment to support efforts by owner/operators to conduct the self-assessment. Owner/operators will use this information to address vulnerabilities and TSA will use the information to assess the current posture and the need for additional actions. This use of the information is consistent with the mandate in section 1557(d) of the 9/11 Act.

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 report cybersecurity incidents and to review cybersecurity recommendations in TSA's current Guidelines, conduct an assessment, develop a plan to address vulnerabilities identified during the assessment, and to report the results of the assessment to TSA within 30 days of issuance of the SD. TSA is requiring the TSA Pipeline Cybersecurity Self-Assessment form to be used for conducting the assessment and reporting the results.

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.[4] 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."[5]

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. In addition, DHS would not be able to share information with federal law enforcement partners who would initiate an investigation to identify potential criminal activity and perpetrators.

Conclusion

TSA respectfully requests that OMB grant TSA's request for emergency clearance for a revision to both TSA pipeline security collections 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.

[4] 49 U.S.C. § 114(d).
[5] EO 13416, section 3(a) (Dec. 5, 2006).