



Filed Via Email (TSAPRA@tsa.dhs.gov)

August 30, 2021

Christina A. Walsh
TSA PRA Officer, Information Technology (IT), TSA-11
Transportation Security Administration
6595 Springfield Center Drive
Springfield, VA 20598-6011

RE: Comments of the American Gas Association regarding:

1) *Intent To Request Revision From OMB of One Current Public Collection of Information: Critical Facility Information of the Top 100 Most Critical Pipelines*, 86 Fed. Reg. 34775 (June 30, 2021), and

2) *Intent To Request Extension From OMB of One Current Public Collection of Information: Pipeline Operator Security Information*, 86 Fed. Reg. 34777 (June 30, 2021)

Dear Christina A. Walsh:

The American Gas Association (“AGA”) appreciates the opportunity to comment on two Information Collection Requests (“ICR”) issued by the Transportation Security Administration (“TSA”) and related to a recent TSA Security Directive¹ (“Security Directive 1”) applicable to pipelines. First, in *Intent To Request Revision From OMB of One Current Public Collection of Information: Critical Facility Information of the Top 100 Most Critical Pipelines*, 86 Fed. Reg. 34775 (June 30, 2021), TSA is seeking to renew and revise the collection, Office of Management and Budget (“OMB”) control number 1652–0050, as it expires on November 30, 2021 (“Critical Pipeline ICR”). The Critical Pipeline ICR concerns statutory requirements for TSA to develop and implement a plan to inspect critical pipeline systems. On May 26, 2021, OMB approved TSA’s request for an emergency revision of this collection to address the ongoing cybersecurity threat. TSA is now seeking to extend its collection authority for the maximum three-year approval period. Second, in *Intent To Request Extension From OMB of One Current Public Collection of Information: Pipeline Operator Security Information*, 86 Fed. Reg. 34777 (June 30, 2021), TSA is seeking a three-year renewal of the existing emergency revision of this collection, OMB control number 1652-0055, to collect information involving the submission of data concerning pipeline security incidents, appointment of cybersecurity coordinators, and coordinators’ contact information (“Operator Security Information ICR”). TSA is seeking comment on both ICRs.

Since both of the notices relate to TSA Security Directive 1, and for administrative efficiency, AGA provides the following comments in response to the two above mentioned Federal Register notices in a single letter.

¹ Security Directive 2021-01, issued May 26, 2021.

I. Introduction

The American Gas Association, founded in 1918, represents more than 200 local energy companies that deliver clean natural gas throughout the United States. There are more than 76 million residential, commercial and industrial natural gas customers in the U.S., of which 95 percent — more than 72 million customers — receive their gas from AGA members. AGA is an advocate for natural gas utility companies and their customers and provides a broad range of programs and services for member natural gas pipelines, marketers, gatherers, international natural gas companies, and industry associates. Today, natural gas meets more than thirty percent of the United States' energy needs.²

On May 26, 2021, TSA issued Security Directive 1 in order to address the ongoing cybersecurity threat to pipeline systems and associated infrastructure. Security Directive 1 is applicable to owners/operators of a hazardous liquid and natural gas pipeline or liquefied natural gas facility notified by TSA that their pipeline system or facility is critical. AGA's natural gas utility members are subject to TSA's security authority and are affected by the new requirements set forth in Security Directive 1 and the IRCs noted above.

II. Review Of Critical Facilities Of The 100 Most Critical Pipeline Systems

The Critical Pipeline ICR addresses a statutory requirement for TSA to develop and implement a plan to inspect critical pipeline systems. On May 26, 2021, OMB approved TSA's request for an emergency revision of this collection to address the ongoing cybersecurity threat to pipeline systems and associated infrastructure. TSA is now seeking to renew and revise the collection as it expires on November 30, 2021.

Pursuant to the 9/11 Act Mandate, TSA visits and conducts a review of critical pipeline facilities using a Critical Facility Security Review ("CFSR") form. TSA is now revising the information collection to align the CFSR questions with the revised Pipeline Security Guidelines, and to capture additional criteria. As a result, the questions in the CFSR form have been edited to meet the Pipeline Security and criticality needs. In Security Directive 1, owners/operators are required to review Section 7 of TSA's Pipeline Security Guidelines and assess current activities, using the TSA Pipeline Cybersecurity Self-Assessment form.³ The form is based on the instrument used for the CFSRs but edited to address the scope of Security Directive 1. TSA is seeking renewal of this information collection for the maximum three-year period.⁴

A. Self-Assessments

TSA performs their review of critical facilities based on the TSA Pipeline Security Guidelines that were developed as part of the 9/11 Act. The questions asked as part of the CFSR are similar to the questions proposed in the Security Directive. The amount of detail and requested information within Security Directive 1, however, requires more defined responses. This can cause these two review forms to appear to not be in sync due to the inconsistency on guidance. AGA recommends that TSA consider having additional consistency and clarity between the forms. If an entity completes a CFSR, then it should not have to complete the TSA Pipeline Cybersecurity Self-Assessment form or vice-versa.

² For more information, please visit www.aga.org.

³ 86 Fed. Reg. 34776.

⁴ *Id.*

AGA recommends that TSA consider not leveraging the provided “information to make a global assessment of the cyber risk posture of the industry.”⁵ Companies had difficulties identifying the appropriate scope for completing the assessment. Organizations may have taken different approaches to completing the assessment based on the lack of guidance provided by TSA to date. Therefore, the various scope perspectives driving responses will result in inconsistencies that will cause the cyber risk posture to potentially be inaccurate. This can cause future TSA decision making to be inaccurate. AGA requests the TSA issue clear guidance and definitions that further define the scope of the Pipeline Cybersecurity Self-Assessment.

B. Three-Year Extension

TSA is seeking renewal of the Critical Pipeline ICR for the maximum three-year approval period.⁶ Due to the fact that the Security Directive 1 has a stated expiration date of May 28, 2022, AGA recommends that the Critical Pipeline ICR renewal should correspond with that expiration date. It is unclear why the renewal is for a longer term than the effectiveness of Security Directive 1. If TSA seeks to extend the term of Security Directive 1, a further renewal can be requested.

C. Burden Of Compliance

For the mandatory collection, TSA estimates 100 owners/operators will complete and submit the Pipeline Cybersecurity Self-Assessment form. TSA also estimates it will take each owner/operator approximately 6 hours to complete and submit this form, for a total of 600 hours (100 × 6).⁷ TSA estimates that total burden for the entire information collection is 1,400 hours annually—320 hours for the CFSR form, 480 hours for the recommendations follow-up procedures, and 600 hours for the Pipeline Cybersecurity Self-Assessment form.⁸

Operators have reported to AGA that the time spent on the Pipeline Cybersecurity Self-Assessment was between 60-150 hours (10 – 25 times the TSA estimate). AGA requests that TSA accurately reflect the excessive amounts of time it took owners/operators to complete the Pipeline Cybersecurity Self-Assessment, update the estimate in the Critical Pipeline ICR, and take the burden on owners/operators into consideration in future directives/regulations. TSA has underestimated the burden on owners/operators to complete the Pipeline Cybersecurity Self-Assessment form. This underestimation also calls into question TSA’s other estimates. TSA should update the estimated burden in the Critical Pipeline ICR (and the Operator Security Information ICR) to reflect the burdens on owners/operators.

III. Pipeline Operator Security Information

On May 26, 2021, OMB approved TSA’s request for an emergency revision of this collection to address the ongoing cybersecurity threat to pipeline systems and associated infrastructure. The Operator Security Information ICR describes the nature of the information collection and its expected burden. TSA is requiring all owners/operators subject to the Security Directive 1’s requirements to report cybersecurity incidents or potential cybersecurity incidents on their information and operational

⁵ See 86 Fed. Reg. 34776.

⁶ *Id.*

⁷ *Id.* at 34776 - 34777.

⁸ *Id.* at 34777.

technology systems to the Cybersecurity & Infrastructure Security Agency (“CISA”) using the CISA Reporting System. TSA is now seeking to renew this revised information collection as it expires on November 30, 2021, for the maximum three-year period.⁹

A. Incident Reporting

The Pipeline Security Guidelines encourage pipeline operators to notify the Transportation Security Operations Center (“TSOC”); however, the requirements for notification to the TSOC are very different than the requirements to notify CISA in Security Directive 1. In addition, Security Directive 1 provides that CISA would take all incident reports due to their experience. AGA requests TSA to clearly articulate who and what is the appropriate cyber incident handling authority for TSA and clarify the inconsistencies between TSA’s Pipeline Security Guidelines and Security Directive 1.

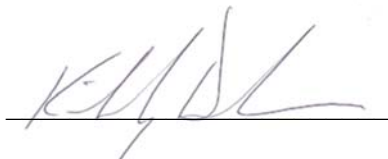
B. Three-Year Extension

TSA is seeking renewal of the Operator Security Information ICR for the maximum three-year approval period.¹⁰ As noted above, Security Directive 1 has a stated expiration date of May 28, 2022. Therefore, to the extent this collection relates to Security Directive 1, it should terminate when the directive expires.

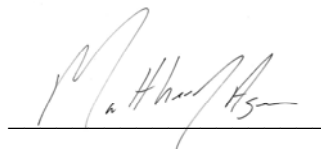
IV. Conclusion

AGA respectfully requests that TSA consider these comments in response to the ICRs. AGA looks forward to continuing to work with TSA on cybersecurity matters.

Respectfully submitted,



Kimberly Denbow
Managing Director, Security & Operations
American Gas Association
400 N. Capitol Street, NW
Washington, DC 20001
kdenbow@aga.org



Matthew J. Agen
Assistant General Counsel
American Gas Association
400 N. Capitol Street, NW
Washington, DC 20001
202-824-7090
magen@aga.org

Dated: August 30, 2021

⁹ 86 Fed. Reg. 34777.

¹⁰ *Id.* at 34778.