August 30, 2021

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

**Re: Docket No: TSA-2021-13884 – Intent to Request Revision from OMB of One Current Public Collection of Information: Critical Facility Information of the Top 100 Most Critical Pipelines**

Dear Ms. Walsh:

The American Fuel & Petrochemical Manufacturers Association (AFPM), the Association of Oil Pipelines (AOPL), the American Petroleum Institute (API), the American Public Gas Association (APGA), GPA Midstream Association, and the Interstate Natural Gas Association of America (INGAA)[1] (collectively, "the Associations") appreciate the opportunity to respond to the Transportation Security Administration's (TSA) Information Collection Request (ICR) requesting public comment on the renewal and revision of the existing approved ICR[2], Office of Management and Budget (OMB) control number 1652-0050, to continue collection of critical facility security information for TSA-identified critical pipeline systems. Through this ICR, TSA is revising the information collection to align the Critical Facility Security Review (CFSR) with the revised Pipeline Security Guidelines, and to capture additional criticality criteria. TSA is also seeking a three-year renewal of the May 26, 2021, emergency revision to allow for the institution of mandatory cybersecurity requirements within the Pipeline Security Guidelines. The Associations strongly support federal efforts to enhance the security posture of our nation's critical infrastructure, including pipeline systems, in partnership with the owners/operators of such systems. However, we are concerned about the process under which

[1] These trade associations represent almost all aspects of U.S energy pipeline operations that serve customers reliably across North America. The Associations' members represent refineries and petrochemical operators -- through which pipelines receive and distribute products, regional and local natural gas distribution pipelines, liquids pipelines, integrated and midstream natural gas and oil companies, operators of municipal natural gas systems, natural gas transmission pipelines, and natural gas product pipelines and processors.
[2] Office of Management and Budget (OMB) control number 1652-0050.

TSA issued the subsequent Security Directives (SDs)[3] for which the emergency revision is based, the rationale for the SDs, and the impact to operational safety of the prescriptive measures required therein.

## I. General Comments

The Associations have been actively involved in the development of and revisions to TSA's Pipeline Security Guidelines, including the most recent April 2021 update, and understand the agency's need to periodically review and revise the criticality criteria. Nevertheless, the criticality designation remains ambiguous as it relates to the impact of high consequence areas (HCAs) on facility operations. Furthermore, the Associations do not believe a three-year renewal of the May 26, 2021, emergency revision is warranted given that it undermines the emergent need for an SD. The prescriptive nature of the measures required in the two TSA-issued pipeline SDs do not allow for companies to effectively respond to the dynamic nature of the cybersecurity threat, the cost of implementing the measures outlined in the SDs do not adequately enhance the security posture of the affected facilities (cost-benefit analysis is absent) and the burden of compliance directs necessary resources away from prevention. The prescriptive measures required in the SD may impair pipeline operational safety and reliability. Additionally, TSA is basing the emergency revision on vague cybersecurity threat information that has not been shared so companies can adjust risk-based security programs. Should TSA seek to regulate pipeline cybersecurity, the agency must proceed through regular notice and comment rulemaking.

## II. Updates to Criticality Criteria

The Pipeline Security Guidelines are an important tool for pipeline owner/operators to manage their policies and procedures for security-related threats, incidents, and responses. Whether or not an asset should be deemed critical is determined by risk, consequence, mitigation, and other factors, using the operator company's methodology. The Associations appreciate TSA's intent in allowing the operator company to apply their methodology to determine asset criticality; however, a more focused approach on designation would eliminate ambiguity between the operator and TSA. Furthermore, the Associations recognize TSA's need to periodically review the Pipeline Security Guidelines to reflect additional criticality criteria, but High Consequence Areas (HCAs) should not be weighed more than other criteria in determining criticality. As HCA is not determinate of criticality for US critical infrastructure, the effect of HCAs on critical infrastructure operations should be the criteria.

## III. Extension of Emergency Revision to Address Cybersecurity Risks

A three-year extension of the May 26, 2021, emergency revision to allow for the institution of mandatory cybersecurity requirements is not warranted because it invalidates the necessity for the two pipeline SDs. A more appropriate approach to issuing mandatory cybersecurity requirements would be through notice and comment rulemaking.

---

[3] Security Directive 2021-01, issued May 26, 2021, and Security Directive 2021-02, issued July 19, 2021.

In this ICR, TSA cites that to address "the *ongoing* [emphasis added] cybersecurity threat to pipeline systems and associated infrastructure, TSA issued a Security Directive (SD)" requiring affected owner/operators to "review section 7 of TSA's Pipeline Security Guidelines and assess current activities… to address cyber risk, and identify remediation measures that will be taken to fill those gaps and a timeframe for achieving those measures." To issue SDs, the TSA Administrator must determine that "a regulation or security directive *must be issued immediately* [emphasis added] in order to protect transportation security."[4] This emergent requirement supposes that an urgent threat to pipeline systems will otherwise directly impact pipeline systems if not immediately addressed. However, the "ongoing" threat cited by TSA suggests that the threat has been in existence for an extended period of time and therefore does not meet the threshold for an immediate regulatory action such as an SD.

Indeed, the subsequent release of CISA Alert (AA21-201A), "Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013"[5] – a ten-year old threat, released one day following the issuance of the second SD - was cited as evidence by TSA of this ongoing threat. When asked how many groups have declared an intent to commit cyberattacks on pipeline systems, and further, if these known groups have the capability to conduct a cyberattack, TSA reported three threat actors (animal rights' extremists, anarchist violent extremists, and environmental rights' extremists) "have expressed interest" in conducting attacks, but that "none of these three movements have demonstrated the capability to conduct any sort of sophisticated cyber attack or intrusion."[6]

Similarly, this ICR notes that the emergency revision was "necessary as a result of the recent ransomware attack on one of the Nation's top pipeline supplies *and other emerging threat information* [emphasis added]." The inclusion of "other emerging threat information" without clarity or operator knowledge of such threat information weakens the ability of the owner/operator to respond to such threats based on their own risk-based security programs, as outlined in the TSA Pipeline Security Guidelines. The Oil & Natural Gas Subsector Coordinating Council (ONG SCC), the Associations, and individual operating companies have repeatedly requested threat briefings from TSA and other intelligence community (IC) agencies. Without such information, companies are unable to adjust their security programs and defend against the threat. While there are recent efforts to brief pipeline stakeholders, the lack of information sharing to-date and the action only after multiple requests from owners and operators, is a clear undercut to the public-private partnership that has, to this point, contributed to the safe and secure operation of our nation's critical pipeline systems.

Notably absent from the ICR is a cost-benefit analysis of the measures prescribed in the statutory requirements for issuance of an SD. Safety and security of pipeline operations are the top concern of pipeline operators, and the Associations' members are proactive in improving the security posture of their facilities; however, the measures outlined in the two SDs do not enhance operational security and the TSA Administrator has not presented a cost-benefit analysis

[4] *See* 49 USC 114(l)(2)(a).
[5] *See* CISA Alert (AA21-201A), Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013 (released July 20, 2021), https://us-cert.cisa.gov/ncas/alerts/aa21-201a.
[6] C. Phillips, email to trade association representatives, July 20, 2021.

justifying the security benefit for these measures. Specifically, the enabling statute requires the TSA Administrator to consider "*whether the costs of the regulation are excessive in relation to the enhancement of security the regulation will provide* [emphasis added]."[7] From the operator perspective, it remains unclear how many of the prescriptive security requirements outlined in the two SDs functionally benefit pipeline cybersecurity, and until this is known, the burden of compliance with the SDs is directing necessary resources away from prevention. As such, the absence of a cost-benefit analysis for these regulations are indicative of hastily constructed policies that do not adequately account for how such mandatory actions improve security.

While not specifically seeking comment on this issue, the Associations would be remiss if they did not provide consideration to the unintended consequences that several of the highly prescriptive measures in the second SD may have on pipeline operational safety and security. During the SD drafting process, the Associations provided specific comments around potential operational concerns that could arise by imposing prescriptive cyber requirements without specific understanding of a company's existing approach or protections. Although some of the compliance timelines have been extended, there remain significant concerns regarding rigid implementation of the SD to pipeline operating systems, which might unnecessarily impact the integrity and reliability of these systems. The Associations urge TSA to work with operators and The Pipeline and Hazardous Materials Safety Administration (PHMSA), to ensure that, as changes are required, operators are not sacrificing one risk to reliability for another.

## IV. Conclusion

The Associations and their members appreciate the opportunity to comment on both this ICR and the associated SDs. We strongly support the longstanding public-private partnership to prevent and mitigate cybersecurity threats to critical infrastructure, and we encourage the federal government to continue working with industry to ensure that pipeline operations are safe, secure, and that threat information is shared in a timely and bi-directional manner which protects the risk-based corporate security programs that TSA, CISA, and other federal agencies espouse in their guidance. The Associations sincerely appreciate the collaborative relationship we have with TSA. Thank you for your support to our industry and for jointly seeking reasonable solutions to issues of concern.

Sincerely,

American Fuel & Petrochemical Manufacturers (AFPM)

Association of Oil Pipelines (AOPL)

American Petroleum Institute (API)

[7] *See* 49 USC 114(l)(3).


American Public Gas Association (APGA)

GPA Midstream Association

Interstate Natural Gas Association of American (INGAA)