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-2021-13885 – Intent To Request Extension From OMB of One Current Public Collection of Information: Pipeline Operator Security Information**

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 a three-year renewal of the existing emergency revision to this ICR[2] to collect information involving the submission of data concerning pipeline security incidents, appointment of cybersecurity coordinators, and coordinators' contact information. The Associations support federal efforts to enhance the security of the nation's pipeline systems, in partnership with owners/operators. While we stand ready to work with TSA to ensure the secure operation of the nation's most critical pipelines, the Associations do not believe a three-year extension to the May 26, 2021, emergency revision is warranted, because TSA is not accurately calculating the burden to the public from the broad scope of applicability for cybersecurity incidents that require reporting across both the information technology (IT) and operational technology (OT) networks. Furthermore, while the Associations' members do not oppose appointing cybersecurity coordinators within their companies, TSA fails to account for the increased resources required to maintain such position at little-to-no added security benefit for the pipeline system. Ultimately, a three-year extension undermines the need for the subsequent

[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 1652-0055.

two Security Directives (SDs)[3] for pipeline cybersecurity for which the emergency revision is based. As previously stated to the agency, the Associations maintain that, should TSA seek to regulate pipeline cybersecurity, the agency should proceed through notice and comment rulemaking.

## I. General Comments

The Associations appreciate the opportunity to provide feedback during the development of both SDs; however, TSA has not addressed many of the substantive concerns raised in those comments. Among those concerns include a lack of information regarding the threat for which these SDs are based. In this ICR, TSA notes that the emergency revision "was required as a result of the recent ransomware attack on one of the Nation's top pipeline supplies and *other emerging threat information* [emphasis added]." While industry fully understands the significance of the May 2021 cyberattack on the Colonial Pipeline system, the subsequent investigation into the attack revealed no breach into the pipeline system and the company's decision to temporarily shutdown the pipeline was solely preventative. As such, that incident should no longer be used to justify the emergency revision. Similarly, "other emerging threat information" is vague, and despite repeated attempts from the Associations and the Oil & Natural Gas Subsector Coordinating Council (ONG SCC) to receive classified threat briefings, the agency has only just recently responded, but has still yet to schedule such briefing. Without timely, actionable intelligence, pipeline operators cannot defend against the ever-evolving cybersecurity threat, nor can they make appropriate adjustments to their risk-based security programs per the TSA Pipeline Security Guidelines.

Moreover, the statutory authority under which TSA may issue SDs requires the TSA Administrator to determine that "a regulation or security directive must be *issued immediately* [emphasis added] in order to protect transportation security." This emergent requirement supposes that an urgent threat to pipeline systems will otherwise directly impact pipeline systems if not immediately addressed. As of July 19, 2021, the issuance date of the second SD, no timely threat information had been shared with industry. Meanwhile, the "ongoing" threat cited by TSA suggests that the threat has existed for an extended period of time and therefore does not meet the threshold for an immediate regulatory action such as an SD. TSA has previously cited an unnamed 2017 Director of National Intelligence (DNI) Report referencing pipelines as support for the SDs, but that is a four-year old report. Similarly, the subsequent release of CISA Alert (AA21-201A), "Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013"[4] – a ten-year old threat, released one day following the issuance of the second SD – is being used 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

[3] Security Directive 2021-01, issued May 26, 2021, and Security Directive 2021-02, issued July 19, 2021.
[4] *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.

attacks, but that "none of these three movements have demonstrated the capability to conduct any sort of sophisticated cyber attack or intrusion."[5]

As discussed in our collective comments during the SD development process, it is unclear whether the prescriptive measures within the SDs afford functional benefits to pipeline cybersecurity. One tangible action that will assuredly increase the security posture of our nation's pipeline systems is information sharing. This demonstrable lack of information sharing to-date between the intelligence community, TSA, and other federal agencies with the private sector severely weakens the public-private partnership that pipeline operators rely on to support their use of federal voluntary security programs. Without this trust, pipeline operators are left behind to defend against a threat to which they have no knowledge, potentially resulting in a significant cyberattack to critical systems.

## II. Cybersecurity Coordinators

Among the requirements within the first SD, issued May 26, 2021, TSA requires all affected pipeline companies to designate a "cybersecurity coordinator and to provide contact information for the coordinators to TSA." Per the SD, the coordinator is to be available to both TSA and the Cybersecurity and Infrastructure Security Agency (CISA) 24 hours a day, seven days a week. While the Associations do not oppose the appointment of cybersecurity coordinators, TSA should, through this ICR, consider the company's additional resource burden for maintaining that position, with no clear benefit to the security posture of the pipeline system. TSA should also consider the realities of how large, integrated companies with multiple operational segments are organized. Designating a single, corporate-level official in a multi-operational enterprise is less appropriate than at the functional level.

## III. Incident Reporting

In addition to the above requirement, TSA is requiring all affected pipeline operators to report cybersecurity incidents or "potential" cybersecurity incidents on *both* their IT and OT systems to CISA within 12 hours using the CISA reporting system. Congress gave TSA authority over pipeline security. The SD, however, exceeds TSA's authority to the extent it requires reporting of cybersecurity incidents on corporate IT systems that are not directly linked to pipeline OT. The encroachment of the SD's application to the entire corporate IT system is beyond the jurisdiction of the agency.

The Associations understand the benefits of an incident reporting framework that supports more efficient federal guidance and information sharing with the private sector. However, the requirements in the SD are ambiguous and overly broad. The reporting requirements apply to any event that "actually, imminently, or potentially jeopardizes, disrupts or otherwise impacts the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident on the system." This definition is potentially broad enough to capture any

[5] C. Phillips, email to trade association representatives, July 20, 2021.

incident, no matter how insignificant, including those that would not otherwise cause IT management to be alerted. To address this problem, TSA should integrate the concept of "materiality" as a trigger for reporting.

From the outset, the Associations have encouraged reporting narrowly focused on key assets. In prior engagements with the Associations, TSA has indicated a sensitivity to that concern by expressing a desire to focus reporting on events that would otherwise be elevated to an operator's Board of Directors or executive leadership. The ICR, however, indicates TSA anticipates operators will need to submit up to 20 incidents annually. This estimate exceeds significantly the number of events that would rise to the level of Board or Executive awareness. TSA must avoid designing regulations that would require reporting of otherwise minor, nonmaterial incidents. This volume of information may overwhelm CISA with massive amounts of low-value data.

The Associations also believe the 12-hour reporting timeframe is aggressive and far too short. The Associations underscored this point during the SD development process; however, it was not considered in the final SD. This short reporting timeframe is likely to result in a lot of "just in case" false reporting to avoid noncompliance.

Additionally, the Associations feel that affected entities should be afforded strong liability and disclosure protections given the breadth of the reporting requirements. Despite industry efforts to engage with TSA on this issue during the SD development process, protections were ultimately not included in the final SD. It is important to underscore that if affected companies comply with the obligations in the SD and are, in good faith, defending against robust and dynamic cybersecurity threats, but an attack is still somehow successful, a lack of protections ultimately results in victim punishing.

## IV. Conclusion

The Associations and their members appreciate the opportunity to provide feedback on both this ICR and the associated SDs. As discussed, the little meaningful expert input ultimately included in the final SDs, the absence of reciprocal information sharing, the development of an incident reporting structure with an ambiguous materiality threshold, and the lack of liability protections for affected operators are concerning and do not clearly effectuate security under TSA's emergency authorities. The Associations support the longstanding public-private partnership to prevent and mitigate cybersecurity threats to critical infrastructure, and we encourage the federal government to work closely with industry to ensure that pipeline operations remain safe and secure. The Associations sincerely appreciate the collaborative relationship we have with TSA. We 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)

American Public Gas Association (APGA)

GPA Midstream Association

Interstate Natural Gas Association of American (INGAA)