February 5, 2025

Submitted via regulations.gov

Docket Management Facility (M-30)
U.S. Department of Transportation
1200 New Jersey Avenue SE
West Building Ground Floor, Room W12-140
Washington, DC 20590-0001

Re: Notice of Proposed Rulemaking on Enhancing Surface Cyber Risk Management (Docket No. TSA-2022-0001)

The undersigned trade associations, hereinafter referred to as "the associations," respectfully submit this comment letter on behalf of the oil and natural gas subsector in response to the Transportation Security Administration's (TSA's) Notice of Proposed Rulemaking (NPRM) on *Enhancing Surface Cyber Risk Management*.[1] Collectively, our associations represent each segment of the oil and gas industry, including the midstream hazardous liquid and gas pipelines, gas processing plants, refineries, gas utilities, and LNG facilities covered under TSA's proposed rule. While many of our associations submitted individual comments to the NPRM, the associations submit this supplemental letter to underscore our industry's alignment with several major considerations and concerns with the NPRM.

The associations appreciate TSA's thorough proposal for cybersecurity regulations. We recognize TSA had been working towards cybersecurity rulemaking for pipelines well before the instatement of the pipeline Security Directives (SDs). For the past four years, the SDs have served as an effective tool to put into practice different approaches to pipeline cybersecurity regulations. The associations appreciate how TSA has worked closely with the covered pipeline community to refine and revise the requirements in the SDs to more appropriately align with the pipeline operational environment. Most importantly, we commend TSA for recognizing the value and applicability of the risk-based and outcome-driven approach defined by the current SDs.[2] To that end, the associations are concerned that TSA's NPRM diverges from this fundamental tenet in many regards; a precept that is imperative to the pipeline operators who will implement the requirements of the final rule with limited human and financial resources.

The NPRM's broad reference to and application of aviation security requirements onto surface transportation undermines over two decades of pipeline operations education the associations and their members have provided to TSA. While the associations understand TSA's intent to streamline the regulatory process within its own agency, there is no security benefit or utility to surface transportation by aligning their requirements with aviation. TSA further does the owner/operator a disservice by pairing pipeline with rail and over-the-road bus. Lastly, TSA knows pipelines are a part of the broader Energy

[1] *Enhancing Surface Cyber Risk Management*, Docket No. TSA-2022-0001, RIN 1652-AA74, 89 Fed. Reg. 88488 (November 7, 2024).

[2] *Security Directive Pipeline 2021-01D* issued on May 29, 2024 and *Security Directive Pipeline 2021-02E* issued on July 26, 2024.

Sector and subject to other security regulators over portions of the pipeline system not under TSA jurisdiction, (e.g., United States Coast Guard and the North American Electric Reliability Corporation TSA is encouraged to take the lead in driving regulatory harmonization and reciprocity.

The associations strongly encourage TSA to consider the specific comments our organizations submitted in response to the request for comment to this NPRM and the following broader observations.

TSA should limit the scope of this rulemaking to **only** those operator-designated Critical Cyber Systems. Throughout the proposal, TSA makes multiple references to information technology (IT) and operational technology (OT) systems. A broad application of scope to all IT and OT systems is prescriptive, impractical, and in some cases, inapplicable. TSA should clearly state that the scope of this rulemaking is limited exclusively to Critical Cyber Systems.

TSA should avoid prescriptive management of owners/operators' personnel decisions. While the associations understand TSA's intent in the proposed rule for owners/operators to have designated professionals, who would be available and held accountable, TSA fails to consider that covered organizations vary significantly in size, structure, and corporate office location (domestic vs international). TSA should afford operators the authority to designate the most qualified individual(s) as appropriate rather than prescriptively governing a company's organizational chart. Further, TSA should limit requisite training to only those with access to Critical Cyber Systems. Regarding "accountable executive", TSA is encouraged to specify this as "management level" as opposed to "corporate level," which more effectively suits a wide range of organizational structures. TSA should also have a clear waiver process should an owner/operator only have foreign nationals available to fulfill these roles.

TSA should re-evaluate the expanse of compliance obligations for covered owner/operators. The associations urge TSA to reexamine the compliance obligations and proposed timelines in favor of an approach that can be uniformly applied across organizations of ALL sizes and structures. The arbitrary timelines TSA is proposing and the addition of new notification requirements, (i.e., TSA is proposing to require covered owner/operators notify the agency if their assets are in scope with the rule) may require the addition of staff resources dedicated solely to TSA cyber compliance. These are resources that will be redirected from active cyber defense to regulatory compliance.

TSA should clearly articulate the transition from SDs to regulation. The impact on owners/operators, who have been complying with the SDs, should take precedence in the transition so that compliance work they have already completed is properly credited. TSA should also define how the transition from SD to regulation will impact current Cybersecurity Assessment Plan (CAP) submittals. For example, some owners/operators already have CAPs approved by TSA that encompass a three-year plan to meet requirements. What happens to these plans once the regulation is finalized? The associations hope TSA is not moving backwards to more prescriptive requirements.

TSA should not take possession of owners/operators' sensitive security information. TSA is requesting a large volume of sensitive security information from owners/operators. Throughout the SD process, TSA afforded owners/operators some flexibility in providing security sensitive information. The associations implore TSA to avoid introducing risks to the Critical Cyber Systems and not to take possession (neither hardcopy nor digital) of owners/operators' sensitive security information.

TSA is encouraged to be appropriately resourced to address the threat and risk posed to pipeline systems. The associations have worked with TSA and Congress to ensure TSA has the appropriate staffing and expertise necessary to achieve its mission. TSA has and continues to address critical gaps in its workforce by adding full-time staff at headquarters and in the TSA regions with specialized knowledge of operational technology cybersecurity. These professionals have bolstered the agency's efforts and reputation among industry and the federal government. TSA should continue to collaborate with industry and the associations to understand where resource challenges may exist and require attention.

In closing, the associations thank TSA for providing a comprehensive framework for enhancing surface cyber risk management. Our suggestions aim to improve clarity, reduce compliance burdens, and ensure flexibility in implementing cybersecurity measures while ensuring covered owner/operators' security sensitive information is protected. The associations remain committed to working with TSA in the implementation of the final rule and are available to provide any additional information or clarity as requested.

Sincerely,

American Fuel & Petrochemical Manufacturers Association

American Gas Association

American Petroleum Institute

American Public Gas Association

GPA Midstream Association

Interstate Natural Gas Association of America

Liquid Energy Pipeline Association