American
Fuel & Petrochemical
Manufacturers

1800 M Street, NW
Suite 900 North
Washington, DC
20036

202.457.0480 office
202.457.0486 fax
afpm.org

February 5, 2025

Ashley Marks
U.S. Department of Transportation
1200 New Jersey Avenue SE
West Building Ground Floor, Room W12-140
Washington, DC 20590-0001

Attention: Docket ID No. TSA-2022-0001
Submitted to the Federal eRulemaking Portal (www.regulations.gov)

Re: Enhancing Surface Cyber Risk Management Notice of Proposed Rulemaking, 89 Fed. Reg. 88488 (Nov. 7, 2024), Docket No. TSA-2022-0001

Dear Ms. Ashley Marks,

The American Fuel & Petrochemical Manufacturers (AFPM) is pleased to submit these comments on the Enhancing Surface Cyber Risk Management Notice of Proposed Rulemaking, 89 Fed. Reg. 88,488 (Nov. 7, 2024) (Proposed Rule).

AFPM is the national trade association representing nearly all U.S. refining and petrochemical manufacturing capacity, including the midstream transport that moves products from facilities to consumers. AFPM members support more than three million quality jobs, contribute to our nation's economic and national security, and enable the production of thousands of vital products used by families and businesses throughout the United States. AFPM members are committed to filling these roles in a way that is responsible and sustainable for the long term. AFPM has a strong interest in this proposal, as AFPM has numerous members subject to the current TSA Pipeline Cyber Security Directives (SDs) and this proposed rule could increase the number of AFPM members subject to TSA pipeline cybersecurity regulations.

I. Introduction:

AFPM members operate and manage hazardous liquid and gas pipelines that are subject to the current TSA Pipeline Cybersecurity SDs. AFPM members have been subject to numerous cyber security regulations and initiatives from multiple agencies such as CISA, MTSA under the USCG, NIST, and DOE's CMMC2. AFPM has commented on past SDs and is encouraged that TSA is pursuing a notice and comment approach to codify the current SD guidelines. Prior to the publication of the SDs, AFPM members were actively implementing the voluntary TSA Pipeline

Security Guidelines and have had a cooperative and collaborative relationship with TSA as they have implemented the SDs.

II. Harmonization:

AFPM members are subject to multiple cyber security incident reporting regulations—including SEC, USCG, and the TSA SDs. AFPM has long supported a more harmonized approach by the government to reduce duplicative efforts on industry and streamline an efficient government response if needed. AFPM supports regulatory harmonization across all government agencies, including the DOD/USCG, and the reporting of incidents directly to CISA rather than the TSA. Unfortunately, this Proposal demonstrates that little progress has been made to harmonize with other agencies. CISA is currently developing the CIRICIA Harmonization rule, and there is no attempt in this proposed rule to recognize and coordinate the same reporting timing and information or even indicate this will be changed when CIRCIA is finalized. By contrast, the USCG Cybersecurity final rule recognized the CIRICIA harmonization effort. AFPM strongly encourages TSA to take a similar approach as the USCG and commit to harmonizing with the CIRCIA rule. More importantly, it creates more problems than it solves for TSA to move forward with a new rule BEFORE harmonization is determined. AFPM urges that TSA works on a truly good faith effort to harmonize with the CIRICA rulemaking to reduce the reporting burden on industry. There is no urgency when approximately 100 of the pipeline systems are already in compliance with the SDs.

The present duplicative reporting regulatory regimes would seem to be a good example of regulatory inefficiency that is currently under rising scrutiny. As it stands, a single oil and natural gas (ONG) company could be wrestling with three (or more) new regulatory programs, all dropping at roughly the same time—each with its competing reporting requirements, annual inspections, evaluations, program documents, and plans. TSA should carefully consider the duplicative and potentially counterproductive regulatory burden by multiple agencies competing to regulate the same companies in the same sector. America's national security interests are undermined if agencies consume ever more of a company's cybersecurity resources with an endless compliance do-loop when their focus should be on mitigating cybersecurity risks.

III. Applicability of Expanded NPRM (SDs) to AFPM Members:

AFPM urges TSA to maintain existing regulatory requirements. TSA should continue to focus on the definition of Critical Cyber Systems and ensure that the scope of that definition does not expand beyond the definition used in the SDs. AFPM and other industry stakeholders originally supported the idea that TSA would codify the requirements of the SDs into a rule as this would allow for a more thoughtful approach that will consider stakeholder comments and avoid the confusion that occurred with the original SDs. However, TSA instead expanded the scope of the rule, added physical security requirements from the voluntary TSA Pipeline Security Guidelines, and included a host of additional requirements such as CISA secure-by-design and employee

background checks. AFPM reiterates and urges that TSA work on a truly good faith effort to harmonize with the CIRCIA rulemaking to reduce the reporting burden on industry. There is no urgency to go forward with this rulemaking until at least the cyber incident reporting information is harmonized and when approximately 100 of the pipeline systems are already in compliance with the SDs.

TSA is proposing to apply the Cyber Risk Management (CRM) program requirements to owner/operators of hazardous liquid or carbon dioxide pipeline facilities and systems that meet any of the following criteria:

- Owns or operates a hazardous liquid pipeline or facility subject to 49 CFR part 195 that—
  - Annually delivered hazardous liquids in excess of 50 million barrels in any of the three calendar years before the effective date of the final rule, or any single calendar year after the effective date of the final rule; or
  - Is in excess of 200 segment miles of pipeline transporting hazardous liquid or carbon dioxide that could affect a High Consequence Area, as defined by PHMSA.
- Owns or operates a primary control room responsible for multiple hazardous liquid or carbon dioxide systems regulated under 49 CFR part 196 and the total annual delivery for those systems combined is greater than 50 million barrels annually in any of the three calendar years before the effective date of the final rule, or any single calendar year after the effective date of the final rule.
- Owns or operates a hazardous liquid pipeline or facility subject to 49 CFR part 195 that has a contract with the Defense Logistics Agency (DLA) to supply hazardous liquids in excess of 70,000 barrels annually.

Based on pipeline systems and facilities that report annual throughput to the Federal Energy Regulatory Commission (FERC), the TSA estimates these systems and facilities account for ***approximately 90 percent of the total annual volume transported in the United States.*** TSA is significantly broadening the scope and the requirements of the SDs, even though industry and TSA consider the current requirements within the SDs sufficient and effective. If there is no problem, it is capricious for TSA to expand the scope and requirements of the SDs.[1] Unfortunately, TSA did not discuss expanding or adding additional requirements beyond the current SDs with stakeholders when discussing this proposed rule.

The NPRM expands TSA's regulatory oversight while taking away owners/operators' ability to use its expertise to manage its system and program. For example, section 1586.217 Protection of Critical Cyber Systems subsection (e) requires secure backups but does not allow an owner/operator the authority over its own operations to identify situations in which it would be preferable to rebuild an environment from scratch, rather than from backups.

[1] *City of Chicago v. Federal Power Com.*, 458 F.2d 731, 742 (D.C. Cir. 1971) ("A regulation perfectly reasonable and appropriate in the face of a given problem may be highly capricious if that problem does not exist.").

Owners/operators need to have flexibility and control over their own operations to make these decisions.

TSA's expansion of the definition of Critical Cyber Systems beyond the current SDs threatens to move the system away from a risk-based system. Throughout the proposal, TSA makes multiple references to information technology (IT) and operational technology (OT) systems. While some of these systems may be considered Critical Cyber Systems based on the operator's risk assessment, a broad application to all IT and OT systems is prescriptive, difficult to implement, and challenging to enforce. Clearly stating that the scope of this rulemaking is limited exclusively to Critical Cyber Systems would ensure this rule is considerably more manageable.

TSA's proposed rule departs from the well-established, already-working SD regime by adding more onerous requirements that either (i) lack a clear tie to any gaps in the already-well-working SDs; or (ii) veer toward introducing new security concerns, and expanding beyond critical pipeline systems. AFPM supports a codification of the well-thought-out and well-working SDs, but AFPM does not support this direction of surprisingly increased requirements (again, many of which could even negatively impact a site's security posture) by expanding the definition of Critical Cyber Systems.

The Proposal creates new vulnerabilities because TSA may require more information about employees and architecture be submitted to TSA. An increase in transferred classified data inevitably increases cybersecurity risk, and it is doubtful that this new vulnerability is offset by the value of the information to TSA. Collection of detailed documentation around software versions and network security for housing with TSA provides a new source for threat actors to obtain blueprints for designing future attacks on our critical infrastructure. Instead, AFPM recommends that the final rule provide that TSA can inspect requested sensitive information but should not be able to receive or retain copies for security purposes. TSA should keep its focus on ensuring (and where appropriate, verifying) that covered entities' plans include / account for desired features, stopping short of micromanaging how those plans do so and requiring documentation that is further distributed (and therefore increases vulnerability).

AFPM proposes the following regulatory language changes:

> For Sections 1586.231, 1580.331, 1582.231, 1586.213, and 1586.231 which states that upon request "the owner/operation must provide for inspection ~~or copying~~ the following … "

AFPM appreciates TSA's thorough proposal for cybersecurity regulations, taking four years from the issuance of the first pipeline Security Directive (SD) to release this NPRM. During those four years, TSA worked closely with the covered pipeline community to refine and revise the requirements in the SDs to align with the pipeline operational environment more appropriately and, most importantly, with a risk-based and outcome-driven approach that aligns with accepted standards in industry. To that end, AFPM is 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.

Indeed, TSA's broad reference to and application of aviation security program requirements onto surface transportation within the NPRM undermines the significant work of industry stakeholders in educating TSA. Stakeholders and industry professionals have communicated with TSA on how pipeline operations work and why risk and outcome-based security programs afford operators the flexibility to adjust in the constantly evolving threat landscape. As TSA knows well, the pipeline subsector is also a part of the broader energy sector and has dependencies with chemical, water, electricity, financial services, telecommunications, and refining, among others. While AFPM appreciates TSA's intent to streamline the regulatory process within its own agency, there is no security benefit or utility to surface transportation by coupling each of the covered modalities and aligning their requirements with the aviation security program.

TSA should clearly limit the scope of this rulemaking to only those operator-designated Critical Cyber Systems. . Lastly, for organizations with contracts involving the DLA, further guidance on how these requirements interact with contractual obligations would be valuable.

IV. Support for a Regulatory Proposal:

It should be noted that AFPM and other industry stakeholders originally supported the idea that TSA would codify the requirements of the SDs into a rule as this would allow for a more thoughtful approach that will consider stakeholder comments and avoid the confusion that occurred with the original SDs. However, TSA instead expanded the scope of the rule, added physical security requirements from the voluntary TSA Pipeline Security Guidelines, and included a host of additional requirements such as CISA secure-by-design and employee background checks.

There are presently approximately 100 regulated pipeline systems deemed critical by TSA under the current SDs. By TSA's estimate, the new rule would apply to 115 pipelines. However, AFPM believes the expanded scope of the rule will exceed the TSA estimated additional 15 pipeline systems. If so, the timing of this proposed rule will be especially burdensome because many in the ONG industry are going to be addressing significant rulemakings like the Coast Guard Cyber rule, the CIRCIA rule, SEC Cyber Incident Reporting, and in some cases CMMC 2 and a host of other cyber programs. This NPRM should only apply to critical IT and OT systems related to the functioning of the critical pipeline system.

V. Concerns with New Requirements:

AFPM appreciates TSA taking comments on this proposal and strongly encourages TSA to consider stakeholder comments seriously before finalizing the rule. If TSA decides to move forward with the rule we have the following concerns. There should be no further rulemaking until progress is made with harmonization. We need security cooperation between the public and private sectors that is effective. We need to see accountability and cooperation among agencies to ensure that this is not yet another pen and paper exercise that ends up undermining security and

sapping resources. Once again, we want an effective program with an end goal that is undeniably security and resiliency oriented.

TSA should provide appropriate time for business compliance with the proposed requirements and take a risk-based approach. Below are the concerns of AFPM members with the new requirements being proposed:

a. Cybersecurity Evaluations

Cybersecurity evaluations under Section 1586.205 state that the evaluations must be conducted annually; however, AFPM urges TSA to consider aligning the NPRM with the current SDs which only require frequency based on the risk of the facility, rather than annually. The existing risk-based model from the TSA has been effective by all accounts. This approach allows the owner/operator to focus resources on high-risk facilities which is the intent of the TSA, rather than watering down efforts across all facilities. Resources are limited, even for the largest companies, and adverse effects of a non-risk based approach can inadvertently lead to a less secure environments due to overly stressed resources across the board.

b. Initial Security Evaluations

TSA should clarify whether existing SDs that have already undergone initial security evaluations need to undergo another initial security evaluation or if the requirement under 1586.205 includes owners/operators newly in scope.

c. Cyber Incident Response Plans

AFPM acknowledges the importance of implementing a robust Cybersecurity Incident Response Plan (CIRP) to protect Critical Cyber Systems from evolving threats and operational disruptions. However, the Agency should consider the resource-intensive nature of these requirements, particularly the frequency of updates, annual exercises, and strict notification deadlines, which could strain both smaller operators and larger organizations with complex systems. Additionally, we urge the Agency to address concerns surrounding the security of sensitive CIRP data submitted for compliance, as this information could pose significant risks if exposed.

d. Cybersecurity Operational Implementation Plan (COIP)

AFPM believes a longer time frame for submission of the COIP is warranted. AFPM encourages TSA to consider a 1-year time frame be allowed for submission instead of the proposed 180 days and request clarification of whether the COIP will replace the current CIP (1586.207). As written, the NPRM states that TSA's approval of a COIP becomes effective 30 days after the approval is granted. This is unnecessary and creates additional regulatory lag and uncertainty on top of the newly proposed requirement for TSA to approve amendments prior to the occurrence of a change in operations. AFPM strongly recommends TSA to strike the proposed language that would create this unnecessary delay between approval and approval effectiveness.

Additionally, requiring COIP approval before a change not only significantly deviates from current practice, but also is untenable, especially in the context of merger and acquisition activity. The SDs currently require owners/operators to request an amendment to their COIP 50 days after a permanent change. If there is a significant merger between companies 50 days after the closure of a significant merger this provision does not provide an owner/operator with sufficient time to understand differences in security philosophy across two environments—let alone review and integrate two distinct COIPs. As such, owners/operators will be faced with regulatory uncertainty in the form of requesting 90-day action plans. Moreover, a move to prior approval is impractical as those responsible for maintaining TSA compliance will likely not be aware of change with sufficient time to request an amendment to a COIP 45 days before the change will occur. TSA should allow an owner/operator to request an amendment to its COIP within 90 days of change in operations.

In addition to the high cost of compliance, the Proposed Rule also reduces security by providing yet another place (TSA files) where detailed software / attack vector information lives. With absent extraordinary justification for TSA needing this information at this level, it should be sufficient for TSA to continue its current practice (under the SDs) of simply checking that a covered entity internally maintains the required software inventory as part of its COIP implementation.

Finally, TSA should recognize that previously approved TSA assessments, such as Cybersecurity Architecture Design Review (CADRs), should be sufficient to fulfill the COIP obligation. Moreover, the timing of this evaluation should not be tied to submission of COIP.

e. Policy and Procedures Assessment

TSA should consider and propose that all policies and procedures evaluated under 1586.229 must be evaluated in their entirety every three years, rather than one third of each to be reviewed per year. This approach would streamline compliance for regulated entities rather than require unclear, staggered evaluations. A single, holistic evaluation ensures consistency and harmonization across all policies and procedures because you are looking at them at the same time.

TSA should also clarify whether owner/operators will be able to evaluate a representative sample of assets for Cyber Assessment Plan (CAP) and strike the requirement to provide Snapshot Data as identified in 1586.231(d).

f. Control Room Requirements

AFPM members are concerned about the potential overlap between TSA's requirements and existing Pipeline and Hazardous Materials Agency regulations under 49 CFR Parts 192, 193, and 195. Harmonizing these requirements is essential to avoid duplication, operational inefficiencies, and undue regulatory burdens. Additionally, the proposed measures, particularly

those related to primary control rooms managing multiple systems, introduce significant operational and cybersecurity challenges for those owner/operators previously not regulated in the SDs.

g. Withdrawal of Approval of a Security Program

Section 1570.155 of the Proposed Rule gives holders of a security program 15 calendar days to respond to a proposed withdrawal of approval, or to petition for reconsideration. TSA should lengthen the time to respond to a withdrawal of approval or to a petition for reconsideration from 15 calendar days to 30 calendar days to align with other standard regulatory processes and to allow sufficient time for business response.

h. Secure by Design

Ensuring that software that is purchased or used for critical infrastructure meets CISA Secure By Design and Secure by Default Principles is a great, aspirational concept. AFPM supports CISA's efforts to promote a more secure software supply chain. Supply chain risk management, as written, is a challenge in organizations that do not have centralized procurement. If promulgated, documentation to establish compliance should be clearly limited to items related to Critical Cyber Systems (e.g., asset inventory should be clearly limited to assets used on Critical Cyber Systems). TSA also needs to consider whether companies will be able to operate existing equipment let alone find vendors who are willing and able to certify these standards. If they cannot, this will substantially increase the cost of compliance.

Requiring pipeline owner/operators to ensure that the numerous software they employ is compliant will be difficult at best. A one-size-fits-all approach, especially in a varied space such as IT vs. OT, could easily leave owners and operators in a worse position compared to an individual owner/operator's internal robust IT/OT risk assessment process applied to proposed purchases. Setting a very prescriptive standard might unintentionally discourage some better systems because those systems, for whatever reason, don't meet the prescribed standard. Moreover, the resources required to conform to a one-size-fits-all approach will divert resources away from focusing on cybersecurity needs of the owner/operator.

At the very least TSA should develop guidance that is promulgated with the final rule. The TSA should regulate vendors directly pertaining to cybersecurity, rather than require the end user to enforce vulnerability management [1586.215]. Rather than require all contracts to include information outlined under 1586.215, it is more efficient and effective for the government require vendors to provide this information to all customers. The government should ensure technology companies in the OT space have vulnerability management planning and ensure vulnerabilities are addressed as soon as possible. Other than contracts, owners/operators have little enforcement authority compared to the government. Furthermore, there is no way to fully verify distributors/venders own supply chain so that the owner/operators can have a strong supply chain understanding and program cybersecurity risks within the supply chain based on dependencies and dependents. Finally, AFPM strongly urges TSA to apply this to prospective contracts and not retroactively, as retroactive application would call into question

perhaps thousands of existing agreements, which would require a costly review process and potentially upend many of these agreements.

h. Training and Certification Programs

TSA has expanded who is required to have training and certification programs. While regular cyber security training is beneficial, TSA should clarify the seemingly contradictory training requirements in 1586.219. For example, are employees allowed access before training is complete as long as it is done before the deadline, or are they prohibited access until training is complete? Also, in many instances, TSA has proposed training for roles that do not exist, such as "accountable executive." Given the vagueness of these terms, TSA must propose to define or propose clear, new terms that are understandable and provide notice and comment before finalizing any provisions to which terms these apply.

TSA should also consider allowing a 6-month to a year extension for training compliance, as the existing 60-day compliance requirement is likely not long enough for development and implementation of proposed training.

TSA should avoid prescriptive management of owner/operators' personnel decisions. In the Proposed Rule as is with the SDs, TSA requires covered owner/operators to designate a primary and secondary Cybersecurity Coordinator, who must be a U.S. citizen, eligible for a security clearance, and is available to the agency 24/7/365. In the proposal, TSA includes this requirement, a matching requirement for a physical security coordinator, an "accountable executive" charged with managing the Cybersecurity Risk Management (CRM) program, and is proposing to require foundational knowledge, training, and potentially baseline security vetting for certain employees. These positions could be redundant, specifically the account executive and CISOs. TSA should afford operators the authority to designate a single person to fulfill one or more of these roles and limit requisite training to those with access to Critical Cyber Systems. While AFPM understands TSA's intent in some of these proposed requirements, the agency fails to consider that covered organizations vary in size and structure, qualified personnel are difficult to attract and retain, training for sensitive security employees may encompass a significant portion of the organization, TSA security vetting is time and resource consuming, and – importantly – many of AFPM's members have operations or headquarters outside of the U.S. TSA should clearly specify the level of executive that can be considered the "accountable executive," such as a CISO, and should have a clear waiver process for certain foreign nationals that may fulfill these roles. The nationality of the CISO or account executive should not matter as long as they are qualified for that role. Limiting this to Americans might severely hamstring multinational companies.

The timelines in the NPRM for training are unrealistic (e.g., TSA requires training within 10 days of onboarding, while FERC gives 30 days for training and PHMSA provides 90 days (49 CFR 172.704)). Annual training should not be tied to a specific date—but should simply be required that it occurs annually.

i. TSA Security Threat Assessment

The Proposed Rule requests comments on whether to require accountable executives and cybersecurity coordinators to go through a TSA Security Threat Assessment. Although AFPM is not opposed to enhancing the security of our nation's critical pipeline systems by conducting limited employee threat assessments, TSA fails to justify why C-suite executives need to go through a TSA Threat Assessment. For the purposes of this rulemaking, these threat assessments should be limited to those involved with cybersecurity critical functions that could cause a significant cybersecurity event. TSA should recognize that executives and coordinators that hold a TWIC Card or a security clearance (possibly even from TSA) have an equivalency status that does not require a redundant TSA Security Threat Assessment. TSA should conduct outreach on the TSA Security Threat Assessment as there are many executives and coordinators who are unfamiliar with this program and what it entails. Ultimately, only front-line workers that are working in security sensitive areas should be required to be vetted. The vetting should also be done on a one time filing or a minimum number of filings.

j. Minimum Cyber Assessment Plan Requirements

TSA should maintain the current Cyber Assessment Plans in SD 3.1.A for this rulemaking. While TSA could consider periodic reviews, there is currently no reason to consider expanding CAP requirements.

Furthermore, AFPM strongly recommends that the TSA consider allowing owner/operators who already developed a CAP under the existing SDs not be required to resubmit their CAP documents for approval if already submitted under the current SD. Requiring all regulated entities to submit within 90 days may strain both industry resources and TSA's ability to review and approve these documents in a timely manner, as evidenced by significant delays experienced under current SDs. Additionally, we urge caution regarding the requirement to conduct a Validated Architecture Design Review (VADR) within 12 months of this rule becoming final, as it presents similar resource challenges.

k. Physical Security Incident Reporting

TSA has not provided a clear explanation for including physical security incident reporting in a cybersecurity proposed rule, nor has it explained why it thinks additional requirements and the incorporation of physical security requirements are necessary. Including physical security incident reporting under a cyber security final rule adds yet another responsibility to cyber security staff, even though they are not responsible for physical security issues and may not be directly informed of these types of security incidents. In fact, this is already in Appendix B (TSA Notification Criteria) of the TSA Physical Security Guidelines of 2021. AFPM is concerned with the proposed requirements outlined in §1586.103 and 1586.105. While we recognize the importance of comprehensive security measures, this section falls outside the intended scope of a Cybersecurity NPRM.

The inclusion of physical security provisions in a cybersecurity-focused NPRM risks conflating two distinct areas of security management. Physical security already has established

guidelines and practices tailored to address specific risks, operational realities, and stakeholder feedback. Reiterating or redefining these requirements within the scope of a cybersecurity NPRM creates redundancy and potential conflicts in compliance and enforcement.

Instead of incorporating physical security mandates into this rulemaking, we recommend TSA continue relying on and updating the current Physical Security Guidelines as needed. This approach would maintain clarity for stakeholders and avoid diluting the focus of the cybersecurity regulation. If TSA finalizes the requirement to report physical security incidents, it should only be for those incidents that affect critical operations.

l. Network Segmentation

The network segmentation proposed requirement may limit use of cloud services in the future, which could substantially increase the cost and burden on companies without a clear corresponding cyber security benefit. Enhancing monitoring, incident response, and network segmentation capabilities will require substantial investments and resources, and we recommend phased implementation timelines to account for these complexities.

m. Compliance Timelines

TSA's proposed requirements ask that covered owner/operators meet a variety of compliance deadlines. This, coupled with the introduction and revision of existing terms (i.e., Cybersecurity Implementation Plan to Cybersecurity Operational Implementation Plan) will undoubtedly create compliance confusion. TSA should reexamine the compliance obligations and proposed timelines in favor of an approach that can be uniformly applied across organizations of all sizes with limited financial and human resources.

n. Information Sharing

Throughout the SD process, TSA approached owner/operators with some flexibility in providing security sensitive information, going as far as to allow covered operators to only provide certain documents during the in-person inspection process. TSA should take this approach with the final rule. Owner/operators must have assurance that their information is secure and protected. The requirements for maintaining detailed records, such as asset inventories and network diagrams, and for mandatory incident reporting, could impose a significant administrative burden, particularly on smaller operators. We also remain concerned about the financial implications of compliance, including necessary upgrades, training, and assessments. To support industry-wide adoption, we encourage TSA to consider streamlined reporting mechanisms. Lastly, for organizations with contracts involving the DLA, further guidance on how these requirements interact with contractual obligations would be valuable.

VI. Conclusion:

AFPM members are committed to keeping our nation's critical pipelines secure. AFPM has a long history of working with TSA on security guidelines and in the development of the SDs. AFPM supports TSA taking a thoughtful approach to turning the current SDs into a final

rule that provides transparency and regulatory certainty to the pipeline industry. However, TSA may want to hold off finalizing this rule to ensure final provisions are harmonized with other regulatory programs. AFPM supports the use of an SD if quick implementation of certain security requirements is required. If TSA moves forward with finalizing the rule, then TSA should clearly limit the scope of this rulemaking to only those operator-designated Critical Cyber Systems. Similarly, AFPM encourages TSA, as well as other agencies, to work towards the harmonization of cyber security requirements, including at least the incident reporting timelines and information. AFPM looks forward to continuing our collaborative partnership with TSA as this proposed rule develops. If you need further information or have any questions, please contact me at jgunnulfsen@afpm.org or at 202-844-5483.

Sincerely,

Jeff Gunnulfsen
Assistant Vice President
Security & Risk Management Issues
AFPM