American Fuel &
Petrochemical
Manufacturers

1800 M Street, NW
Washington, DC
20036

Feb. 1, 2023

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: Enhancing Surface Cyber Risk Management - Docket No. TSA-2022-0001

To whom it may concern:

The American Fuel & Petrochemical Manufacturers (AFPM) offers the following comments on the Transportation Security Administration's (TSA) Advanced Notice of Proposed Rulemaking (ANPRM) [Docket No. TSA-2022-0001], "Enhancing Surface Cyber Risk Management."

AFPM is a national trade association whose members comprise most of the U.S. refining and petrochemical manufacturing capacity. Our members work closely with TSA and the Department of Homeland Security (DHS) in strengthening critical infrastructure security. Our members are the owners or operators of TSA-regulated pipelines in many different parts of the country. Developing practical cyber security regulations for critical pipelines is of particular importance to AFPM members.

AFPM members are committed to enhancing the cyber security of U.S. pipelines and to continuing to work collaboratively with TSA. AFPM and our members are encouraged that TSA has issued this ANPRM to explore the many complex operations and practices that are part of an organization's security environment. In these comments we will endeavor to address the questions individually and some generally by each section; however, as a trade association we cannot provide responses to questions related to specific company operations and costs.

The main points of these comments that are important for TSA to strongly consider are:

-Performance based regulations that are based on widely adopted standards (ex: the NIST Cyber Security Framework) work better than prescriptive regulations because they allow critical flexibility to allow agile response to the constantly changing cyber threats and to tailor their assessments and plans to the individual facilities and operations to protect people, assets, and operations.

-AFPM has strong concerns regarding the cost, burdens, and feasibility of imposing a one-size fits all regulatory approach to pipeline cybersecurity regulations.

-AFPM encourages harmonization of cyber security regulatory approaches rather than layering on another duplicative or conflicting requirement.

-Requiring the use of third party auditors for cyber security assessments would penalize companies that have already invested resources in developing and implementing these capabilities and expertise internally.

We look forward to continued engagement with TSA to ensure the best outcomes for the resilience and safety of pipeline operations in the United States.

Section Comments:

B. Identifying Current Baseline of Operational Resilience and Incident Response

B.1. What cybersecurity measures does your organization currently maintain and what measures has your organization taken in the last 12 months to adapt your cybersecurity program to address the latest technologies and evolving cybersecurity threats? What are your plans to update your cybersecurity program in the next 12 months? How much does your organization spend on cybersecurity annually?

Many AFPM members direct their information technology (IT) and industrial control systems (ICS) cybersecurity programs to leading frameworks and best-in-class standards, especially the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the ISA/IEC 62443 Series of Standards on Industrial Automation and Control Systems (IACS) Security. Reliance upon performance-based mechanisms, including proven frameworks and public-private collaboration, rather than prescriptive standards or regulations, is the preferred method to strengthen the cybersecurity posture of critical energy infrastructure such as pipelines. These methods and standards provide the necessary flexibility and agility to respond to the constantly changing cyber threats targeting our member’s critical assets. Additionally, over the last 12 months, many AFPM members have been working to implement the requirements of TSA’s Security Directive 2(a-c) and to convey to the TSA some of the challenges the initial prescriptive directive contained. Time spent on prescriptive measures can take away from a company’s ability to respond to changing threats in a nimble and responsive manner.

AFPM members utilize various types of assessments across their networks for various reasons. The use of assessments are based on business and operational needs that may change over time and as technology changes within an operation. Some assessments may take more time to plan or may have different risks that need to be accommodated. For instance, penetration testing may be appropriate for an IT environment but could be incredibly disruptive in the operational technology (OT) environment. IT assessments can help optimize and create efficient IT systems in order to decrease costs, reduce risk, and improve governance and security. while a vulnerability assessment is a systematic review of security weaknesses in an information system. Security vulnerability assessments evaluate if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed. The frequency of the security vulnerability assessments will differ with each company's needs.

AFPM members implement cybersecurity programs that are comprised of many components. Many AFPM members match these components with the NIST Cybersecurity Framework (CSF), a voluntary framework intended to provide a common language to use to assess and manage cybersecurity risk. Developed in response to Executive Order (EO) 13636 "Improving Critical Infrastructure Cybersecurity," the CSF recommends risk management processes that enable organizations to inform and prioritize decisions regarding cybersecurity based on business needs, without additional regulatory requirements. It enables organizations—regardless of sector, size, degree of cybersecurity risk, or cybersecurity sophistication—to apply the principles and effective practices of risk management to improve the security and resilience of critical infrastructure. Through widespread industry adoption of the NIST CSF, many AFPM member companies are able to effectively communicate cybersecurity issues for internal evaluations of capabilities and programs, internal program prioritization, and for external benchmarking evaluation of suppliers and contractor capabilities. More specifically, many AFPM members currently base their cybersecurity measures on NIST CSF. The NIST suite of standards and frameworks, including the NIST Risk Management Framework, are referenced and applied where applicable in the creation of controls, standards, processes, etc. This framework is used because it is globally recognized and provides a holistic and risk-based approach to cybersecurity. Additional benefits of the framework include the agility of the risk scaled approach for implementation and an assessment framework geared at measuring maturity of implementation. Other standards such as COBIT 5, ISA 62443, ISO/IEC 27001, NERC-CIP, etc. may also be used or reviewed to ensure companies are staying cognizant of best practices across and beyond industry.

Many AFPM members may also use the API Standard 1164 v3, *Pipeline Control Systems Cybersecurity*, published in August of 2021. The NIST CSF, API Std. 1164, as well as the ISA/IEC 62443 series of standards, provide "requirements and guidance for managing cyber risk associated with industrial automation and control (IAC) environments to achieve security, integrity, and resiliency objectives."[1]

AFPM members use various methodologies to assess physical and cyber risk to the operational environment. Two related methodologies are API Recommended Practice (RP) 780, *Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries*, and API RP 781, *Facility Security Plan Methodology for the Oil and Natural Gas Industries*. Combined, these two recommended practices provide the tools and flexibility for operators to tailor their assessments and plans to the individual facilities and operations to protect people, assets, and operations. In addition, many AFPM member use the API RP 1168, Pipeline Control Room Management, Second Edition, which provides pipeline operators, and pipeline controllers with guidance on industry best practices on control room management to consider when developing or enhancing processes, procedures, and training.

[1] https://www.api.org/products-and-services/standards/important-standards-announcements/1164.

The joint industry paper, Defense-in-Depth: Cybersecurity in the Natural Gas & Oil Industry[2] details the industry's approach to network segmentation. Below is a quote from that report that illustrates the industry's approach. More discussion can be found in the report itself.

> Regardless of the structure used for cybersecurity program development, natural gas and oil companies typically buffer ICS from cyberattacks through the use of "defense-in-depth" network architecture.
>
> Natural gas and oil companies segment their systems and implement "demilitarized zones" (DMZ) between industrial controls and internet facing business networks. FIGURE 3 illustrates an example network architecture utilizing the ISA/IEC 62443 series of standards on industrial automation and control systems (IACS) security and a modified "Purdue Model.[3]

In addition to the variety of the above-mentioned standards, AFPM members review and update the OT Cybersecurity Program Framework every 12 months to be aligned with new industrial standard requirements and technologies. This is part of our OT cybersecurity lifecycle. Other common practices AFPM members utilize are firewalls, hardening baselines, USB port blockers, various physical security measures, and security training/awareness training. Mitigating measures commonly used by AFPM members include change management, logging and monitoring, backups, threat intelligence, and intrusion detection systems.

AFPM members assess their cybersecurity programs regularly and the results of those assessments are analyzed for inclusion in operational, strategic, and tactical plans. AFPM members continually monitor the threat landscape in order to make informed risk-based decisions that shape their cybersecurity programs. AFPM members regularly assess emerging technologies for their respective areas in order to stay abreast of current capabilities and opportunities to fill existing gaps.

B.2. What assessments does your organization conduct to monitor and enhance cybersecurity (such as cybersecurity risk, vulnerability, and/or architecture design assessments, or any other type of assessment to information systems)? How often are they conducted? Who in your organization conducts and oversees them? What are the assessment components, and how are the results documented?

AFPM members conduct numerous internal and external cybersecurity assessments varying in scope, scheduling, objectives, and ownership. Examples of the types of assessments performed include architectural, vulnerability, internal audits, red/purple team, program maturity, compliance, tabletop exercises, etc. Results are documented and shared with relevant stakeholders in order to inform planning activities and facilitate risk-based decision making. Many AFPM members' IT/OT cybersecurity programs are designed and built based on the NIST, C2M2, and ISA/IEC 62443 standards. The risk assessment is performed on every new technology introduced to the OT environment. The IT/OT cybersecurity risk assessment includes network, computer systems, human, and process vulnerabilities. In addition, risk assessment verification and validation is performed every 24 months for the selected

[2] https://www.api.org/-/media/files/policy/cybersecurity/2018/defense-in-depth-cybersecurity-in-the-natural-gas-and-oil-industry.pdf.

[3] *Id.* at 14.

systems to ensure cybersecurity controls used to prevent, detect, and mitigate cyber threats are still valid. These risk assessments outlined in the standards are to be performed based on a risk target which occurs every 2 years or when a major change is made to the system (new capabilities or architectural changes).

B.3. Do the assessments you discussed in your response to B.2. use specific cybersecurity metrics to measure security effectiveness? If so, please provide information on the metrics that you use.

Generally, AFPM members' risk assessments are done according to the risk managed framework as developed by NIST. Results are documented in a formal risk register, and reviews are dictated by the security risk profile score from the risk assessments. Some of our members' risk assessments do utilize specific cybersecurity metrics to measure security effectiveness as well as maturity over time. An example of this is maturity assessments members conduct which examines each of the five NIST CSF functions and categories within both IT and OT environments. This is performed regularly, and the results are used to show growth or blocks in progress. However, specific details of a company's cybersecurity lifecycle matrix are generally considered company intellectual property and providing this information outside of an organization is not appropriate or required.

B.4. Are the actions you discussed in response to question B.1. based on any of the standards identified in section I.H. of this ANPRM? If so, please specify which standard. If your response is based on standards not identified in section I.H. of this ANPRM, please identify the standard and provide a link or other information to assist TSA in gaining a better understanding of the scope and benefits of the standard.

Yes—the NIST, MITRE, NERC, CFATS. C2M2 NIST 800-82 r3 regulations and standards. Many OT Cybersecurity Programs are designed and built based on NIST, C2M2, and ISA/IEC 62443.

B.5. For any standards identified in response to question B.3.:

a. Are there fees associated with accessing copies of these standards?
No.

b. Have you found these standards to be effective against cyber related threats? If your answer is no, please explain why.
Yes, there are benefits of adhering to various standards, for example the C2M2. This effectively evaluates and benchmarks cybersecurity capabilities in a clear and organized way, prioritizing actions and investments to improve cybersecurity and consistently measuring and demonstrating progress over time toward organization-specific goals.

B.6. "Operational technology'' is a general term that encompasses several types of control systems, including ICS, SCADA, distributed control systems, and other control system configurations, such as programmable logic controllers, fire control systems, and physical access control systems, often found in the industrial sector and critical infrastructure. Such systems consist of combinations of programmable electrical, mechanical, hydraulic, pneumatic devices or systems that interact with the physical environment or manage devices that interact with the physical environment. If your OT systems are connected to an outside network (satellite, hardline internet, port wide computer network, etc.), what safeguards are you using to protect them from cyber threats? What are the costs

to implement and maintain these safeguards? In addition, please provide details on cyber related standards or guidelines being used to guide actions assessing and mitigating threats to installed OT systems connected to vital operational equipment.

It is a common practice among AFPM members to utilize defense-in-depth methods to protect architectures supporting these types of systems. Methods include network segmentation, secure access control methods, secure architecture (DMZ, etc.) MFA, computer system and network hardening, perimeter protection through firewalls and defensive through threats strategy.

C. Identifying How CRM Is Implemented

C.1. Please describe how your organization has implemented or plans to implement CRM. What frameworks, standards, or guidelines have informed your implementation of CRM for your pipeline and rail operations? Would you recommend any other standards or guidelines not mentioned in the ANPRM for application to pipeline or provide any data available on the overall average cost to initially implement an owner/operator CRM and its annual cost to maintain (even if not a single action).

As discussed in question B1, AFPM member companies take many approaches to how they prepare for potential events, how they determine risk, and how they prepare for and mitigate those risks. Cyber risk management (CRM) is no different. Actions and approaches are based on a myriad of factors. An organization's size, diversity of operations, cyber security program maturity, risk tolerance, and resources are just a few of the factors that shape a company's approach. One company may outsource their CRM if they lack the internal capability, another company may want to bring in a third party to validate or verify what they have created internally, and another may have the resources, capability, and maturity to maintain all of their CRM in-house. There is no one-size-fits-all to how a company develops and maintains CRM, nor should there be.

C.2. Does your CRM include aspects of system protection, system penetration testing, security monitoring, incident response, incident forensics analysis, and a plan for restoration of operations? If not, which features does your CRM address? What are the challenges for incorporating any missing facets? Are some parts of CRM developed in-house while a third-party develops other pieces? If so, why, and what advantages do wither of these approaches offer?

Yes, many AFPM members' CRMs include the aspects listed above. For example, many members have overlapping layers of system and network protections combined with access to only what is required for someone to perform their job duties, and where higher-level privileges are required, leveraging separate accounts to do so. Some pieces of the aspects listed utilize third-parties due to their expertise and layer of independence provided, with the exception of pen tests—which could affect downtime and affect operations, and which most CRMs developed in house.

C.3. Does your CRM include any other core elements identified in Section II.B. or other measures not previously discussed? Are some aspects developed in-house while a third-party develops other facets? If so, why and what advantages do either of these approaches offer?

Yes, many AFPM members' CRMs include the aspects listed in II.B. and while most elements identified are in-house, a small number include third-party engagement due to their ability to provide expertise and an additional layer of independence. When utilizing third-party services, we are extremely cautious about data and information security involving third-parties due to the risk they can introduce into the environment (with or without malicious intent).

C.4. As part of implementing CRM, has your company developed or does it anticipate developing and maintaining CRM using in-house or newly acquired staff, or do you currently contract out developing and maintaining ongoing CRM to a third-party contractor or plan to do so? If your company uses a third-party or contractor to perform this function, please explain why. In addition, if you use a third-party contractor, do you have a vendor management program or framework in place? Do you have a vendor integrity audit program to ensure vendors are legitimate and have additional security measures, such as an insider threat program? Does your vendor also provide penetration testing? If CRM is or will be developed and managed in-house, what is the expected annual cost in terms of wage and hours of development and management? If CRM is or will be contracted out, what are the retainer and associated fees for the third-party? Do annual fees increase by the number of incidents they respond to and, if so, by how much?

Please see the answers provided C.2. and C.3. Many AFPM members utilize the controls specified in NIST CSF sub-category ID.SC. for supply chain, in addition to others, to ensure secure vendor practices are in place. Typically, members use a hybrid approach of both in house and third-party.

C.5. What cybersecurity personnel training and security awareness and skills education should pipeline and rail owner/operators be required to provide, and to which employees (i.e., should it apply to all employees or just those with specific responsibilities, such as cybersecurity personnel, those with access to certain systems, etc.)? Please provide relevant information regarding what CRM training courses are available and the duration of each course, as well as how much it costs you to develop and conduct or otherwise provide CRM training and update current courses and training requirements. This information should include costs for owner/operators to create or procure course content for the types of employees identified.

Many AFPM members utilize the controls specified in NIST CSF sub-category PR.AT for awareness and training to ensure general cybersecurity training for staff, as well as more pointed role/responsibility-based training.

Also, many AFPM members require cybersecurity training (video modules) to be completed by all employees annually. In addition, routine phishing campaigns are run to test the ability of the user-base to detect/avoid/report. Supplemental cybersecurity awareness and education materials are provided routinely to keep everyone aware of the ever-changing threat landscape.

C.6. How does your company address, respond to, or modify business practices due to the cost impacts of a cybersecurity incident? Does your company maintain estimates of the cost impacts (with respect to your organization and external parties) of various types of cybersecurity incidents, including but not limited to ransomware, data breaches, and attacks on operational technology? If so, what is the range of these costs based on the type or severity of the incident? Does your company

insure against these kinds of costs, and, if so, what is the annual cost of insurance, and what kind of coverage is offered? If your company does not have insurance coverage, please explain why.

Cost is not the singular or primary deciding factor when determining response. Overall risk is the deciding factor and is informed by multiple inputs (ex. environmental, loss of life, reputation, loss of revenue, etc.). However, through the After-Action Report for Cyber Incidents, if there are actions that can be done which are cost effective given the cost of the incident, then projects will be made to implement the actions.

D. Maximizing the Ability of an Owner/Operators to Meet Evolving Threats and Technologies

D.1. In addition to the requirements to report cybersecurity incidents, should pipeline and rail owner/operators be required to make attempts to recover stolen information or restore information systems within a specific timeframe? If so, what would be an appropriate timeframe?

AFPM recommends TSA take a very careful approach to regulating requirements for any critical cyber systems. As learned during the development, implementation, and revision of SD2a through c, requirements that are prescriptive or inadequately scoped can cause confusion and may not meet the performance objectives. The diversity of configurations across pipeline operators, in terms of network design, equipment, and operations mission does not comport with a one-size-fits-all approach. Bringing in the even more diverse operations of the railroads will make this challenge daunting at best. TSA should focus on the performance outcomes it desires, rather than any specific system or operation that is unlikely to be homogenous across the regulated community. Prescriptive measures can have unintended consequences and/or impact operational reliability. Any change needs to be well understood, well tested, and an operator must have the flexibility to modify the requirement if it has the potential for harm in their unique operating environment. We encourage TSA to continue to engage with operators and the TSA field personnel who are working to approve and implement the cyber security implementation plans to extract any lessons learned for this rulemaking process.

As stated earlier, companies across the sector utilize various types of assessments for various reasons. A vulnerability assessment comes with its own challenges and benefits. While identifying vulnerabilities can be helpful to a company to address said vulnerabilities, there is a risk in the collection of the information, its protection, and the nature of the assessment. Certain types of assessments can potentially have operational impacts if conducted in a manner that interferes with certain systems and processes.

Regarding the periodic requirement for penetration testing, the availability of third-party personnel is not limited to those providers. Regulated companies also need the personnel and resources to facilitate these assessments. As more CRM requirements are placed on operators, there will need to be a larger workforce of trained professionals to implement them. As noted recently, “the cybersecurity workforce has reached an all-time high, with an estimated 4.7 million professionals, but there’s still a global shortage of 3.4 million workers in this field, according to the 2022 (ISC)2 Cybersecurity Workforce Study.

In the U.S. alone, there are more than 700,000 unfilled cybersecurity jobs, data from Cybersecurity Ventures shows."[4] This challenge is not specific to the pipeline sector, but it is one facing all operators.

The workforce issue creates different challenges for different types of organizations. While some smaller organizations may have one person ultimately responsible for cyber security, in many larger organizations, this is far from the case. Consider a company that is managing IT security at the enterprise level globally but has a subsidiary operating its pipeline business domestically. The IT operations might report to the CIO of the parent company but the operational technology for the pipeline is within operations of the subsidiary and reports to the ops manager. Designating one person could be a significant challenge for the larger company. AFPM recommends that the requirement for a designated CIO should be flexible for confirmed ownership of CRM---providing the ability to designate a team or an individual, but leaving it up to the company based on its organization.

As stated throughout these comments, AFPM recommends TSA consider how the NIST CSF has been implemented in industry over the years, how it has been incorporated in other frameworks, standards, and guidance, and how they can align with those other resources. After broad recommendation through the public comment process, CISA did reorient their cross sector cyber security performance goals to better align with the NIST CSF from their initial proposal. Alignment of the NIST CSF with TSA efforts will allow operators to implement requirements more quickly, improve the efficiency of their actions, and enhance existing programs.

Regarding ransomware and recovering of information and attacker payments, this is difficult to respond to as across industry there are at differing levels of criticality and without analysis or specifics around the level of information lost, business continuity plans, impact to production, etc. being taken into consideration, AFPM cannot say if the risk outweighs the cost of payment. Finally, many victims of ransomware make payment only to find their systems are not restored or are reinfected following restoration. Again, the timeframe for restoration should be gauged on business criticality of assets and capabilities, therefore an appropriate timeframe cannot be answered in one simple unified response.

AFPM cautions against prescriptive measures in this area to account for wide variance across industry and within organizations. This should be on a case-by-case basis and at the discretion of the entity involved as there will be varying levels of data sensitivity. Owners and operators should do what they need to do to supply critical capacity and meet market expectations.

D.2. From a regulatory perspective, TSA is most interested in actions that could be taken to protect pipeline and rail systems by ensuring appropriate safeguards of critical cyber systems within IT and OT systems. What types of critical cyber systems do you recommend that regulations address and what would be the impact if the scope included systems that directly connect with these critical cyber systems? Please provide sufficient details to allow TSA to identify where and how your recommendations relate to our current requirements or recommendations, as discussed in Section I.E.

[4] https://fortune.com/education/articles/the-cybersecurity-industry-is-short-3-4-million-workers-thats-good-news-for-cyber-wages/#:~:text=The%20cybersecurity%20workforce%20has%20reached,Cybersecurity%20Workforce%20Study%20released%20Thursday.

The actions owners/operators take to protect pipeline will depend on a company's identification of systems and services which contribute to critical functions of their operations and business (production, safety, movement, etc.) and their ability to recover such systems following an incident. Those systems and services which would impact critical business/operational function during the recovery window should be considered critical cyber systems. Additional considerations depend on specific architecture within an organization and therefore should be left to each organization to determine which systems and services fall into the critical category. Reviewing and incorporating new technologies is an important aspect of a Cybersecurity Program; not all organizations have the same architecture nor require the same solution. Imposing changing benchmarks can cause loss of focus on core mitigation efforts and principles through the redirection of efforts and personnel to meet a "new" benchmark.

D.3. Recognizing that there are both evolving threats and emerging capabilities to address known threats, how could owner/operators adjust their vulnerability assessments and capabilities if TSA were to issue periodic benchmarks to pipeline and rail owner/operators on the scope of vulnerability assessments that are informed by the latest technologies and evolving threats? The purpose of the periodic guidance and assessments would be to facilitate the owner/operator's evaluation of vulnerabilities and capabilities based on the most current technologies and threats.

Many companies already utilize things such as CIS Benchmarks to ensure configurations are up to standard. These types of benchmarks are typically only available on IT type systems---the OT space depends on vendor specific information. Additionally, many (if not all) industry members regularly track emerging vulnerability information with CISA, ISACs, third-party threat detection companies, etc. and have vulnerability and threat detection programs in place. Without additional information around what an assessment would include, it is difficult to respond to this portion of the question. AFPM cautions against prescriptive measures in this area to account for wide variance across industry not only in practice, but also technology.

D.4. What are some benefits and challenges for pipeline and rail owner/operators in building operational resilience by conducting the vulnerability assessments required/recommended by TSA (whether based on the directives and information circulars discussed in Section I.E. of this ANPRM or the guidelines and assessments discussed in Section I.H.) and any assessments offered by CISA?

The challenge with vulnerability assessments includes defined and controlled boundaries to avoid unintentional operational impact and adequate data protection and privacy. Additionally, the standard against which the assessment will be conducted will be challenging if all companies are held to a single standard. There is a need to continue SD-02C practices of allowing companies to define their CIP and TAP as each company will have different vulnerabilities.

D.5. What would be the benefits and challenges for the pipeline and rail sectors if owner/operators were required to use an accredited third-party certifier to conduct audits/assessments to determine effectiveness of the owner/operator's cybersecurity measures and/or compliance with existing requirements? What would be the costs of implementing a requirement to use a third-party certifier?

Please see responses to D.4. Additionally, requiring assessments be performed by a third-party certifier would unintentionally penalize companies who have invested resources in developing and implementing these capabilities and expertise internally. AFPM recommends the continuation of inspections rather than enforcing third-party certification as the burden placed on organizations would be less without compromising cybersecurity. The value of a security assessment directly correlates to the expertise of the party administering the assessment, so if a third-party were to be used, some sort of demonstrated level of understanding and expertise should be required for accreditation, although the process would need to not be so rigorous/onerous as to dissuade or prevent a viable company from proving their capabilities.

D.6. What impacts (positive and negative) to the pipeline and rail sectors workforce do you anticipate regarding the implementation of CRM? Will there be a need to hire additional employees? If so, how many and at what level and occupation?

Where CRM does not currently exist, there will be a significant monetary strain. This is particularly concerning for smaller organizations which do not have resources available to fund this sort of endeavor. Additionally, there is concern around the need for a large number of people and resources even as the cybersecurity (even more so for OT cybersecurity) workforce is already facing a shortage. Furthermore, an organization's size and complexity will impact this number.

D.7. Should pipeline and rail owner/operators be required to conduct third-party penetration testing to identify weakness or gaps in CRM programs? Please address the identified costs and benefits of this action, and any legal, security, privacy, or other issues and concerns that may arise during the testing process or prevent third-party penetration testing.

Please see D.4. and D.5. Penetration testing is a valuable cybersecurity practice; however, prescribing that a third-party performs the testing does not seem a valuable requirement. We again defer to NIST CFR subcategory ID.RA controls for a risk-based approach to these controls.

D.8. How could TSA maximize implementation of CRM by providing for innovative, effective, and efficient ways to measure cybersecurity performance? Please provide specific references or resources available for any measurement options discussed, as available.

Again, AFPM encourages TSA to consider using existing and globally accepted frameworks (such as NIST CSF) which already accomplishes this as well as C2M2 for maturity and comprehensive pen tests to ensure technical readiness/hardening.

D.9. Should pipeline and rail owner/operators designate a single individual (such as a chief information security officer) with overall authority and responsibility for leading and managing implementation of the CRM? Or should they designate a group of individuals as responsible for implementation or parts thereof?

There is benefit in having a designated individual who determines an organization's cybersecurity program strategy and decision making. However, smaller organizations may not have the resources, or it may be infeasible for them. This should be at the discretion of the organization, as not all have the same org structure or capabilities within, so companies should have the latitude to structure it for what makes sense for them.

D.10. Should the individuals who you identified under D.8. be required to have certain qualifications or experience related to cybersecurity, and if so, what type of qualifications or experience should be required? If not, what specific requirements should there be for who would implement a pipeline and rail owner/operators' CRM program? Would implementing this type of requirement necessitate hiring additional staff? If so, how many and at what level and occupation?

Please see D.9. and consider workforce issues mentioned in D.6. regarding actual cyber security/OT security experience*.*

D.11. Should pipeline and rail owner/operators be required to monitor and limit the access that individuals have to OT and IT systems in order to protect information and restrict access to those who have a demonstrated need for access to information and/or control? Actions include limiting user access privileges to control systems to individuals with a demonstrated need-to-know and using processes and tools to create, assign, manage, and revoke access credentials for user, administrator, and service accounts for enterprise assets and software. What would be the cost of implementing this type of requirement?

For those pipeline companies which are deemed especially impactful to sustaining U.S. critical infrastructure and the economy, such as those subject to the TSA Security Directives, AFPM recommends implementing the controls seen in NIST CSF sub-category PR.AC. The cost around doing this depends on the organization's size and complexity and must consider ongoing maintenance cost. Over-provisioning of access should be avoided via implementation of least-privileged access as a best-practice.

D.12. What CRM security controls should pipeline and rail owner/operators be required to maintain, and in what manner? Please address each of the following:

a. Defense-in-depth strategies (including physical and logical security controls);
b. Network segmentation;
c. Separation of IT and OT systems;
d. Multi-factor authentication;
e. Encrypting sensitive data both in transit over external networks and at rest;
f. Operating antivirus and antimalware programs;
g. Testing and applying security patches and updates within a set timeframe for IT and OT systems; and
h. Implementing, integrating, and validating zero-trust policies and architecture.

By implementing the NIST CSF, these controls (plus others not mentioned here such as continual monitoring) are in place in a manner which equals an organization's risk appetite. Simply stating yes or no to these controls is not possible without understanding an organization's criticality, critical systems, and role within the industry supply chain. TSA should not create regulations using a one size fits all mentality without considering the vast variations present and the potential negative impact enforcing broad regulation could create by consuming limited resources within some organizations.

D.13. Please provide information on the cost to implement and integrate the CRM security controls identified in your response to question D.12.

Please see answer provided in section D.6.

D.14. What baseline level of physical security of CRM architecture should pipeline and rail owner/operators be required to maintain, including ensuring that physical access to systems, facilities, equipment, and other infrastructure assets is limited to authorized users and secured against risks associated with the physical environment? How much would it cost to implement the baseline physical security measures you identified in your response? How many of the identified measures are currently maintained (if such information has not already been provided to TSA)?

Physical security, as a principle, is applied in layers using risk and consequence as driving factors. We caution against using prescriptive measures in this area. Some mitigation efforts may work in some instances and not be cost effective or reliable in others, depending on geographical dispersion and varying architectural protections/mitigations. How that is accomplished should be decided by the company in a performance-based approach.

D.15. What would the benefits and challenges be for pipeline or rail owner/operators to build operational resilience by adopting an ''impact tolerance'' framework to help ensure that important business services remain operational after a cybersecurity incident, as provided for in the Bank of England's Operational Resilience: Impact Tolerances for Important Business Services?

Operational resilience is currently practiced across industry although the specifics will depend on each organization's existing architecture. AFPM members continually assess their cyber security environments and critical assets to better understand our operational dependencies in order to ensure minimal impact in the event of an incident.

D.16. What minimum cybersecurity practices should pipeline and rail owner/operators require that their third-party service providers meet in order to do business with pipeline and rail owner/operators? What due diligence with respect to cybersecurity is involved in selecting a third-party provider? For example, do pipeline and rail owner/operators include contractual provisions that specifically require third-party service providers to maintain an adequate CRM program? Should TSA require such provisions, and if so, for what pipeline and rail segments and under what circumstances?

Please reference NIST CSF sub-category ID.SC. for controls pertaining to vendor requirements.

D.17. How can pipeline and rail owner/operators develop a process to evaluate service providers who hold sensitive data, or are responsible for enterprise critical IT platforms or processes, to ensure that these providers are protecting those platforms and data appropriately?

Requiring vendors to provide a SOC 2 Type II report, or equivalent attestation/evidence, is a viable option for validating vendor security. Many AFPM members try to avoid allowing sensitive data to be held by vendors outside of their network.

D.18. Please address the extent to which pipeline and rail owner/operators should ensure that processes to procure control systems include physical security and cybersecurity in acquisition decisions and contract arrangements? In addition, please address the extent to which pipeline and rail owner/operators should ensure that vendors in the supply chain are vetted appropriately and that vendors vet their own personnel, service providers, and products and software.

Please reference NIST CSF sub-category ID.SC. for controls pertaining to vendor requirements.

D.19. Are there any new technologies in use or under development that may be relevant to the future of secure IT and OT systems, and how should these technologies be considered or used to establish an effective regulatory CRM regime?

The technology landscape is ever evolving and at a rapid pace. Hence, security requirements need to account for some latitude in order to be durable. Please see answers provided for D.21. as an example of where government can provide guidance as new technologies are developed. For example, GRC platforms, Priv. Access Management tools, SIEMs, and SOARs are tools that should aid in the effectiveness of the CRM regime.

D.20. Please explain how pipeline and rail owner/operators can identify and mitigate risks associated with migration of data, services, or infrastructure to a public or shared cloud storage system and/or perspective on the security benefits and challenges that may arise from the use of commercial cloud infrastructure.

The type of cloud service utilized will dictate the amount of shared responsibility owned by either the organization or the service provider. For instance, the organization could choose to utilize a third-party Software as a Service (SaaS). In this scenario, much of the responsibility of securing the customer data is owned by the third-party. An organization may opt to develop new cloud-based tools and capabilities using a Platform as a Service (PaaS). In this scenario, the organization takes on more of the responsibility for protecting the data. Finally, an organization may choose to migrate existing on-premises systems into Infrastructure as a Service (IaaS) offerings. In this scenario, the organization is mostly responsible for protecting their data. For each of these scenarios, there are different considerations to mitigate risk which are addressed by the NIST CSF ID.SC category.

D.21. How can pipeline and rail owner/operators most effectively address the risks of using very small aperture terminals networks and commercial satellite communications for remote communications? Please address how pipeline and rail owner/operators can identify and mitigate risks associated with use of these systems, which were often built for speed of communication without security in mind or specific measures to address known vulnerabilities. What **would be the cost of implementing the actions you recommend for identifying and mitigating risks associated with these systems? If cost data**

are provided, please break it down by unit and extent to which they are implemented (e.g., isolated or system-wide).

The FBI and CISA's "Satellite Guidelines" and the NSA's "Protecting VSAT Communications" documents should be considered.

> Strengthening Cybersecurity of SATCOM Network Providers and Customers | CISA
> CSA_PROTECTING_VSAT_COMMUNICATIONS_05102022.PDF (defense.gov)

D.22. What other regulatory or procurement regimes do pipeline and rail owners/operators need to comply with (e.g., are you required to comply with Defense Federal Acquisition Regulation Supplement (DFARS) requirements)? What actions/documentation can pipeline and rail owner/operators take/provide to allow TSA to consider compliance with another state or federal requirement to establish full compliance with TSA's requirements? How could TSA validate that the other requirements are, in fact, being fully implemented and provide the same level of security as TSA's requirements? Are there other regulatory regimes, potentially in other sectors or other countries, that pipeline and rail owners/operators believe would be good references for TSA?

Examples of regulations impacting owners/operators within the industry can be widespread depending on their asset diversity. A few examples include PHMSA, CFATS, MTSA, etc. We are now seeing a trend in state governments creating cyber regulations within the industry (ex. Minnesota Executive Order 22.20). There is a ***vital need for harmonization*** and/or centralization of requirements and assessment across the regulatory bodies. If TSA is considering moving to a certification process opposed to inspection***, harmonization across regulatory bodies to accept a singular certification to meet their respective requirements would be beneficial.***

D.23. How can maturity-based cybersecurity frameworks, such as CISA's Cross-Sector Cybersecurity Performance Goals and the NIST Framework for Improving Critical Infrastructure Cybersecurity,52 be leveraged in the pipeline and rail sectors to calibrate adoption in a manner that is tailored and feasible for these sectors?

Please see responses in B.1. Additionally, NIST CSF has a process for creating profiles which help tailor the framework for different industries or asset types. It would be beneficial to work with NIST to develop profiles specific to pipeline and rail which have a stronger maturity focus on the areas of cybersecurity the TSA finds most relevant. This would facilitate holistic program implementation utilizing a proven framework while also providing additional focus/tailoring opportunities. TSA should also consider mapping to the C2M2 program.

D.24. What existing statutes, standards, or TSA-issued regulations, policies, or guidance documents may present a challenge or barrier to the implementation of CRM in the pipeline and rail sectors? How could these statutes, standards, regulations, policies, or guidance documents be changed to remove the barriers or challenges? Please be as detailed and specific as possible.

The objective-based requirements seen in SD-02C, paired with the ability to describe an organization's defense-in-depth strategy was a meaningful move forward. However, as mentioned in previous sections, the primary concern is providing scalability based on criticality of an organization to the overall industry supply chain. Smaller organizations are going to struggle to implement robust or prescriptive regulations within their environments due to resource shortages. The entirety of the industry will continue to struggle with workforce challenges. Additionally, harmonization continues to become a greater issue even for larger organizations as there are competing requirements and deadlines.

D.25. How could a future rulemaking implement risk-based and/or performance-based requirements that achieve an effective cybersecurity baseline across the pipeline and rail industry?

Please see responses to questions B.1. and D.23.

E. Identifying Opportunities for Third-Part Experts To Support Compliance

E.1. How would you envision using third-party organizations to improve cyber safety and security in the pipeline and rail sectors? For example, should pipeline and rail owner/operators be able to use third parties to administer their CRM programs, and if so, to what extent and in what manner? Should pipeline and rail owner/operators use third-party certifiers to verify compliance and the adequacy of their CRM programs? Please explain the basis for your position and provide specific examples and, where possible, estimated costs.

The use of third parties for various types of activities within an operator's network, as mentioned earlier, comes with its own risks and challenges. Every time a third-party enters a network, there is a risk of loss of data or information because they are not native to that network. There is also significant concern about legitimate or nefarious removal of company sensitive data from the site. AFPM members have concerns about how the information could be used, the protections for sensitive data that would be available to a third-party and the potential of sharing non-anonymized data with any other external party, even TSA. A third-party's understanding of specific company operations also presents a challenge. A third-party familiar with the requirements of any new program may not have the expertise or knowledge of pipeline operations and specific company designs to adequately certify compliance. AFPM suggests TSA gather lessons learned from the current cyber security implementation plan process, and from this ANPRM, before pursuing third-party verification. AFPM strongly recommends TSA meet with the industry trade associations on the pros and cons of the use of third parties.

Many AFPM members believe that owner/operators should be allowed to use third parties to administer their CRM programs but should not be required to. There should be secure practices in use, such as those outlined throughout the NIST CSF, when doing so in order to minimize the risks which are introduced with or without malicious intent. It should be noted that most organizations envision getting services from trusted third-party vendors where the organizations will validate their qualifications and industrial experiences because the risk owner is the organization and not the vendor or agency.

E.2. What would the benefits and challenges be were TSA to require owner/operators to conduct compliance assessments by an accredited third-party certifier, similar to that described in the Bank of England's CBEST Threat Intelligence-Led Assessments (2021)? What features should be included in a compliance scheme that leverages third-party validators?

Please see responses in sections D.4., D.5., D.22. and E.1. Pipeline owners/operators that are already conducting compliance assessments by their trusted third-party vendors do not see value in engaging an additional assessor or third-party certifier accredited or not.

E.3. What minimum cybersecurity practices or experience should TSA require that third-party experts meet for them to do business with the pipeline and rail owner/operators?

Developing criteria for experts on certifying compliance with regulations that have not been created yet is nearly impossible. However, it would be highly beneficial for anyone assessing these types of environments to be knowledgeable in IT, OT and industry cybersecurity practices and challenges as well as commonly used standards such as NIST, C2M2, and ISA/IEC 62443.

F. Cybersecurity Maturity Considerations

F.1. What special considerations or potential impacts (i.e., risks, costs, or practical limitations) would pipeline and rail owner/operators have to consider before implementing CRM in their respective operations? Are there differences between startup costs to implement and the ongoing costs to maintain CRM? Do small entities (including business owner/operators) face unique or disproportionate costs in implementing and maintaining CRM?

Please see responses to B.1., D.6., D.12. and D.24.

F.2. What is your estimate of the percentage of pipeline and rail owner/ operators that have already implemented CRM within their organizations? If you do not know specifically, please provide us with your best estimate or any sources of data that TSA may use to determine this number. Does your organization currently have a CRM program? Do you think there are disparities between the percentages of large and small entities that have implemented CRM? If so, why, and what are they?

Based on industry conversation and the number of existing regulations touching the environments, we would estimate that the majority of pipeline and rail owner/operators have CRM implemented within their organizations. There may be disparities between the degree in which CRM practices are implemented due to the resourcing and workforce issues discussed in previous responses, as well as factors such as risk present in the environment, logical architecture, cost, and limitations of architecture for more remote sites.

F.3. Some sectors may have regulatory regimes in place imposing cybersecurity requirements. As some owner/operators may be subject to regulatory requirements imposed by multiple Federal, state, or local agencies, how should TSA most effectively achieve regulatory harmonization consistent with our transportation security responsibilities and relevant to pipeline and rail owner/operators?

AFPM strongly encourages partnership among the Federal bodies with authority and responsibility to regulate the industry in hopes of producing ***harmonized*** requirements and a single method of ascertaining compliance. Additionally, it would be beneficial to brief appropriate state governments on the resulting requirements to discourage creating their own duplicative or contradictory requirements.

G. Incentivizing Cybersecurity Adoption and Compliance

G.1. If you have implemented CRM, was implementation required or incentivized by insurance companies, existing commercial contracts, or contracts with the Federal Government? How long did it

take to implement CRM and what was the estimated cost of the implementation? What are the estimated annual costs of maintaining your CRM program?

CRM has been a longstanding practice within our membership due to our members' commitment to providing safe and reliable operations. Requirements of insurance companies, commercial contracts, or Federal contracts are merely additional incentivization.

G.2. Does your company insure against significant cybersecurity incidents? If so, what are the general terms of your insurance, and how does it factor into your decision on how to respond to significant cybersecurity incidents? What is the scope of review or audits that your insurer conducts, or requires you to conduct, in order to assess insurance worthiness?

Many AFPM members insure against terrorist/nation state attacks certified by the US government.

G.3. What tools, technical assistance, or other resources could TSA provide to facilitate compliance with any specific federally imposed cybersecurity requirement?

This answer would be more meaningful coming from organizations within industry who are struggling with resources. General ideas to consider are optional tooling availability, assessment performance teams, training, etc.

****

AFPM appreciates the chance to provide this feedback to TSA. AFPM recognizes TSA's challenge to replace the security directives and to enhance the cyber security practices of U.S. railroads and pipelines. We look forward to continuing engagement with TSA. AFPM members stand ready to provide additional information and engage TSA on these comments.

Respectfully,

Jeffrey Gunnulfsen

Jeff Gunnulfsen
Senior Director
Security & Risk Management Issues
AFPM