Submitted via www.regulations.gov.

February 5, 2025

Transportation Security Administration
Department of Homeland Security
6595 Springfield Center Drive,
Springfield, VA 20598–6028

Re: Comments of the American Gas Association
Enhancing Surface Cyber Risk Management, Docket No. TSA-2022-0001, RIN 1652-AA74, 89 Fed. Reg. 88488 (November 7, 2024)

The American Gas Association (AGA) respectfully submits the following comments in response to the Transportation Security Administration (TSA), Department of Homeland Security (DHS) proceeding[1] referenced above. The Notice of Proposed Rulemaking (NPRM)[2] on *Enhancing Surface Cybersecurity Risk Management* is an imperative regulation, and AGA strongly advocates for reasonable cybersecurity regulations.

AGA, founded in 1918, represents more than 200 local energy companies that deliver clean natural gas throughout the United States. There are more than 79 million residential, commercial, and industrial natural gas customers in the U.S., of which 94 percent — more than 74 million customers — receive their gas from AGA members. AGA is an advocate for natural gas utility companies and their customers and provides a broad range of programs and services for member natural gas pipelines, marketers, gatherers, international natural gas companies, and industry associates. Today, natural gas meets more than one-third of the United States' energy needs.[3]

AGA member natural gas utilities appreciate the opportunity to inform TSA's *Enhancing Surface Cyber Risk Management Rule* and promote the common goal of a safe and reliable natural gas system hardened against cyber risks. To this end, AGA members have worked extensively on developing comments in response to the proposed rule. Throughout the proposed rule there are ***overarching themes*** that are paramount to the successful implementation of reasonable cybersecurity regulations and to which we draw TSA's attention. These three overarching themes are:

- **Focus on Critical Cyber Systems**
  AGA strongly encourages TSA to focus the regulation only on Critical Cyber Systems (CCS). The priority should be laser-focused on the safe and reliable delivery of the commodity; in the case of AGA member utilities, this is the safe and reliable delivery of natural gas. The proposed language as written introduces potential requirements unrelated to CCS.

- **Refrain from Collecting Sensitive Security Information**

[1] Refer to the Acronyms List in Appendix A for the acronyms throughout this document.
[2] *Enhancing Surface Cyber Risk Management*, Docket No. TSA-2022-0001, RIN 1652-AA74, 89 Fed. Reg. 88488 (November 7, 2024).
[3] For more information, visit www.aga.org.

TSA should refrain from collecting and aggregating sensitive security information and insights. AGA recommends TSA reserve access to any potentially sensitive or exploitable information to on-site inspections or digital reviews. Ultimately, the owner/operators should be permitted to retain sole possession of sensitive materials and choose which materials may be submitted to TSA.

- **Maintain a Risk-Based Approach**
  TSA should adopt a risk-based and outcome-focused regulatory approach that capitalizes on owner/operators' unique operations rather than driving owner/operators to a single solution.

To organize AGA's most notable concerns, AGA divided these comments into two high-level categories: **Foundational Concerns** and **Operationally Unattainable & Ineffectively Prescriptive Requirements**. Each category is elaborated by subcategories. See Table 1.

TABLE 1: HIGH LEVEL CATEGORIES OF CONCERN

FOUNDATIONAL CONCERNS	OPERATIONALLY UNATTAINABLE & INEFFECTIVELY PRESCRIPTIVE REQUIREMENTS
• Collection of Sensitive Security Information • Prescriptive Governance • Scope Creep • Overriding Due Process • Underestimate of Costs	• Compliance Timelines • Incident Reporting • Prescriptive vs Risk-based Requirements

AGA and AGA member natural gas utilities applaud TSA's ongoing efforts to strengthen cybersecurity and resilience in the transportation sector, specifically for natural gas pipelines. By providing attainable and sustainable requirements rather than prescriptive mandates, TSA can promote regulation that preserves the operational diversity which contributes mightily to the industry's resilience.

AGA Member High Level Categories of Concern

Categories of Concern 1) *Foundational Concerns*

TSA has championed – through the pipeline security directives – a risk-based approach to cybersecurity requirements. While much of this approach is reflected in the NPRM, numerous areas in the proposed language mandate prescriptive actions that are inapplicable or unattainable. In the latter case, TSA's requirements ultimately force pipeline utility owner/operators to comply at the expense of security or at

the risk of violating State or U.S. Department of Transportation (DOT) requirements. Owner/operators should be allowed to adhere to existing corporate processes to conduct business.

We draw TSA's attention to the following concerns, which AGA considers foundational, because, as proposed, TSA is exposing the owner/operator to unintended consequences.

Collection of Sensitive Security Information

AGA continues to adamantly oppose the collection and centralization of operational and security-related information. TSA's repository is an enticing target for malicious actors.

> *For example, §1586.231 would require detailed information about operations, security measures, and normal traffic, all of which may be exploited to great effect if compromised. This information could be incorporated into an Advanced Persistent Threat (APT) attack by providing information about the normal flow of activity through a network.*

While a baseline or high-level depiction of the sensitive information may be submitted or shared on-screen for TSA's preparation of on-site audits, details should be retained at the entity and not be removed by TSA physically nor digitally. To this end, AGA recommends amending the language in §1586.231 to strike "…or copying…" to read as follows "For the purposes of the requirements in this subpart, at the time of inspection and upon TSA's request, the owner/operator must provide for inspection ~~or copying~~ the following types of information to establish compliance…[.]" Additionally, TSA should add a paragraph after §1586.231 (f) stating that all information and documentation reviewed by TSA shall remain in owner/operator possession and not leave owner/operator premises.

SENSITIVE SECURITY INFORMATION

While a baseline or high-level depiction of the sensitive information may be submitted or shared on-screen for TSA's preparation of on-site audits, details should be retained at the entity and not be removed by TSA physically nor digitally.

The following are further citations of sensitive information proposed by TSA to be submitted or made available for copying.

- The Cybersecurity Operational Implementation Plan (COIP) in §1586.207 including defense-in-depth plan, identification of critical cyber systems, network architecture, interdependencies, measures to protect Critical Cyber Systems (CCS), measures to detect cybersecurity incidents, and the Plan of Action and Milestones (POAM).
- The Cybersecurity Assessment Plan (CAP) Vulnerability Assessment in §1586.229 (e).
- The Cybersecurity Evaluation required in §1586.205 includes details of security controls.
- The measures taken to respond to compromise as required in the Cybersecurity Incident Response Plan (CIRP) in §1586.227.
- The information required in §1586.231, including asset inventory, Supervisory Control and Data Acquisition (SCADA) systems, firewall rules, network diagrams, configurations, network traffic, and log files.
- The identification of Critical Cyber Systems as required in §1586.213 and the potential operational impacts of cybersecurity incidents poses a significant threat to operators if exposed. This section

alone requests more than 13 types of sensitive information, creating a valuable and centralized repository for potential malicious exploitation.

AGA and its members support making the information listed above available to TSA during on-site inspections or through digital reviews prior to inspections, (e.g., web conference calls with screen sharing capabilities) that allow owner/operators to retain possession. The submission requirements as proposed in the NPRM create a risk for the organization that it otherwise would not have; the potential exploitation of valuable, strategic information that could enhance the impact of a successful compromise and undermine recovery. The risks to owner/operators of TSA aggregating this information far exceed any benefit to be derived by TSA's retention of these documents.

TSA is also encouraged to cite its data retention policy and ensure compliance by deleting data at the appropriate time and in a manner compliant with the policy.

Prescriptive Governance

Supply Chain Risk Management

Supply chain cyber integrity is a leading concern for owner/operators, and the proposed language compounds that concern by restricting vendor selection. The proposed supply chain requirements in §1586.215 will constrain owner/operator discretion in the selection of vendors and technologies, which ultimately introduce supply chain integrity concerns. The federal overreach into private procurement practices and, further, the transfer of risks to the regulated community by placing owner/operators in a regulatory role that they are not authorized to assume are problematic for several reasons.

First, it is unclear whether TSA has the legal authority to issue this type of procurement mandate. Under the Aviation and Transportation Security Act (ATSA), TSA has the authority to assess security risks, develop security measures to address those risks, and enforce compliance for the same.[4] AGA is unaware of any ATSA authority that allows the agency to substitute its judgment for a private entity's and steer commercial decision-making through a regulatory standard.

Second, the proposed requirements are based on cross-sector voluntary guidelines developed by the Cybersecurity and Infrastructure Security Agency (CISA), which are being inappropriately imposed as "one-size-fits-all" supply chain risk management. Procurement practices differ among owner/operators – reflecting the unique nature, risk, and safety considerations of each owner/operator's system. TSA should not prescribe procurement practices for owner/operators or dictate the outcome of private procurement decisions. To this end, AGA recommends striking §1586.215 (c), which states "[w]hen provided two offerings of roughly similar cost and function, giving preference to the offering that provides the greater level of cybersecurity necessary to protect against, or effectively respond to, cybersecurity incidents affecting the owner/operator's Critical Cyber Systems."

There is no clear way to consistently compare the level of cybersecurity between vendors, and many essential factors beyond price, function, and security are taken into consideration when selecting a vendor or service provider. System compatibility, longevity, and employee familiarity all rightfully contribute to

[4] 49 U.S.C. 114(f).

successful procurements. Relatedly, TSA should clearly state that adhering to supply chain requirements does not require renegotiation or abrogation of existing contracts.

Third, while the proposed language in §1586.215 (b) mandates that the owner/operators serve as intermediary regulators, owner/operators do not have the authority to collectively dictate incident reporting terms or evaluate the cybersecurity measures of large vendors and service providers. Owner/operators cannot guarantee contract terms and conditions, especially for highly specific industry procurements where there may be a limited number of vendors. Owner/operators may also lack bargaining power to persuade vendors or suppliers to agree to such terms or to allow for cybersecurity controls. Put simply, it is impractical for TSA to expect owner/operators to include corresponding contract terms in "[a]ll procurement documents and contracts, including service-level agreements."[5] Owner/operators cannot be held responsible for evaluating vendor or service providers as described in §1586.215 (b). These systems are beyond owner/operators' control and expertise.

DIVERSIFICATION BENEFITS NATIONAL SECURITY

Market diversity promotes sector resilience and is necessary to support varied operations.

Fourth, and most disconcerting, is that compliance with the TSA proposed requirements as written will unduly limit the number of vendors willing to offer compliant services which can ultimately introduce more risk to the owner/operator. Diversification of supply benefits industry and national security. The owner/operators can neither operate effectively without the provision of such goods or services nor can they force vendors and service providers to offer services compliant with TSA proposed requirements. Additionally, flexibility is necessary when contracting with operationally irreplaceable vendors and service providers. Owner/operators should be permitted to engage vendors and service providers in a manner consistent with their risk tolerance, available mitigations, and operational requirements. By respecting existing processes, the rulemaking would establish attainable criteria that drive attainable practices for supply chain risk management.

For these reasons, TSA should reevaluate its supply chain risk management approach in the NPRM and permit the owner/operator to apply a risk-based approach to supply chain risk management, which considers mitigating controls as appropriate. TSA has an opportunity to assist owner/operators in tackling supply chain cybersecurity integrity by leveraging the rulemaking to incorporate existing consensus-based standards by reference. Such standards require the development of a cybersecurity risk management plan addressing many of the features outlined in §1586.215, including notification by vendors of cyber incidents and vulnerabilities. Further, owner/operators should be permitted to document their security considerations within their procurement policies, which can then be audited during on-site inspections; this approach would be more effective than compelling documentation of the security considerations for each procurement.

[5] NPRM at 88587.

Pre-Approval of Program Changes

The proposed requirements in §1570.107 (b) regarding preapproval of any changes to the Cybersecurity Risk Management (CRM) Program potentially prolong vulnerability by delaying the implementation of changes. The owner/operators must retain flexibility to respond to emerging threats and exploitable vulnerabilities as soon as possible. Sidelining the implementation of necessary program changes by 30 days or more – depending on the outcome of TSA's determination – exposes the owner/operator to heightened cybersecurity risks.

Additionally, given the evolving nature of cyber threats and actors, an owner/operator may not be aware of a necessary modification 45 days ***prior*** to the need for changes. It is common for owner/operators to make unplanned changes on an expedited basis prompted by operational necessity and reliability. TSA must take operational needs into consideration and provide an expedited approval pathway or allow owner/operators to work with TSA on immediate implementation for necessary changes to policy, procedure, or measures. Ideally, TSA would afford the owner/operator the flexibility to make necessary changes and provide justification to TSA afterwards. Similarly, the preapproval of COIP changes and the 30-day delay before approved changes become effective are incompatible with responsibly addressing time-sensitive cyber risks and exploitable vulnerabilities.

The rigid approval and appeals process proposed by TSA prevents the owner/operator from pivoting in a timely manner to preserve CCS. Owner/operators should be allowed to implement changes at their discretion with reasonable notice and justification provided to TSA.

Designation of Security Coordinators and Accountable Executive

As written, §1586.103, §1586.209, and §1586.211 – detailing the requirements for the Governance of the CRM program, Cybersecurity Coordinator, and Physical Security Coordinator – ineffectively prescribe the governance of the owner/operator risk management programs. Rather than requiring the creation of new roles, TSA is strongly encouraged to defer to existing risk management plans, procedures, and organizational structures when possible.

> *For example, instead of designating continuously accessible Coordinators,[6] owner/operators should be permitted to satisfy the requirements by providing access to 24/7 operational centers (like Security Operation Centers (SOCs)) as an alternative for compliance. These round-the-clock operational centers provide immediate access to professionals for TSA while the owner/operator is not forced to change internal incident response plans or employee scheduling to comply.*

Similarly, §1586.209 (a) implies the addition of a sixth role within the proposal, "the primary individual to be contacted about the owner/operator's CRM Program" (this is in addition to the Accountable Executive, Cybersecurity Coordinator, Physical Security Coordinator, and alternates). AGA recommends that this language be modified to account for 24/7 operational centers, and that "the primary individual" be replaced by "Cybersecurity Coordinator" for owner/operators who comply with the availability requirements by designating Coordinators.

[6] NPRM at 88584 and 88586

For owner/operators without 24/7 operational centers, TSA is discouraged from requiring all Cybersecurity, Physical Security Coordinators, and alternates be perpetually available. AGA recommends the adoption of language indicating that one physical security and one cybersecurity representative be available 24/7.

> *For example, §1586.211 (b) should be rewritten as follows "The Cybersecurity Coordinator ~~and~~ **or** alternate(s) must……Be accessible to TSA and CISA 24 hours per day, 7 days a week."*

A similar change should be adopted in §1586.103. Compelling the Coordinator and the alternate to be continuously accessible diminishes the benefit of an alternate and severely curtails employee flexibility.

While AGA and its members understand TSA's intent to hold executives accountable for security, AGA strongly encourages TSA to change the requirement from "corporate level" to "management level" Coordinators. "Corporate level" is an ambiguous term; whereas "management level" is a common industry designation with wider recognition that appreciates different corporate organizational models across the sector.

> *For example, a "corporate level" Point of Contact (POC) would likely align with a parent company's corporate governance, while the CCS that falls in the scope of this regulation could be part of a subsidiary. It would not make sense to have a "corporate level" POC for a subsidiary's CCS. A "management level" POC from the subsidiary would be more appropriate. This is particularly true for larger operators and those with diversified holdings.*

Lastly, restricting the Physical Security and Cybersecurity Coordinator roles to employees with United States citizenship limits owner/operators' ability to manage their internal threat profile. Many owner/operators' non-citizen security professionals are already responsible for CCS and routinely interface with the FBI and other federal agencies on threats. The US citizenship requirement would force owner/operators to restructure their security teams and, in many cases, hire and train new security professionals. If TSA insists on a nationality restriction for these roles, AGA recommends the final rule include a specific list of countries from which citizens are ineligible to serve as Coordinators and only apply the restriction to new hires after the effective date of the final rule.

Training

Counter to TSA's approach with much of the proposed language, which is risk-based and outcome-focused, TSA is proposing a prescriptive approach to cybersecurity training requirements. Just as each pipeline system is unique, owner/operators should be provided the flexibility to design a unique training program for the employees protecting their systems. Rather than requiring approval of owner/operator training programs in §1586.219 (b), TSA should elaborate on the elements to be incorporated in a cybersecurity training program and audit these programs during on-site inspections.

Further, requiring TSA approval of training programs and their course materials introduces the unintended consequences of delays in training team members and possible reissuance of training in the same calendar year since many companies already have cybersecurity training requirements for their team members. As with the COIP, TSA and the owner/operator mutually benefit from TSA auditing the training program rather than collecting, assessing, and approving the training program materials. TSA is encouraged to

replace the prescriptive measures with a clear outline of the criteria for a training program. During program inspections, TSA should audit how well the training program designed by the owner/operator meets those criteria. AGA suggests providing the following elements for owner/operators to include in their training programs as applicable:

- Cybersecurity policies
- Physical access controls
- Electronic access controls
- Visitor control program
- Recovery plans
- Response to Cybersecurity Incidents
- Cybersecurity risks associated with removeable media
- Identification of a Cybersecurity Incident and initial notifications in accordance with the entity's incident response plan

Additionally, some training requirements in the proposed language seem arbitrary.

> *For example, the proposal should require training prior to an employee gaining access to critical systems rather than within 10 days of onboarding for cybersecurity-sensitive employees.*

TSA should focus training requirements on securing CCS. The requirement in §1586.219 (c)(1) that "[a]ll employees and contractors with access to the owner/operator's Information or Operational Technology [OT] systems, must receive basic cybersecurity training…" consumes resources without a comparable cybersecurity benefit. Employees and contractors may have limited access to systems but not work with CCS. TSA should limit the scope of this requirement and amend the proposed language to focus on those employees and contractors with access to CCS. Refocusing the scope of this requirement allows owner/operators to concentrate limited resources on training workers responsible for systems essential to the safe and reliable delivery of natural gas.

Regarding training record retention, TSA is encouraged to accept the owner/operator's record of an employee's completion of a training program rather than all the other subparts in the proposed language.

> *For example, §1586.219 (g)(1) requires the date of hire, which can lead to confusion and false impression of noncompliance, as employees shift between roles that may or may not require cybersecurity training. §1586.219 (g)(2) requires maintaining the course length and topic list, which can be administratively burdensome without a benefit to cybersecurity. Similarly, §1586.219 (h) requires indefinite record retention. Also, owner/operators should not be required to provide training records to current and especially former employees.*

Scope Creep

While other systems across a company may have a level of importance to the enterprise, TSA's mission is to "***protect the nation's transportation systems to ensure freedom of movement for people and commerce.***" Straying from these guardrails undermines the regulation's attainability and sustainability for

owner/operators and complicates compliance auditing for TSA. AGA and its members strongly encourage TSA to keep the cybersecurity regulations focused solely on those systems necessary for the safe and reliable delivery of the commodity. For the purposes of AGA's comments, the commodity is natural gas and Liquified Natural Gas (LNG).

The following comments specifically apply to areas in the proposed rule where there is notable scope creep, which has great potential to result in unintended consequences if not addressed properly. Revisions are suggested to strengthen the proposed regulations.

Critical Cyber Systems

AGA strongly encourages TSA to focus the rulemaking on mitigating risk for CCS. The proposed language requires significant reporting of incidents and documentation of operations unrelated to the assurance of CCS. The citation follows with harmful language struck and beneficial language added and bolded.

§1586.105 (a) should be amended as follows:

> "Each owner/operator identified in §1586.101 (b) must report…., ~~any potential threats and~~ significant physical security concerns ~~involving transportation-related operations~~ **impacting Critical Cyber Systems** in the United States…"

AGA also recommends amending the definition of CCS in Table 5 of the proposed rule as follows:

> "Any Information Technology or Operational Technology system used by the owner/operator that, if compromised or exploited, could directly result in an operational disruption **to the safe and reliable delivery of the commodity**~~—incurred~~ by the owner/operator. CCS include those business support services that, if compromised or exploited, could directly result in **an** operational disruption **to the safe and reliable delivery of the commodity**. This term includes systems whose ownership, operation, maintenance, or control is delegated wholly or in part to any other party."

By limiting the scope of the rulemaking, TSA properly focuses on the aspects of operations <u>most</u> essential for the safe and reliable provision of gas service. Without proper scoping, the requirements jeopardize critical operations by distracting owner/operators and TSA with compliance efforts of negligible security benefit to the underlying mission.

In particular, AGA recommends TSA clarify that this rulemaking applies <u>only</u> to CCS. When determining the criticality of a cyber system, AGA recommends the adoption of the following language "a cyber system is considered critical if it provides primary service to designated critical infrastructure and is determined by the operator to be a single point of failure, taking into consideration system redundancies, contingency plans and available mitigations."

SCOPING

Without proper scoping, the requirements jeopardize critical operations by distracting owner/operators and TSA with compliance efforts of negligible security benefit.

Additionally, AGA recommends striking §1586.213 (d) and encourages TSA to review the list of CCS on-site. TSA should audit the owner/operator's reasoning, redundancies, and mitigations rather than mandating the inclusion of systems.

Applicability Criteria Called into Question

To prevent confusion, TSA should amend §1586.1 to clearly state that only those entities meeting the criteria in §1586.101 are subject to the requirements. Additionally, the peak-shaving facility and meter/services count criteria threaten to greatly expand the regulated community.

Peak Shaving/LNG

TSA substantially underestimates the number of owner/operators meeting the applicability criteria as written in §1586.101. This gross underestimation is due in large part to the inappropriate inclusion of peak-shaving and import LNG facilities in this section.

§1586.101 (b)(7) would apply Part 1586 physical security and CRM requirements to each owner/operator of an LNG facility regulated under 49 CFR part 193 that operates as a peak-shaving facility.[7] However, unlike the other applicability criteria, §1586.101 (b)(7) does not specify any operational impact for qualifying peak-shaving facilities. As a result, §1586.101 (b)(7) would incorporate non-critical owner/operators and all of their pipeline systems and facilities. Owner/operators of critical pipeline systems and facilities with LNG facilities will already be subject to Part 1586 according to the criteria in §1586.101 (b)(1) through (6); so, §1586.101 (b)(7) will only bring in smaller, non-critical owner/operators who happen to have LNG facilities. If TSA intends to scope in critical owner/operators' peak-shaving and import LNG facilities under CRM program requirements, these facilities should be addressed in the sections of the proposed rule regarding CCS. To focus compliance efforts on protecting CCS, **AGA requests that the LNG facilities criterion be removed from §1586.101** so that the rule is appropriately applied.

Meters Threshold

The 275,000-meter threshold for applicability specified in §1586.101 appears to be arbitrarily selected. TSA provides no justification for the selection of 275,000 meters, and AGA would like to understand how TSA determined the appropriateness of this threshold. Further, TSA incorrectly conflates 'meter count' with 'service points[,]' [8] which can be two very different numbers. A great deal of thought went into designating the thresholds used for determining physical security facility criticality in the TSA Pipeline Security Guidelines.[9] AGA requests TSA share the methodology used to determine the meter threshold for the proposed rule and to distinguish between 'meter count' and 'service points.' AGA invites TSA to reach out to AGA and the Department of Transportation Pipeline & Hazardous Materials Administration for further explanation.

[7] NPRM at 88584. Defining "peak-shaving facility" as "a pipeline facility that stores liquefied natural gas to meet demand spikes."
[8] NPRM at 88584.
[9] TSA, "Pipeline Security Guidelines", 2018/2021. Retrieved from Microsoft Word - 2018 Pipeline Security Guidelines FINAL, 03-19-18.doc.

Physical Security/Physical Security Incident Reporting

Physical security requirements in this proposed rule should be restricted to the physical protection of CCS. Additionally, the Physical Security Incident Reporting requirements as proposed are too broad and should be limited to incidents that **actually jeopardize** CCS or the safe and reliable delivery of the commodity.

PHYSICAL SECURITY

Physical security requirements should be restricted to the physical protection of CCS…

Reporting requirements should be limited to incidents that **actually jeopardize** CCS or the safe and reliable delivery of the commodity.

Applying the Physical Reporting Requirements to all facilities dramatically increases the scope of the rulemaking, requiring near-constant reporting and the reallocation of limited resources without measurable return. In addition to physical incident reporting being limited to CCS, AGA recommends the reporting timeline be extended from 24 hours to 72 hours to allow the operator the opportunity to confirm incident information. As the list of reportable incidents in the proposed rule encompasses minor events unlikely to result in broader impacts, the reporting requirement could also result in inadvertent compliance violations if seemingly innocuous occurrences are not reported. To this end, AGA also recommends that the triggering event for §1586.105 (a) be **determination** of a physical security concern, rather than **initial discovery**, since owner/operators will be incapable of assessing potential threats and significant physical security concerns upon initial discovery.

> *For example, certain categories in Appendix A for Part 1586 include loitering, photography, notetaking, "asking….about particular facets of a facility's or system's purpose…" or "deliberate interactions with employees…that reveal physical, personnel, or security capabilities or sensitive information." These activities are unlikely to cause concern upon initial discovery, and reporting should be focused on incidents which could lead to impacts to CCS.*

Cyber Incident Response Plan Inclusion in the COIP

The inclusion of the Cyber Incident Response Plan (CIRP) in the COIP is unduly burdensome and creates a security risk. AGA proposes TSA return to the Security Directive approach of keeping the CIRP separate from the COIP and subject to periodic on-site inspections.

§1586.207 of the proposed rule requires that the entire §1586.227 CIRP be included in the COIP.[10] The submission of the CIRP would threaten the exposure of owner/operator highly sensitive security information, processes, and protocols if TSA's systems are successfully infiltrated. As advocated throughout AGA's comments, sensitive security information, like that contained within the CIRP, should be made available only during on-site inspections or digital reviews.

[10] NPRM at 88585.

Overriding Due Process (III(B)(2)), §1570.107(d), §1586.205)

AGA is concerned by the potential introduction of avenues by which TSA may make changes to the regulatory requirements without going through the administrative procedure.

> *For example, the TSA Evaluation Form[11] and the Lexicon are both incorporated into the proposed language by reference. This means, TSA has full control of the content of both and the ability to dramatically change the content without due process. The end result could have broad implications on owner/operator compliance efforts.*

AGA strongly discourages including by reference any non-consensus-based standards. Without a consensus-based or regulatory procedure, the owner/operator risks TSA circumventing valuable stakeholder feedback and introducing infeasible, impractical, and damaging requirements.

Cybersecurity Lexicon (III(B)(2))

CHANGES TO CYBERSECURITY LEXICON BYPASSES APA

TSA may not circumvent owner/operator procedural rights. TSA should include all relevant definitions within the rule and strike all references to the Lexicon.

While recognizing the importance of the TSA Cybersecurity Lexicon as a common and authoritative source for information, AGA strongly encourages TSA to incorporate important definitions directly into the final rule without reference to external sources. Terms, such as "Critical Cyber System," "Cybersecurity incident," "Information technology system," "Interdependencies," "Operational disruption," "Operational technology system," "Reportable cybersecurity incident," and "Unauthorized access," among others, [12] that TSA proposes to include in the Cybersecurity Lexicon are foundational to an owner/operators' compliance. The process for amending the Cybersecurity Lexicon as referenced in Section III(B)(2)[13] allows TSA to bypass administrative procedure to make sweeping changes that could increase the scope and burden of compliance. Such a result would be inappropriate and run afoul of the Administrative Procedure Act, which generally requires an agency to afford notice-and-comment procedures before amending a final rule.[14] AGA understands that TSA is seeking flexibility to react to the fast-changing terminology used in the cybersecurity space, but TSA may not circumvent owner/operator procedural rights. **TSA should include all relevant definitions within the rule and strike all references to the Lexicon.**

TSA Amending Corporate Security Plans (§1570.107(d))

§1570.107(d) provides sweeping powers to TSA to amend owner/operators' Corporate Security Plans without providing the owner/operator due process to comment. The proposed requirement would grant TSA the right to direct an amendment to a security program if, in TSA's sole discretion, the amendment

[11] NPRM at 88585.
[12] NPRM at 88505-88507.
[13] NPRM at 88555.
[14] See *Liquid Energy Pipeline Ass'n v. FERC*, 109 F.4th 543, 548 (D.C. Cir. 2024).

would be "[i]n the interest of the public and transportation security."[15] The standard TSA proposes to apply to these amendments is broad, ambiguous, and untethered to a compliance function. **TSA should strike this section from the final rule.**

If TSA believes there is a need to amend a security program, TSA should contact the owner/operator regarding the reasons an amendment might be necessary, allowing the owner/operator to address the deficiencies and resubmit to TSA on a mutually agreed timeframe. Mutual agreement to the timeframe is critical as, depending on the scope and complexity of the change to the program, a one size fits all timeframe can lead to additional work for both TSA and the entity to negotiate extensions.

Annual Cyber Evaluation (§1586.205)

As described in the preamble, the Annual Cyber Evaluation mandate in §1586.205 will be duplicative of information that is provided in the COIP and CAP. **AGA recommends this section be deleted in its entirety.** The regulatory text fails to elaborate on the content of TSA's cybersecurity evaluation form. As such, owner/operators are unable to provide feedback or commentary. Note, the unique information likely to be requested in the evaluation relates to company-wide operations that may have little or no bearing on gas assets or critical cyber systems. This represents a departure from TSA's regulatory authority.

If TSA opts to keep the Annual Cyber Evaluation, it should, at a minimum, include the evaluation form in the final rule and involve stakeholders in the creation of the evaluation form. Since the evaluation form seems designed to primarily inform TSA about the operations of newly regulated entities, TSA should grandfather any owner/operator that was governed by the family of Security Directives.[16] Further, AGA requests an extension from 90 days to one year for the initial evaluation. A thorough cybersecurity evaluation takes time to scope and complete, and 90 days is inadequate for effective evaluations.

Lack of Defined Audit Process

TSA is strongly encouraged to outline the plan for auditing owner/operators' CAPs. This allows the owner/operator to know what to expect and what to prepare to effectuate the audit.

Additionally, §1586.229 (d) states that "Owner/operators must ensure that the assessments, audits, testing, and other capabilities to assess the effectiveness of its TSA-approved COIP are not conducted by individuals who have oversight or responsibility for implementing the owner/operator's program and have no vested or other financial interest in the results of the CAP." AGA believes this section intends to ensure that operators or contractors who design controls and conduct assessments, audits, and tests are not the same as those who perform the function being reviewed. AGA member companies designate specific roles within the company to serve as independent auditors on a variety of different programs. §1586.229 (d) should be rewritten to ensure that internal teams are not disqualified from performing assessments, audits, or testing as long as they are not involved in the operation of the controls being assessed. To resolve any confusion, AGA suggests the language be revised to: "Owner/operators must demonstrate controls to maintain independence in oversight of assessing the effectiveness of their TSA-approved COIP."

[15] NPRM at 88555.
[16] Ratification of Security Directives, 90 Fed. Reg. 5491-5493 (January 17, 2025).

Underestimate of Costs

COST ANALYSIS

… the Cost Benefit Analysis may underestimate compliance costs by as much as a factor of 10.

Generally, TSA underestimates the costs of compliance. Information Technology (IT) and Operational Technology (OT) infrastructure vary widely across a diverse, and centuries-old sector, and the costs of implementing the requirements of this proposal for different utilities will vary widely as well. Variations in customer base, geographic footprint, corporate structure, in-house cyber expertise, access to vendors and services, size, and the extent of an operator's pipeline system designated by TSA as critical defy uniform cost expectations. Some owner/operators have determined TSA's Cost Benefit Analysis may underestimate compliance costs by as much as a factor of 10. TSA's estimates do not appear to capture the full costs associated with cybersecurity evaluations, physical and cybersecurity reporting, CRM Governance, Supply Chain Risk Management, Personnel Training, and the POAM as required by the proposed rule.

> *For example, TSA predicts 25.29 calls per pipeline entity per year at 3 minutes each.*[17] *However, current physical security incident reports require a longer time duration. Owner/operators estimate that preparation for a Transportation Security Operations Center (TSOC) call takes 60 to 90 minutes, and calls take between 10 to 15 minutes.*

Specifically for natural gas utilities, all costs are borne by customers – primarily residential – and must be approved by State Utility Commissions.

Categories of Concern 2) *Operationally Unattainable & Ineffectively Prescriptive Requirements*

While a substantive portion of the proposed language supports a risk-based approach to security compliance, there are certain proposed requirements that are operationally unattainable or ineffectively prescriptive. Prescriptive requirements force operators to take actions out of regulatory necessity for compliance rather than for operational integrity or security advancement. Prescriptive cybersecurity requirements disregard operational dynamics and paralyze the owner/operator, preventing the pivoting necessary to adapt to a constantly morphing threat landscape.

Compliance Timelines

SEEMINGLY ARBITRARY TIMELINES

Compliance timelines must be longitudinal and sequential rather than overlapping and dependent.

The compliance timelines proposed by TSA are aggressive, incompatible with regular business cycles, and fail to consider the factors addressed in the "Underestimate of Costs" section above. Throughout the proposed language, the compliance timelines are seemingly arbitrary with large discrepancies between the reporting requirement and compliance deadlines found in different sections of the rulemaking. Compliance timelines must be longitudinal and sequential rather than overlapping and dependent. To improve regulatory outcomes AGA recommends

[17] Transportation Security Administration (September, 2024). Enhancing Surface Cyber Risk Management – Notice of Proposed Rulemaking – Preliminary Regulatory Impact Analysis and Initial Regulatory Flexibility Analysis [Docket Number: TSA-2022-0001]. Retrieved from https://www.regulations.gov/document/TSA-2022-0001-0043.

TSA refer to Table 2, below, listing the TSA proposed language, the AGA recommendation, the AGA reasoning, and the citation.

TSA is encouraged to specify that all timelines refer to "calendar days" to prevent confusion. In general, annual timelines should be amended to read "within a calendar year, not to exceed 15 months."

While TSA proposes strict timelines for all owner/operator compliance activities, the timelines for TSA responsibilities within the rulemaking are often left undefined.

> *For example, regulated entities are expected to conduct cyber assessments, compile results, and submit reports on strict timelines, but the timeframe for TSA review of these elements is ambiguous. The absence of a defined timeline for TSA reviews could lead to uncertainty and impact subsequent actions and planning thus setting the owner/operator up for noncompliance – by no fault of the operator.*

Further, owner/operators are mandated to report significant cybersecurity incidents within 24 hours, a time-sensitive and resource-intensive requirement, while TSA's timeline for responding to or acting on this information is indefinite.

TSA is urged to elaborate a timeline for the retention of procurement documents and contracts, as required by §1586.215 (b). An indefinite retention of documents exposes owner/operator to the risk of technical noncompliance for failing to retain obsolete records. AGA recommends that retention periods throughout the rulemaking respect existing corporate retention policies.

With compliance timelines varying widely, AGA is concerned that compliance will provide logistical challenges. To help owner/operators navigate the web of competing timelines, AGA recommends the creation of a chart showing various operator/owner timelines and corresponding TSA approval dates for the different elements of the rulemaking.

TABLE 2: AGA RECOMMENDATIONS TO TSA PROPOSED COMPLIANCE TIMELINES

TSA Proposed	Recommendation	Reasoning	Citation
Reporting of significant physical security concerns: Each owner/operator identified in §1586.101(b) must report, within 24 hours of initial discovery, any potential threats and significant physical security concerns involving transportation related operations…	Within 24 hours of initial discovery should be revised to 72 hours upon IRP determination, NOT upon discovery.	Upon initial discovery, owner/operators are poorly equipped to determine whether a potential threat or physical security concern is worth reporting.	§1586.105(a)
Cybersecurity Evaluation: 90-day compliance deadline for the initial cybersecurity evaluation.	The compliance deadline should be extended to a year.	The nature and details of the evaluation are unknown. A thorough cybersecurity evaluation takes time to scope and complete, and 90 days is inadequate for effective evaluations.	§1586.205(b)
Annual updates: The evaluation required by paragraph (a) of this section must be updated annually, no later than one year from the anniversary date of the previously completed evaluation.	This section should be revised to read as follows: The evaluation required by paragraph (a) of this section must be updated ~~annually, no later than one year from the anniversary date~~ **each calendar year, not to exceed 15 months after the date** of the previously completed evaluation.	Making it based on calendar year removes a layer of confusion and respects business cycles.	§1586.205(c)
COIP Submission: No later than 180 days after effective date of final rule.	Considering all new requirements, the 180-day timeline for submitting the COIP to TSA should be extended to 1 year.	An extension is needed to comply with all the new requirements in a sustainable way. The integration of a Plan of Action and Milestones in the COIP in the event that owner/operators do not meet every requirement is a very specific and time-intensive requirement.	§1586.207(e)
COIP Submission: No later than 45 days before commencing new or modified operations. **CRM Amendment:** …an owner/operator requesting approval to amend its security program must request an amendment in advance of implementing the proposed change…at least	TSA should reinstate the following language: "The Owner/Operator must file the request for an amendment to its Cybersecurity Implementation Plan with TSA no later than 50 calendar	There needs to be an option for reporting necessary, short/no-notice operational changes after the fact.	§1586.207(e) §1570.107(b)(1)

TSA Proposed	Recommendation	Reasoning	Citation
45 days before the date it proposes for the amendment to become effective.	days after the permanent change takes effect, unless TSA allows a longer time period." From SD-02E, VI, D - *Schedule for requesting amendment*.		
COIP: After considering all relevant materials and any additional information required by TSA, TSA will notify the owner/operator's accountable executive of TSA's decision to approve the owner/operator's COIP. The COIP becomes effective 30 days after the owner/operator is notified whether its COIP is approved.	COIP should be made effective immediately or on an agreed timeline between TSA and owner/operator rather than 30 days after approval.	The reason for the delay is unclear, and operators should be able to act in accordance with an approved COIP immediately.	§1586.207 (e)(2)
COIP: Must be reviewed and updated by the owner/operator within 60 days of completing the Cybersecurity Evaluation or CAP Report.	TSA should extend the timeline for required updates to the CRM Program from 60 days from the evaluation or assessments to 180 days.	The proposed timeline is too aggressive and fails to account for the internal operational changes necessary to implement updates. The requirement to submit a Plan of Action and Milestones in the COIP in the event that owner/operators do not meet every requirement will be very burdensome for owner/operators and auditors.[18]	§1586.207 (f)
Accountable Executive: No later than 30 days from the effective date of the final rule, the owner/operator must provide to TSA the names, titles, business telephone numbers, and business email addresses of the owner/operator's accountable executive and the primary individual to be contacted about the owner/operator's CRM program. If any of the information required by this paragraph changes, the owner/operator must provide the updated information to TSA within 7 days of the change.	TSA should allow 30 days rather than 7 days for the owner/operator to notify TSA of an Accountable Executive change.	The timeline can be extended since the Cybersecurity Coordinator is the main POC.	§1586.209 (a)
Supply chain risk management: Procurement documents and contracts, including service-level agreements, incorporate an evaluation by the owner/operator or qualified third-party of the	The retention period for the documents in §1586.215 (b) should be clarified.	To ensure proper cyber hygiene and limit the likelihood of extraction by malicious cyber actors, TSA should permit owner/operators	§1586.215 (b)

[18] Making appropriate cyber supply chain determinations is likely impossible within TSA's 60-day window.

TSA Proposed	Recommendation	Reasoning	Citation
cybersecurity measures implemented by vendors or service providers of goods, services, or capabilities that will be connected to, installed on, or used by the owner/ operator's Critical Cyber Systems.		to retain these document consistent with corporate retention policies.	
Initial cybersecurity training: Each owner/operator must provide initial cybersecurity training (basic and role-based, as applicable) to employees and contractors, using the curriculum approved by TSA no later than 60 days after the effective date of the owner/operator's TSA-approved COIP required by this subpart.	Owner/operator should be allowed 6 months after the effective date of the COIP and, should it be included in the final rule, TSA's approval of the owner/operator's curriculum.	60 days is an extremely short window in which to implement a cybersecurity training program and fails to respect normal training cycles which may occur at regular intervals.	§1586.219 (d)
Recurrent cybersecurity training: Employees and contractors must receive annual recurrent cybersecurity training no later than the anniversary calendar month of the employee's initial cybersecurity training. If the owner/ operator provides the recurrent cybersecurity training in the month of, the month before, or the month after it is due, the employee is considered to have taken the training in the month it is due.	The recurrent cybersecurity training timeline should be amended from "no later than the anniversary month of the employee's initial cybersecurity training[,]" to within each calendar year not to exceed 15 months, allowing owner/operator to standardize training timelines instead of maintaining individual timelines for each employee.	The proposal requires strict adherence to a regular training cycle for each employee. The recommended change allows owner/operators to standardize their training cycle for all employees and significantly reduces the burden of compliance.	§1586.219 (e)
Retention of training records: The owner/operator must retain records of initial and recurrent cybersecurity training records for each individual required to receive cybersecurity training under this section for no less than 5 years from the date of training that, at a minimum…	TSA should allow companies to retain these records in accordance with corporate retention policies.	Owner/operators should not have to create separate retention policies for information required by federal agencies and standard business documents. Additionally, cybersecurity training is an annual requirement for most owner/operators and five years of records are unnecessary.	§1586.219 (g)
Reporting cybersecurity incidents: Owner/operator must notify CISA of any reportable cybersecurity incidents within 24 hours of identification.	Incident reporting timelines should be reconciled to Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) extending the Reportable Incident timelines from 24 hours to 72 hours.	Since cyber incidents are reported to CISA, TSA should reconcile reporting timelines with CIRCIA. TSA should not require incident reporting to CISA on a tighter timeline than the CIRCIA statute.	§1586.225 (a)

TSA Proposed	Recommendation	Reasoning	Citation
CIRP: The owner/operator must notify TSA within 15 days of any changes to the CIRP. As the owner/operator must separately notify TSA, updating the COIP to align with information provided to TSA under this section does not require an amendment subject to the procedures in §1570.107 of this subchapter.	TSA should adopt a timeline for notification of only those changes that would impact the ability to execute the CIRP.	Updates that would impact the ability to execute the CIRP should be submitted in the 15-day timeline. Owner/operator should maintain a change control log on all changes, substantive or nominal, for TSA to review when inspections are conducted.	§1586.227(f)
CAP Submission: CAP Submitted to TSA no later than 90 days from approval of COIP.	TSA should retain an annual CAP submission timeline in §1586.229 (a), consistent with the Security Directives, rather than making this requirement dependent on COIP approval.	The recommended change would allow owner/operators to adopt a regular compliance cadence without the variability introduced by COIP approval.	§1586.229 (a)

Incident Reporting

Reportable Cyber Incidents should be only those which **actually result** in operational disruptions affecting CCS. As proposed, the definition of Reportable Cyber Incident[19] will compel overreporting solely for the purpose of compliance and without measurable benefit to the owner/operator or the government. TSA's proposed definition, which requires reporting of cybersecurity incidents with "the potential to result in" operational disruption, will lead to the reallocation of limited owner/operator resources from crucial security functions to the administrative reporting of empty noise. AGA recommends adoption of a definition consistent with the CIRCIA statute.[20] Additionally, TSA should require only the reporting of ***significant*** cyber security incidents, consistent with criteria established in Presidential Policy Directive 41 (PPD-41).[21] By narrowing the definition of a reportable incident, TSA will glean valuable information that warrants attention and response.

TSA's requirement to report the details of cyber incidents to CISA within 24 hours contradicts stated harmonization goals. AGA recommends TSA align the proposed incident reporting timeframe of 24 hours with the CIRCIA statute[22] and proposed rule[23] timeline of 72 hours. TSA should not dictate a new and more demanding timeline for reporting to CISA. Additionally, TSA's proposed language obstructs owner/operator investigation, mitigation, and response/recovery efforts with administrative compliance distractions. The 24-hour reporting requirement occupies valuable resources during a critical window of time for little to no discernible value.

WHAT TO REPORT & WHEN

Reportable Cyber Incidents should be only those which **actually result** in operational disruptions affecting CCS…and align the proposed incident reporting timeframe of 24 hours with the CIRCIA statute and proposed rule timeline of 72 hours.

[19] NPRM at 88507.

[20] 6 U.S.C. §681 (2025).
("The term 'cyber incident'-
(A) has the meaning given the term 'incident' in section 2209; and
(B) does not include an occurrence that imminently, but not actually, jeopardizes--
(i) information on information systems; or
(ii) information systems.")
6 U.S.C. §650 (2025) "The term 'incident' means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system."

[21] Presidential Policy Directive/PPD-41, The White House (July 26, 2016) ("A cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people"), https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidentialpolicy-directive-united-states-cyber-incident

[22] 6 U.S.C. §681 (2025).

[23] See *Cyber Incident Reporting for Critical Infrastructure (CIRCIA) Reporting Requirements*, Docket No. CISA-2022-0010, RIN 1670-AA04, 89 Fed. Reg. 23644 (April 4, 2024).

Unreasonable and Overbroad Criterion

The reportable cybersecurity incident definition in Table 5 of the NPRM should be rewritten because it is overly inclusive and unreasonable for owner/operators to apply. Under 'criterion a,' owner/operators are required to report incidents involving "[u]nauthorized access of an Information Technology or Operational Technology system." The proposed rule defines "unauthorized access" as, "Access from an unknown source; access by a third party or former employee; an employee accessing systems for which he or she is not authorized. **This term may include a non-malicious policy violation such as the use of shared credential by an employee otherwise authorized to access it**."[24]

It is unreasonable for owner/operators, especially larger ones, to be required to detect and report every instance of qualifying, non-malicious policy violations on all systems. The result would be significant overreporting of questionable value to CISA.

Overly Complex Criteria

The incident reporting framework is unnecessarily complex. 'Criterion d' in Table 5 of the proposed rule, relies on a layering of the multiple, nested terms "reportable cybersecurity incident," "operational disruption," "business critical functions," and "supply chain expectations."[25] Neither TSA nor owner/operators can objectively and consistently apply this criterion to every potential cybersecurity incident. Adopting a definition consistent with the CIRCIA statute[26] and focusing the proposal on significant cybersecurity incidents[27] would resolve the challenges imposed on owner/operators and TSA by the NPRM's proposed layered definition of "cybersecurity incident." Simplifying and clarifying the definition will drive more consistency in owner/operator reporting and, as a result, TSA will glean more valuable information that warrants attention and response.

Prescriptive vs Risk Based Requirements

Throughout the proposal, TSA toggles between risk-based and prescriptive requirements. Where TSA is prescriptive, TSA sets the owner/operator up for failure. Three such areas pertain to the backing up of CCS, patching, and logging.

---

[24] NPRM at 88507(*emphasis added)*.

[25] d. Any other [cybersecurity incident] occurrence that, without lawful authority, jeopardizes or is reasonably likely to jeopardize the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident on the system. This definition includes an event that is under investigation or evaluation by the owner/operator as a possible cybersecurity incident without final determination of the event's root cause or nature (such as, malicious, suspicious, or benign) that results in, or has the potential to result in, [operational disruption] a deviation from or interruption of [business critical functions] an owner/operator's determination of capacity or capabilities to support functions necessary to meet operational needs and supply chain expectations that results from a compromise or loss of data, system availability, system reliability, or control of systems affecting the owner/operator's Information Technology or Operational Technology systems; other aspects of the owner/operator's systems or facilities, critical infrastructure or core government functions; or national security, economic security, or public health and safety. NPRM at 88507.

[26] 6 U.S.C. §681; 6 U.S.C. §650

[27] See Presidential Policy Directive/PPD-41, The White House (July 26, 2016) PPD-41, Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

TSA's prescribed requirements for CCS back-ups are neither feasible nor practical under all circumstances with CCS, such as with modems or other elements of the organization's configuration. See §1586.217 (e), "all Critical Cyber Systems are backed-up on a regular basis…[and]…are securely stored separate from the system, and policies require testing the integrity of back-ups…[.]"[28]

TSA should require that back-ups, where they exist, are secure rather than requiring back-ups for all CCS. Some CCS are cloud-based and dependent on the particular vendor; other CCS have no back-ups and are simply replaced when necessary. Rather than dictate to the owner/operator how and what to back up, AGA recommends TSA require owner/operators to develop a risk-based back-up strategy.

BACK-UP STRATEGY

TSA should require that back-ups, where they exist, are secure rather than requiring back-ups for all CCS. AGA recommends TSA require owners/operators to develop a risk-based back-up strategy.

With respect to patching, the proposed rule reverts to prescribing when patching must be done. Patching should be risk-based rather than mandated in the absence of "severe degradation of operational capability."

§1586.217 (c)(2) states "[i]n instances where the owner/operator cannot apply patches and updates on specific Operational Technology systems without causing a severe degradation of operational capability to meet business critical functions, the owner/operator must provide an explanation for why the actions cannot be taken…"

There are many legitimate reasons an operator may not apply a security patch within the normal timeframe.

For example:

1) *If patches have not been validated by SCADA software vendors.*
    a. *If owner/operators are running a patch that is not supported, it can invalidate support contracts.*
    b. *Waiting for vendor support or guidance to ensure the patch is applied correctly and safely.*
2) *If applying patches would require system downtime, which might not be feasible during critical operational periods.*
    a. *Some owner/operator's critical operational period refers to a specific timeframe (heating season) during which the continuous operation of systems and processes are essential to avoid significant negative impacts.*
3) *If the patch is likely to result in significant Financial Impact(s)/Resource Constraint(s)*
4) *If patch deployments interfere with planned/ongoing projects that may be dependent on unpatched systems.*

[28] NPRM at 88588.

Additionally, AGA recommends that TSA clarify this requirement only applies to security patches. Functional patches should be excluded, as the decision to install them is a business matter.

Lastly, the two sections of the Proposed Rule that require logging by CCS should be modified to reflect that logging is not possible by all OT devices. Specifically, AGA recommends that the words "where technically feasible" be added in the appropriate places in §1586.217 (b)(4)(iii) – *Access Control* and §1586.217 (d) – *Logging Policies*.

In closing for this section of the comments, AGA cannot overemphasize the benefits of a risk-based approach, which were discussed ad nauseum with the first iteration of prescriptive Security Directives. TSA is encouraged to review the Technical Roundtable discussions hosted by TSA in Spring 2022 and return to the risk-based approach for this rulemaking and afford owner/operators the flexibility to apply alternate mitigating controls and pivot as necessary to the evolving threat.

NPRM-Specific Request for Comments

TSA asked for industry feedback on a variety of topics. Below are AGA member responses to this request.

Question 1) Impact of regulations and requirements being imposed by other Federal, State, and Local entities, including DHS components, and potential options for regulatory harmonization.

AGA encourages TSA to coordinate with other regulatory authorities, including but not limited to the United States Coast Guard, the Federal Energy Regulatory Commission, the Department of Transportation Pipeline and Hazardous Materials Safety Administration (PHMSA), and the Department of Energy to minimize redundancies and effectuate compliance. In particular, AGA urges harmonization with the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) requirements to which many natural gas utilities are already held for their electric operations. Reducing redundancy eases the compliance burden and frees the regulated community to advance the actual work of protecting and recovering from cyber incidents. Definitional consistency across regulations will also clarify requirements and relieve confusion. Where possible, TSA should align its definitions with the CIRCIA statute specially regarding reportable cyber incidents. TSA's definition of a reportable cyber incident is overly broad and could needlessly inundate TSA with reports – distracting TSA as well as the owner/operator from significant and operationally disruptive incidents. Additionally, harmonization is necessary to prevent contradictory regulatory requirements. For example, physical incident reporting requirements in §1586.105 could easily violate state privacy laws, like the California Consumer Privacy Act[29] or the Illinois Public Utilities Act.[30] AGA encourages TSA to actively engage state regulators and regulated entities to better understand the long-extant cybersecurity regulatory environment for pipelines.

[29] See California Consumer Privacy Act (CCPA). (2018). *California Civil Code* §§ 1798.100 – 1798.199. Retrieved from https://oag.ca.gov/privacy/ccpa

[30] See Illinois Compiled Statutes. Chapter 220. Public Utilities Act (Act 5). Retrieved from Illinois Compiled Statutes | Act 5 - PUBLIC UTILITIES ACT | Casetext

Question 2) Whether proposed requirements for supply chain risk management should also include requirements to ensure that any new software purchased for, or to be installed on, Critical Cyber Systems meets CISA's Secure-by-Design and Secure-by-Default principles.

AGA supports the encouragement of vendors to abide by CISA's Secure-by-Design and Secure-by-Default principles. However, requiring these principles for all new software has the potential to undermine market integrity – limiting product offerings to a smaller pool of vendors, increasing prices, enhancing the scale of potential compromise, and limiting support. Owner/operators should be allowed to mitigate risks associated with their software choices and select the software that best complements continued operations. Market diversity promotes sector resilience and is necessary to support varied operations.

Also, without further guidance, this requirement would be infeasible. Currently, there is no established process for validating adherence to Secure-by-Design and Secure-by-Default principles. Additionally, owner/operators should not be made responsible for ensuring vendor compliance with Secure-by-Design and Secure-by-Default Principles.

Question 3) Existing training and certification programs that could provide low-cost options to meet proposed qualification requirements for Cybersecurity Coordinators. If identified and determined by TSA to be sufficient, TSA could recognize them as examples for owner/operators that would be subject to these requirements.

AGA encourages widespread TSA reciprocity with existing training programs. Many owner/operators have certifiable training programs, selected to prepare employees to administer, manage, and sustain systems that complement business operations. By allowing owner/operators the flexibility to administer risk-based, outcome-focused training programs, TSA will support effective and efficient compliance while promoting diverse training that aligns with diverse operations.

Question 4) TSA is proposing to require owner/operators to have a Cybersecurity Assessment Plan (CAP) to annually assess and audit the effectiveness of their TSA-approved Cybersecurity Operational Implementation Plan (COIP). TSA is requesting comments on methodologies owner/operators could use to develop a plan that would meet the required annual minimum for assessments and audits, assessment and auditing capabilities that could be included in the CAP, and other options and resources that could ensure a robust auditing and assessment program that provides frequent and regular reviews of effectiveness of CRM program implementation.

AGA discourages annual testing requirements and urges TSA to consider a risk-based approach for control testing. More frequent testing of high-risk controls will promote effective allocation of resources for the reduction of enterprise-wide risk. Many operators already test critical controls regularly and test other controls on a longer cadence consistent with operational necessity and risk management plans.

Question 5) TSA is requesting comments from pipeline owner/operators on opportunities to streamline compliance and reduce redundancies and duplication of efforts for pipeline facilities regulated under 33 CFR 105.105(a) or 106.105(a).

This question is nonapplicable for AGA members.

Question 6) TSA is requesting comment on whether accountable executives and Cybersecurity Coordinators, for all covered owner/operators, should be required to undergo a TSA-conducted Security Threat Assessment (STA), which would include a terrorism/other analyses check, an immigration check, and a criminal history records check (CHRC).

AGA recognizes the importance of ensuring that accountable executives and Cybersecurity Coordinators undergo thorough vetting. At the same time, requiring a TSA-conducted Security Threat Assessment (STA), including terrorism and other analyses check, presents several challenges.

First, the implementation of such assessments could result in significant administrative and operational burdens on the owner/operator. More importantly, there is great potential for delays in onboarding or assigning necessary company personnel if TSA's review is mandated on top of already existing owner/operator procedures for vetting. The time and resources required to conduct these checks could delay critical cybersecurity initiatives and impact overall efficiency.

Second, given the sensitive nature of these roles, maintaining a balance between security and privacy is important. This proposal should be carefully evaluated to ensure it does not infringe upon the privacy rights of individuals or create unintended consequences for the organization.

Lastly, AGA suggests considering alternative approaches that leverage existing internal vetting processes and compliance programs. Many organizations already have robust security and background check procedures in place that could be aligned with TSA requirements, to minimize redundancy and optimize resource allocation. For example, entities that must comply with NERC CIP should be able to leverage those procedures and controls prior to approving access to CCS or CCS data. Alternatively, TSA may offer to conduct Security Threat Assessments as an option, while also publishing criteria that would allow owner/operators to conduct a similar assessment themselves. These minimum requirements allow the owner/operators the flexibility to choose TSA provided services or to conduct their own process which meets minimum requirements.

AGA recommends TSA work closely with covered owner/operators to develop a streamlined and effective vetting process that addresses security concerns while maintaining operational efficiency and respecting privacy considerations.

Question 7) TSA is requesting comments on whether TSA should require all frontline workers (''security-sensitive employees'') in the pipeline industry to also be vetted by TSA. Although TSA is not proposing this requirement, TSA seeks comments on how the vetting would impact their operations and costs, and specifically how many employees the entity has that would likely be considered security-sensitive employees.

Implementation of this requirement would exponentially increase administrative, personnel, and legal expenses with minimal added value to cybersecurity. Cybersecurity is an extremely competitive field and delays in onboarding processes can lead to loss of qualified candidates to other sectors. If such a requirement were adopted, it should not apply to all frontline workers, as many positions lack the ability to cause widespread disruptions. Alternatively, a voluntary, no-cost TSA screening option for all new hires and existing employees could complement an owner/operators flexible, risk-based approach.

Question 8) TSA is requesting comments on the inputs used in the Regulatory Impact Analysis (RIA), including those related to the Security Directives (SDs), their implementation, and associated costs and benefits. Comments that will provide the most assistance to TSA will reference a specific portion of this proposed rule, explain the reason for any suggestions or recommended changes, and include data, information, or authority that supports such suggestion or recommended change.

The Regulatory Impact Analysis underrepresents industry's costs for compliance. By incorporating suggestions within these comments and leveraging accurate data, TSA can develop a more effective and sustainable regulatory framework that balances security needs with operational and financial realities. AGA recommends that the TSA reevaluate the cost estimates for SD implementation by incorporating data from a diverse range of covered owner/operators. Consultation with owner/operators indicates the compliance costs presented in the NPRM may be underestimated by as much as a factor of 10. Thorough consultation with the different segments of the oil and natural gas pipeline industries will inform a more accurate understanding of the financial and resource commitments required for compliance. AGA recommends a formal Request for Information so that this important aspect of the rulemaking receives attention consistent with its significance.

Given the substantial resource allocation required, AGA is urging TSA extend the implementation timelines to allow organizations adequate time to comply without compromising other critical operations.

To mitigate the financial impact, we propose exploring support programs that can assist organizations in meeting the regulatory requirements without undue financial strain.

Question 9) TSA invites all interested parties to submit data and information regarding the potential economic impact on small entities that would result from the adoption of the requirements in the proposed rule.

AGA does not have comments at this time.

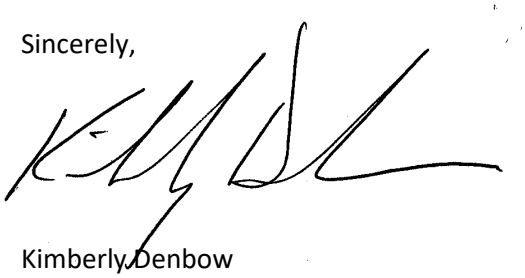
Question 10) TSA invites comments on the proposed collection of information and estimates of burden.

As elaborated in more detailed comments above, the proposed collection of information is burdensome, and often without a justifying benefit to industry or the public. AGA strongly recommends TSA require the submission of only high-level information, (e.g., general procedures that support compliance and records to demonstrate the implementation of controls). Submitted records should be allowed to be redacted as necessary. The CIRP, network diagrams, CCS information, and other highly sensitive information should be provided only during on-site inspections.

In closing, AGA and AGA member natural gas utilities thank TSA for the opportunity to contribute to the knowledge base that will be leveraged by TSA for the development of risk-based cybersecurity regulations. Our shared mission is ensuring the security of the safe and reliable delivery of natural gas. AGA and AGA's members look forward to continuing our work toward this common goal.

Should you have any questions, please do not hesitate to contact Kimberly Denbow at 202-824-7334 or kdenbow@aga.org.

Sincerely,



Kimberly Denbow
Vice President, Security & Operations
American Gas Association

APPENDIX A

ACRONYMS LIST

AGA	American Gas Association
APT	Advanced Persistent Threat
CAP	Cybersecurity Assessment Plan
CBT	Computer-Based Training
CIP	Critical Infrastructure Protection
CCS	Critical Cyber System
CIRCIA	Cyber Incident Reporting for Critical Infrastructure Act of 2022
CISA	Cybersecurity and Information Security Agency
COIP	Cybersecurity Operational Implementation Plan
CPG	Cybersecurity Performance Goals
CRM	Cybersecurity Risk Management
CSA	Cloud Security Alliance
DHS	U.S. Department of Homeland Security
DOT	U.S. Department of Transportation
FBI	Federal Bureau of Investigation
FERC	Federal Energy Regulatory Commission
IRP	Incident Response Plan
IT	Information Technology
LNG	Liquified Natural Gas
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards Technology
NRC	Nuclear Regulatory Commission
OT	Operational Technology
PHMSA	Pipeline and Hazardous Materials Safety Administration
POAM	Plan of Action and Milestones
SCADA	Supervisory Control and Data Acquisition
SD	Security Directive
SOC	Service Organization Control
TSA	Transportation Security Administration
TSOC	Transportation Security Operations Center