Kimberly Denbow
Vice President, Security & Operations
American Gas Association

Testimony before the House Homeland Security Committee Subcommittee on Transportation & Maritime Security

"Impacts of Emergency Authority Cybersecurity Regulations on the Transportation Sector"

November 19, 2024

Chairman Gimenez, Ranking Member Thanedar, and members of the Subcommittee, I am Kimberly Denbow, Vice President of Security and Operations, at the American Gas Association (AGA). I have led AGA's security policy and technical program for nearly three decades. I am a former voting member of the Transportation Security Administration (TSA) Surface Transportation Security Advisory Committee and helped stand up and co-chaired the Cybersecurity Subcommittee. I also stood up and presently co-chair the Cybersecurity Working Group of the Oil & Natural Gas Subsector Coordinating Council. Additionally, I have worked with TSA and its pipeline security section since TSA's inception. Thank you for inviting me to share my perspectives on the natural gas utility experience with TSA, specifically as they relate to how TSA puts its regulatory authority into practice.

AGA, founded in 1918, represents more than 200 local energy companies that deliver clean, domestic, and reliable natural gas throughout the United States. There are more than 78 million residential, commercial, and industrial natural gas customers in the U.S., of which 95 percent – more than 74 million customers – receive their gas from AGA members. Today, natural gas meets more than one-third of our nation's energy needs. AGA members recognize that with the benefits and opportunities natural gas offers our country, there comes great responsibility to protect our distribution pipeline system network from cyber compromise.

AGA members have been at the forefront of cybersecurity investment and are continually seeking ways to improve their cybersecurity readiness. The AGA Board of Directors passed a resolution in 2021 in favor of reasonable cybersecurity regulations, and AGA and its members engage in every opportunity to work with federal government partners and regulators to promote risk-based cybersecurity programs that support security measures that are attainable, sustainable, and auditable. This includes extensive work with TSA to help strengthen and add value to the pipeline

Security Directives (SDs)[1] and reduce risk for the industry. Risk-based cybersecurity aligns with the National Security Memorandum on Critical Infrastructure Security and Resilience[2].

Technological advances continue to make natural gas operations safer, more cost-effective, and better able to serve customers via web-based programs and tools. The corollary to a more connected and more efficient industry is our attractiveness as a target for increasingly sophisticated nefarious cyber actors. This said, America's natural gas utilities are combatting the threat daily via:

- Skilled personnel,
- Robust cybersecurity system protections,
- Industry commitment to security,
- Collaboration with other industries and associations,
- Ongoing cybersecurity partnerships with the federal government, and
- Interaction with the Downstream Natural Gas Information Sharing & Analysis Center (DNG-ISAC) Community for real-time awareness and action.

A Common Mission – Protecting America's Natural Gas Utilities

AGA and its member companies are committed to utilizing leading security practices and training, investing in purposeful security technologies, and promoting an industrywide vigilant security culture to fortify our security defenses and enhance all aspects of safety. TSA's mission is to "Protect the nation's transportation systems to ensure the freedom of movement of people and commerce"[3]. To that end, America's natural gas utilities and TSA share a common mission – critical infrastructure and operator security.

In a cojoined journey over two decades, TSA and natural gas utilities have challenged the traditional prescriptive regulatory model, piloting unconventional approaches to achieve this common mission. All parties acknowledge that "check-the-box" compliance does not equate to security, and that numerous paths can lead to the same security outcome. The following provides an overview of AGA and AGA-member natural gas utility experience with TSA in its role as the federal pipeline security regulator but also as a model of functional public/private partnership.

Structured Oversight

TSA was created in the aftermath of 9/11 to oversee the security of multiple transportation modes including commercial and general aviation, mass transit systems, freight and passenger rail, and

[1] Security Directive Pipeline 2021-01, issued May 26, 2021: *Enhancing Pipeline Cybersecurity* (SD1), and Security Directive Pipeline 2021-02, issued July 19, 2021: *Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing* (SD2). The SD's have been reissued annually since 2021. Per TSA Administrator David Pekoske, the SDs will continue to be reissued until cybersecurity regulations are promulgated.

[2] National Security Memorandum on Critical Infrastructure Security and Resilience, The White House, (April 30, 2024), available at https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/ (last visited November 15, 2024).

[3] TSA's Mission Statement, TSA, available at https://www.tsa.gov/about/tsa-mission (last visited November 15, 2024).

highways, pipelines and ports[4]. TSA became part of the Department of Homeland Security in March 2003 and organizationally consists of two primary divisions, aviation and surface transportation.

The general public associates TSA with airport security, and historically, the majority of transportation security funding goes to aviation security. Secondary to aviation, TSA regulates security operations for the four surface transportation modes – mass transit, freight rail, highway motor carrier, and pipeline.

TSA's first decade of surface transportation security operations was organized by mode. For example, TSA operated a Pipeline Security Branch, staffed by subject matter experts, who understood the complexities of pipeline commerce (e.g., transporting liquids differs from transporting natural gas) and collaborated with pipeline owners/operators to learn the security nuances of individual pipeline systems. While this branch of TSA had full authority to regulate pipeline security, it opted for an unconventional and more effective non-regulatory, collaborative model TSA coined as "structured oversight." TSA chose this methodology in part because a one-size-fits-all regulatory approach was inappropriate given operational variations between the natural gas and liquid hydrocarbons (e.g., oil) value chains. While the structured oversight approach is resource intensive for TSA to effectively prepare, conduct, and follow up on security inspections (as well as track security threats), this collaborative method represents a common public-private mission, benefits both the regulator and regulated entity, and advances pipeline sector security.

This organizational structure changed in the 2012/2013 timeframe. TSA eliminated dedicated modal branch security operations for each surface transportation sector in favor of a multi-modal oversight system where TSA surface transportation staff may or may not have specific expertise necessary to evaluate the infrastructure they were assigned. The Pipeline Security Branch's full-time equivalents (FTEs) were reduced by 93% (from 14 down to 1)[5]. AGA publicly expressed concern about replacing TSA pipeline subject matter experts with generalists. Nevertheless, and despite this ill-advised decision, the collaboration between TSA and pipeline owners/operators did not wane.

Over time at industry's urging, TSA has steadily rebuilt pipeline security capability and personnel. For example, TSA Administrator David Pekoske's testimony before the U.S. Senate Committee on Commerce, Science, and Transportation on July 27, 2021, notes that passage of the *TSA Modernization Ac*t allowed TSA to "...expand pipeline security staff to 39 FTEs working in field operations, headquarters operations, and policy development…[and] trained a 20-member field-

[4]TSA at a Glance Factsheet, TSA, available at https://www.tsa.gov/news/press/factsheets/tsa-glance-factsheet (last visited November 15, 2024).

[5] Critical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management, GEO, (Dec. 18, 2018), available at https://www.gao.gov/products/gao-19-48 (last visited November 15, 2024).

based Pipeline Security Assessment Team (PSAT)..."[6] Today, TSA continues to collaborate with owners/operators to learn about their pipeline systems and improve methods to secure pipeline infrastructure overall.

TSA Pipeline Security Guidelines

The *TSA Pipeline Security Guidelines* (Guidelines)[7] are the heart of the structured oversight model and serve as a foundation upon which pipeline owners/operators have built their security programs for the last two decades. The Guidelines were developed and updated in tandem with pipeline owners/operators and government cohorts, including the Pipeline & Hazardous Materials Administration, the Department of Energy, the Department of Homeland Security (DHS), and the Federal Energy Regulatory Commission (FERC). While adoption of the Guidelines is voluntary, TSA maintains the authority to regulate as necessary.

The first edition of the Guidelines in 2010 mainly focused on physical security (given the events of 9/11) rather than cybersecurity. Following the targeted Chinese cybersecurity campaign[8] against pipelines in 2013, the Guidelines were revised to align with the National Institute of Standards and Technology (NIST) Cybersecurity Framework[9].

Implementing the Guidelines prepares pipeline owners/operators for TSA onsite Corporate Security Reviews (CSR) and Critical Facility Security Reviews (CFSR). CSRs assess the degree to which the Guidelines' physical and cybersecurity measures are integrated into the operator's corporate security plan. CFSRs are conducted at critical pipeline facilities to collect site-specific information on facility security policies, procedures, and physical security measures[10]. Overall, CSRs and CFSRs have historically focused more on physical security and are intended to serve as an opportunity for TSA to work collaboratively with owners/operators to advance security, in notable contrast to an adversarial standard regulatory compliance methodology.

As TSA develops cybersecurity capabilities, AGA encourages TSA to also maintain its attention on physical security. For example, a widely-used TSA resource, the *Pipeline Security Smart Practices*[11], is a compilation of valuable physical security practices observed from CSRs and CFSRs. For a few years, TSA did not update the resource due to directing full attention to the

---

[6] Pipeline Cybersecurity: Protecting Critical Infrastructure, TSA, (July 7, 2021), available at https://www.tsa.gov/news/press/testimony/2021/07/27/pipeline-cybersecurity-protecting-critical-infrastructure (last visited November 15, 2024).

[7] Pipeline Security Guidelines, TSA, (March 2018), available at https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf (last visited November 15, 2024).

[8] Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013, CISA, (July 2021), available at https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-201a (last visited November 15, 2024).

[9] Cybersecurity Framework | NIST (last visited November 15, 2024)

[10] Pipeline Cybersecurity: Protecting Critical Infrastructure, TSA, available at https://www.tsa.gov/news/press/testimony/2021/07/27/pipeline-cybersecurity-protecting-critical-infrastructure#:~:text=Working%20with%20pipeline%20operators%27%20security,the%20operator%27s%20corporate%20security%20plan. (last visited November 15, 2024).

[11] Pipeline Security Smart Practice Observations, TSA, (September 19, 2011), available at https://www.tsa.gov/sites/default/files/tsapipelinesecuritysmartpracticeobservations_2011_508.pdf (last visited November 15, 2024).

SDs. Regularly adding to this resource assists those owners/operators that have not yet undergone a CSR or CFSR.

Additionally, from a threat perspective, TSA continues to miss the mark in characterizing the physical security threat level to domestic pipelines. Despite owners/operators reporting increasing incidences of pipeline sabotage activity, including malicious vandalism, intentional damage to pipeline infrastructure, trespassing and unauthorized operation of pipeline valves and other equipment, finding improvised explosive devices on pipeline infrastructure, and assaults on pipeline operators and contractors, TSA consistently presents the physical security threat level as low. It is our understanding that this threat level assessment is not sourced from within TSA. Regardless, it is incumbent on TSA to reconcile the discrepancy between what the federal government intelligence community is observing and what the pipeline owners/operators are experiencing. The federal government's mischaracterization of the pipeline physical security threat level not only threatens pipeline security readiness, it also negatively impacts gas utility security investment. Natural gas utilities are state regulated via public utility commissions (PUCs), which oversee customer rates and utility expenses and investments. The more TSA continues to underestimate pipeline security threats, the more difficult it is for natural gas utility owners/operators to justify pipeline security investments to state PUCs.

Growing Cybersecurity Capabilities

While the Colonial Pipeline ransomware incident in 2021 propelled TSA into regulating pipeline cybersecurity, TSA considered the importance of pipeline cybersecurity well before 2021. The Chinese cyber campaign targeting pipelines that surfaced in 2012[12] led to a cybersecurity paradigm shift across the pipeline industry and TSA. Over the decade that followed, TSA and pipeline owners/operators worked collaboratively on:

- Applying existing federal government-developed cyber assessments tools,
- Developing a pipeline-specific cyber assessment,
- Conducting DHS Validated Architectural Design Reviews,[13]
- Updating the cyber section of the Pipeline Security Guidelines to align with the NIST Cyber Security Framework,[14] and
- Developing API 1164 3rd edition, *Pipeline Control Systems Cybersecurity,*[15] a consensus-based standard worked on by owners/operators, vendors, and federal government representatives (including TSA and FERC).

[12] Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013, CISA (July 21, 2021), available at https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-201a (last visited November 15, 2024).
[13] Validated Architecture Design Reviews (VADR) Sample Report, CISA, (December 17, 2020), available at https://www.cisa.gov/resources-tools/resources/validated-architecture-design-review-vadr-sample-report (last visited November 17, 2024).
[14] Cybersecurity Framework, NIST, available at https://www.nist.gov/cyberframework (last visited November 17, 2024).
[15] API Standard 1164, 3rd Edition, API, (August 2021) available at https://www.api.org/products-and-services/standards/important-standards-announcements/1164 (last visited November 17,204).

By that time, TSA had worked with pipeline owners/operators long enough to recognize that there is strength in operational diversity and that system disruptions and consequences will differ substantially across the natural gas and oil value chains – and further within the different segments of each value chain (e.g., natural gas utility, natural gas transmission, LNG operations). Beyond basic cybersecurity hygiene, there is no single cybersecurity law, regulation, or standard that can be universally applied across pipelines and LNG operations without having to allow the option of alternative measures or system-by-system customization. TSA further recognized it needed to build up its internal cybersecurity expertise despite minimal funding available for pipeline security, let alone for pipeline cybersecurity.

Despite this concerted effort by TSA to thoughtfully approach the development of cybersecurity regulations for the broader pipeline industry, public pressure in the aftermath of the Colonial Pipeline ransomware incident drove TSA to immediately issue a series of prescriptive emergency Security Directives (SDs) covering pipeline cybersecurity. The initial SDs were filled with unattainable cybersecurity measures and compliance timelines that, rather than improving sector cybersecurity, actually increased pipeline system vulnerability and threatened system reliability. The first iteration of pipeline cyber SDs was a textbook case study of what a regulator should not do.

TSA as Cybersecurity Regulator

Pipeline Security Directives - An Informed Regulator

The first iteration of SDs, specifically the *Security Directive Pipeline-2021-02* series (known as SD2[16], was unreasonably prescriptive, without regard for pipeline owners/operators cybersecurity system applicability, operational feasibility, and compliance timelines. They were issued as a one-size-fits-all, prescriptive cybersecurity measures to TSA-designated critical oil and natural gas pipeline systems. AGA worked tirelessly with every level of TSA to draw attention to the impracticality, ineffectiveness, and financial irresponsibility of these prescriptive measures, which would have resulted in minimally improved security, but at the expense of increased cybersecurity vulnerability in many pipeline systems.

Reflecting two decades of genuine collaboration between TSA and pipeline owners/operators, TSA ultimately agreed to host Pipeline Security Directive (PSD) Technical Roundtables (Technical Roundtables) on SD2 to hear directly from owners/operators about how these mandated cybersecurity measures were unattainable, and that there were alternative and more effective approaches TSA should consider. “On July 21, 2022, TSA issued Security Directive Pipeline-2021-02C, transitioning the requirements of the previous versions in the [SD2] series to be more performance-based and less prescriptive. The performance-based approach enhanced security by mandating that critical security outcomes are achieved while allowing owners/operators to choose the most appropriate security measures for their specific systems and operations.”[17] Bottom line, the TSA Technical Roundtables resulted in a major regulatory course correction that eliminated prescriptive and unworkable cybersecurity requirements in favor

[16] Security Directive Pipeline 2021-02, issued July 19, 2021: *Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing* (SD2). The SD2 is labeled Sensitive Security Information.

[17] Federal Register :: Ratification of Security Directives (last visited November 17, 2024).

of an almost entirely performance-based and outcome-focused regulation. The credibility established between TSA and owners/operators prior to the Colonial Pipeline ransomware incident and reinforced through Technical Roundtables continues to inform improvements to subsequent iterations of the SDs. Particularly noteworthy, TSA's Surface Operations leadership regularly hosts forums to garner feedback from owners/operators regarding ways to strengthen SD implementation and owners/operator compliance.

The pipeline sector has now complied with nearly four years of emergency TSA SDs, and it is highly possible the SDs will be extended into a fifth year or longer. With each iteration, there is a refinement of components in the expiring SD. This is positive. Not so positive is the addition of cybersecurity technical mandates in each new iteration that are inapplicable, confusing, extremely costly, and disruptive to owners/operators, who must substantially alter their compliance procedures from those required by a previous version of the SD. TSA can avoid this ineffectiveness by conducting regular Technical Roundtables in advance of each future iteration. Proactive Technical Roundtables offer owners/operators the chance to clarify new regulatory definitions, requirements, and compliance measures as well as limit potential misinterpretations by TSA and pipeline owners/operators. A proactively informed regulator is less likely to promulgate unclear, misinformed, and unworkable regulations.

SD Governance – While Purposeful, Needs Guardrails

SDs serve a logical purpose – imminent threats require immediate action. That said, long-term compliance with multiple iterations of SDs over multiple years raises due process concerns because, unlike the standard regulatory process, regulated entities have minimal official input into how SDs are developed and enforced. While there is benefit with leveraging SDs to improve on regulatory requirements before the mandates are embedded into final rules, each iteration of the current SDs has resulted in reallocation of industry resources. This constant pivoting for the sake of regulatory compliance distracts from an owners/operators risk reduction efforts, and it makes securing resources (e.g., such as qualified labor force) difficult.

Furthermore, regulating by SD is at odds with how natural gas utilities operate. SDs, by design, do not allow long-term planning. In contrast, natural gas utilities necessarily rely on multi-year capital budgeting and infrastructure investments. Even nominal increases in annual costs can be extremely challenging. Internally, well-planned cybersecurity plans must be reprioritized if the owners/operators must wait for TSA to "approve" changes in cyber plans and assigned personnel. Externally, state PUCs maintain regulatory oversight over natural gas utility expenses and require owners/operators to have clearly defined plans for implementation, sustainability, and benefit to the gas utility customer.

Finally, SDs have a different governance framework than traditional rulemakings. SDs can be issued by the TSA Administrator in response to an imminent threat without due process procedures and activities, such as public comment or economic burden analysis. SDs expire after 12 months, at which time they can be reissued. While recognizing that TSA should maintain some reasonable emergency authority to issue SDs, Congress should consider placing guardrails and time limits on this regulatory mechanism to reduce its potential to be abused or misused.

Rulemaking

In late 2022, following the extension of the original SDs into a second year, TSA issued an Advanced Notice of Proposed Rulemaking. AGA member utilities supported this action, favoring reasonable pipeline cybersecurity regulations provided they are attainable, sustainable, and auditable by TSA. As 2023 progressed, pipeline owners/operators urged TSA to proceed with a pipeline cybersecurity rulemaking rather than continuing to regulate by SDs. The Notice of Proposed Rulemaking for this, now multi-modal, rule was not released until November 7, 2024. Had TSA moved a pipeline-only cybersecurity rulemaking, the whole process would have likely concluded a year ago. While we understand TSA's interest in consolidating three surface modes into a single rulemaking, this has unnecessarily prolonged the SD process for pipelines. Bottom line, we recognize the urgency that drives the issuance of SDs, however, there need to be guardrails to limit the "regulating-by-SD" approach so that government and the affected industry can quickly and appropriately move toward a standard regulatory process.

Relative to the recently released NPRM, AGA commends TSA for issuing proposed rules that are risk-based, outcome-focused, and for the most part, an extension of the recent iterations of the pipeline SDs. That said, two areas within the NPRM, corporate cybersecurity governance responsibilities and supply chain cybersecurity integrity are prescriptive, confusing, and in some cases unachievable and were never covered in TSA's previous pipeline SDs. A third area, employee cyber training, was introduced in the most recent SD, but is fully and unhelpfully prescriptive in the NPRM. These unexpected regulatory roadblocks could have been circumvented had TSA hosted Pipeline Security Technical Roundtables (similar in structure to the Pipeline Security Directive Technical Roundtables) before drafting the proposed regulation. TSA missed opportunities to gain useful owners/operator insight and avoid stakeholder confusion.

Federal Government Possession of Owners/Operators Sensitive Operational Information

While the federal government is driving itself to a zero trust[18] approach, TSA's NPRM proposes to collect and aggregate security and operations-related sensitive information of critical infrastructure; thus, preventing those owners/operators from achieving the same zero trust environment the federal government has been directed to achieve. Many entities in the federal government have been negligent and unsuccessful at protecting owners/operators sensitive information. One glaring example occurred when the DHS Cybersecurity & Infrastructure Security Agency's (CISA) Chemical Security Assessment Tool (CSAT)[19] was successfully hacked and compromised for multiple days before CISA realized the breach had occurred. The CSAT contains chemical facility security vulnerabilities and plans that owners/operators were mandated to submit.

[18] No entity is trusted by default from inside or outside the network, and verification is required from everyone trying to gain access. See Zero Trust Architecture, GSA, available at https://www.gsa.gov/technology/it-contract-vehicles-and-purchasing-programs/information-technology-category/it-security/zero-trust-architecture#:~:text=Zero%20trust%20is%20an%20approach,and%20enterprise%20infrastructure%20and%20workflows (last visited November 15, 2024).

[19] Top-Screen Surveys, Security Vulnerability Assessments, Site Security Plans / Alternative Security Programs, Personnel Surety Program Data, and CSAT User Information.

Given the significant implications of the CSAT breach, it is imperative to address the need for all government entities, including TSA, to be held accountable for the collection, aggregation, and protection of sensitive operations information. What were at one time considered adequate cybersecurity measures for the CSAT data storage still resulted in a breach. Despite government's stringent safeguards and robust incident response protocols, no systems are impenetrable. Effective oversight and enhanced security frameworks on the government's own networks are essential to protect national security interests and not create risks for the owners/operators. More importantly, government should ask itself, "why is possession of sensitive private sector operational information necessary?" AGA and its member companies value government partnership but also seek to limit the vulnerabilities introduced by demonstrably subpar government cybersecurity performance.

Cybersecurity Reciprocity and Harmonization

Cybersecurity harmonization has become a catchphrase that deserves to be placed in perspective. While applicable for cybersecurity assessments and cybersecurity incident reporting, harmonization of cybersecurity regulations is a chokehold for any risk-based, outcome-focused cybersecurity regulatory approach. The majority (if not all) of existing cybersecurity regulations involve prescriptive, check-the-box compliance, which is simpler for the government to measure than performance-based security. Given this landscape, harmonization approaches that do not explicitly endorse performance-based cybersecurity will fail to recognize the operational differences across the oil and natural gas value chains that drive the necessity of risk-based cybersecurity regulations. Along similar lines, government wide reciprocity for relevant agency-led cybersecurity inspections and audits would benefit sector regulators by reducing duplicative evaluations and help improve regulated communities' cyber readiness. Arguably, inspection reciprocity has greater potential than harmonization and can be acted on with less bureaucracy for all stakeholders.

In Closing

America's natural gas utilities recognize their attractiveness as a vector and target for nefarious nation state hackers and cyber criminals. AGA member utilities combat the threat daily by leveraging top notch cybersecurity technologies and personnel and maintaining a productive security partnership with the federal government, in particular TSA. No single standard or prescriptive regulation can secure all pipeline systems along both the natural gas and oil value chains. TSA recognizes this and is admirably taking the more difficult – while more sound and effective - path of implementing performance-based cyber requirements that will be attainable and sustainable by the owners/operators and auditable by the regulator. AGA encourages the government to learn from the successes of TSA in their genuine collaboration with industry owners/operators and encourages TSA to recount the security successes that result from proactive collaboration. Over the decades, TSA and pipeline owners/operators have carried a similar banner into battle in support of our common mission.