**Statement of**

**Chad Gorman, Deputy Executive Assistant Administrator for Operations Support**

**Steve Lorincz, Deputy Executive Assistant Administrator for Security Operations**

**Transportation Security Administration**

**U.S. Department of Homeland Security**

**Before the**

**United States House of Representatives**

**Committee on Homeland Security**

**Subcommittee on Transportation and Maritime Security**

**On**

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

**November 19, 2024**

**Washington, D.C.**

Good morning, Chairman Gimenez, Ranking Member Thanedar, and distinguished Members of the Committee. My name is Chad Gorman, and I serve as the Deputy Executive Assistant Administrator for Operations Support within the Transportation Security Administration (TSA). I am joined today by Deputy Executive Assistant Administrator for Security Operations, Steve Lorincz. We appreciate the opportunity to appear before you today to discuss TSA's role in cybersecurity for our nation's transportation infrastructure.

TSA was established by the *Aviation and Transportation Security Act* (ATSA), which was signed into law on November 19, 2001. With the enactment of ATSA, TSA assumed the mission to oversee security in all modes of transportation, be that aviation or the Nation's surface transportation systems – mass transit and passenger rail, freight rail, highway and motor carrier, pipeline, as well as supporting maritime security with our U.S. Coast Guard (USCG) partners. In the years since 9/11, TSA has not only had to address the ever-present physical threats to aviation and surface transportation modes, but also dynamic and emerging cybersecurity threats to our nation's aviation, rail, highway and motor carrier, hazardous liquid, and natural gas pipeline infrastructure. This is not a mission we can accomplish alone. TSA's mission success is highly dependent on close collaboration and strong relationships with our transportation industry stakeholders and our federal, state, and local partners, including the Department of Transportation (DOT) as the Department of Homeland Security's (DHS) co-Sector Risk Management Agency for the Transportation System Sector.

**Transportation Cybersecurity Threats**

The August cyberattack at the Seattle-Tacoma International Airport serves as another reminder of the significant disruptions and broader impacts cybersecurity incidents can cause to transportation. Cyberattacks are an evolving and persistent threat. Cyber threat actors, including nation states, have demonstrated their intent and ability to conduct malicious cyber activity targeting critical infrastructure by exploiting vulnerabilities present in both Operational Technology (OT) (the hardware and software that controls physical devices, processes, and infrastructure) and Information Technology (IT) systems. Unlike traditional kinetic threats we confront, cyber threats are not bound by global borders. They can cross vast distances between our adversaries and U.S.-based critical transportation infrastructure in seconds, drastically impacting our ability to respond successfully with our more traditional and time-bound approaches. Nation state actors like Russia, China, Iran, and North Korea recognize cyber capabilities bypass geographical limitations and,

accordingly, they have developed and demonstrated capabilities that pose significant cyber threats to the United States The Director of National Intelligence has stated that our adversaries and strategic competitors possess, and in the case of the People's Republic of China (PRC), have prepositioned cyberattack capabilities that could be used against U.S. critical infrastructure, including transportation, especially during times of increased conflict.

This year, the Intelligence Community assessed that the PRC almost certainly could launch cyberattacks that could disrupt critical infrastructure within the United States, specifically highlighting oil and gas pipelines and rail systems. In May 2023, the Cybersecurity and Infrastructure Security Agency (CISA) issued a joint Cybersecurity Advisory which highlighted for the first time a cyber threat cluster associated with the PRC identified as Volt Typhoon. There have been subsequent documents released on Volt Typhoon by CISA and other U.S. Government agencies. Volt Typhoon has been active since at least mid-2021 and targets U.S. critical infrastructure entities, including those in the transportation sector. Volt Typhoon's choice of targets and pattern of behavior is not consistent with traditional cyber espionage or intelligence gathering operations, and the U.S. government assesses with high confidence that Volt Typhoon actors are pre-positioning themselves on IT networks for disruptive or destructive cyber activity against U.S. critical infrastructure in the event of a major crisis or conflict with the United States. Observed behavior suggests Volt Typhoon intends to maintain access without being detected for as long as possible by relying almost exclusively on stealthy "living-off-the-land" techniques in which the cyber threat actor uses legitimate, built-in network administration tools to sustain, advance, and conceal an attack.

In April 2023, after receiving a briefing on the relevant intelligence, the Transportation Security Oversight Board (TSOB) recommended to TSA that a cybersecurity emergency exists that warranted the TSA Administrator's determination to expedite the implementation of critical cyber mitigation measures in aviation, which he had done through the exercise of his emergency regulatory authority by issuing Joint Emergency Amendment (EA) 23-01. Joint EA-2301 on March 7, 2023. The Joint EA amended the security programs for covered aviation entities to require performance-based cybersecurity measures intended to prevent the disruption and degradation of their critical systems. Additionally, in April of this year, President Biden extended the national emergency on malicious cyber-enabled activities, citing the continued significant and malicious activities that are posing an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States.

TSA is dedicated to protecting our Nation's transportation networks against evolving cyber threats and continues to work collaboratively with public and private stakeholders to expand the implementation of intelligence-driven, risk-based policies and programs and continue active information sharing within the federal government and with industry to reinforce the security posture of these networks.

**Addressing Cybersecurity Threats Through Unique TSA Authorities**

In response to these evolving threats, the TSA Administrator has utilized his emergency authorities found in both statute and regulation. In statute, Congress provided the TSA Administrator authority to issue regulations and security directives (SDs) immediately to protect transportation security. *49 U.S.C. §114(l)(2))*. In doing so, the Administrator may waive certain procedural requirements for traditional notice and comment rulemaking to carry out TSA's transportation security mission. SDs issued under this authority are subject to review by the Transportation Security Oversight Board (TSOB). The TSOB was established by the *Aviation and Transportation Security Act of 2001 (ATSA)* and consists of seven statutorily prescribed voting members, including DHS. DOT, Department of Justice, Department of Defense, Treasury Department, Office of the Director of National Intelligence, and National Security Council. The Board is chaired by the DHS Deputy Secretary. The TSOB is charged with reviewing and ratifying, or disapproving, any regulation or SD issued by the TSA Administrator under section 114(l)(2) within 30 days after the date of issuance. If a regulation or directive is not ratified by the TSOB, it may remain in effect for no more than 90 days. To date, the TSOB has reviewed and ratified all of TSA's surface cybersecurity SDs. The TSOB also has discretionary authority to review and make recommendations to the Administrator regarding transportation security plans. *(49 U.S.C. §115)(c)(5),(6))*. Under this authority, the TSOB provided its recommendation to TSA regarding a cybersecurity emergency warranting emergency action in the aviation sector.

By regulation, the TSA Administrator has the authority to issue emergency amendments to the security programs of regulated aviation operators. (*49 CFR §§1542.105, 1544.105, and 1546.105)*. The Administrator may use this authority upon finding that there is an emergency requiring immediate action with respect to safety and security in air transportation or in air commerce. The Administrator has additional regulatory authority to issue SDs to regulated aviation operators where it is determined that additional security measures are necessary to respond to a threat assessment or specific threat. (*49 CFR §§1542.303 and 1544.305.)*

The TSA Administrator's ability to leverage these authorities and respond immediately during emergency situations has significantly mitigated threats posed by a rapidly evolving, and increasingly volatile, cyber environment. The TSA Administrator's emergency authorities are essential and vital to the Nation's transportation security.

**Examples of TSA's Cybersecurity Program**

Immediately following a 2021 ransomware incident impacting a major US pipeline company, there was a clear understanding across the Administration, Congress, industry, and the public for the need to prevent future pipeline cybersecurity incidents. The Administration turned to TSA and the TSA Administrator leveraged his authority under 49 U.S.C. §114 to respond to emerging cyber threats by directing owners and operators of certain pipeline and natural gas facilities to implement a set of select cybersecurity protections to mitigate the threat. The TSA Administrator issued two SDs in 2021 to immediately address these threats. Among the many requirements, the SDs required pipeline companies to report cybersecurity incidents to CISA within 24 hours after they identify a cybersecurity incident; to designate a cybersecurity coordinator and alternate that is available to TSA around the clock; and to implement specific mitigation measures to protect against ransomware incidents.

Credible cyber threat information also supported the TSA Administrator's use of his emergency authority to implement additional security measures to U.S. surface (pipelines and railroads) and aviation (airports and air carriers) transportation networks. In regard to the surface transportation security domain, the cybersecurity SDs require higher risk pipelines, freight railroads, passenger rail, and rail transit operators to take several critical actions (rail transit operators only require the first three):

1. Develop and submit to TSA a Cybersecurity Implementation Plan (CIP) to achieve performance-based security outcomes;
2. Develop and maintain an up-to-date Cybersecurity Incident Response Plan (CIRP) to reduce the risk of operational disruption following cybersecurity incidents;
3. Develop and submit to TSA a Cybersecurity Assessment Plan (CAP) to ascertain the effectiveness of cybersecurity measures and to identify and resolve device, network and/or system vulnerabilities; and

4. Develop and submit to TSA an annual report that provides the results of the Cybersecurity Assessment Plan from the previous year.

Within aviation, the TSA Administrator used his regulatory authority to amend established security programs of the nation's largest air carriers and airports to include cybersecurity. Like the surface SDs, these amendments started with requirements to designate a Cybersecurity Coordinator, report cybersecurity incidents to CISA, and to develop a CIRP. They now also include requirements to develop a CIP and CAP and to allow TSA to inspect these documents.

In promulgating these SDs and security program amendments, TSA engaged with stakeholders to enhance understanding of the threat landscape and gather industry feedback. This included stakeholder discussions at the CEO-level with DHS and TSA leadership, classified threat briefings for industry, multiple policy reviews by industry and government stakeholders, and consistent engagement sessions with transportation associations and regulated entities for awareness on the proposed strategies. Through these regular engagements with industry partners, we quickly learned that our initial approach to cybersecurity in surface modes was too prescriptive. This approach limited innovation and hindered industry's ability to quickly respond to evolving and emerging dynamic cyber threat landscapes. Based on that feedback, TSA quickly transitioned our regulatory framework in 2022 to an outcome focused, performance-based model that remains our model to the present day in both surface and aviation modes. This rapid shift to performance based SDs versus prescriptive SDs demonstrates the flexibility of TSA's emergency authorities and highlights the power of collaboration with our industry partners to collectively address security issues with measures tailored to specific transportation environments.

Since August 2023, TSA also led several in-person and virtual meetings to discuss the pipeline SDswith pipeline owners and operators from various associations and companies. Additionally, TSA hosts a bi-weekly call with the owners and operators subject to the rail SDs to share information and answer questions on the SDs and inspection requirements. Similar calls have begun within the last few months for airports and air carriers. In these engagements, TSA also discusses its cybersecurity policy and strategy, identifies opportunities for improvement, and provides contextual information via the sharing of intelligence and incident information.

Finally, TSA also engages regularly with TSA's Surface Transportation Security Advisory Committee (STSAC) and the Aviation Security Advisory Committee (ASAC) to share and discuss security requirements, issues, and challenges. These statutorily created committees

include representation from the interagency and industry. Whenever able, we will continue to engage with industry partners prior to issuing new security requirements.

Concurrently with these efforts, TSA published a Notice of Proposed Rulemaking (NPRM) that would codify the provisions of the SDs for certain surface modes of transportation into a Cybersecurity Risk Management Program. This proposed rule opened for public comment on November 8, 2024. It continues TSA's commitment to performance-based requirements, builds on TSA's previously issued cybersecurity requirements from the SDs and seeks to establish a sustainable and comprehensive cyber risk management program for owners and operators that have higher cybersecurity risk profiles. Our routine engagements with stakeholders, as well as coordination with inter-agency partners such as DOT, USCG, and CISA, have been critical in this process – as with the SDs, their feedback has informed decisions on the proposed rulemaking.

Within the aviation sector, TSA continues to partner with aviation entities on elevating their cybersecurity stance. TSA has partnered and communicated, at the appropriate level based on the maturity of the covered parties, cybersecurity program changes to their cybersecurity programs. As of October 1, 2024, TSA has reviewed and approved over 70 percent of the cybersecurity implementation plans and conducted several inspections of covered parties.

Within the surface modes, all pipeline CIPs have been approved, and nearly all rail plans have been approved. In preparation for the SD CIP inspections, owners and operators were contacted by their Regional Security Director or inspection point of contact well in advance of the inspection to provide details and to coordinate any documentation in advance to ensure all parties were properly prepared. As of May 2024, TSA completed all initial pipeline inspections. By the end of Fiscal Year (FY) 2024, 96 percent of rail inspections have been conducted.

With the approved CIPs in surface, most owners and operators have developed and submitted their CAPs to test the effectiveness of the measures outlined within their CIPs. As of October 23, 2024, TSA has approved 99 percent of pipeline and 45 percent of rail CAPs.

**Information Sharing and Engagement**

Our work does not simply end after issuing these cybersecurity requirements. On the contrary, TSA continues its robust stakeholder engagement to mitigate cyber threats. We work closely with covered owners and operators to successfully implement these requirements, educate our vast network of transportation owners and operators, and continue to seek input from both the

STSAC and the ASAC on how to best integrate cybersecurity into the fabric of our transportation security mission. TSA conducts extensive outreach with thousands of individual transportation owners and operators to implement these requirements and ensure consistent application across the transportation sector. We continually seek opportunities to expand information exchanges and to provide evaluation tools and training programs to evaluate systems, identify vulnerabilities, and incorporate security measures and best practices that mitigate cyber threats.

On behalf of DHS, TSA and USCG are each a Co-Sector Risk Management Agency for the TSS along with the DOT. In this role, TSA serves with the USCG as the executive agents for developing, deploying, and promoting TSS-focused cybersecurity initiatives, programs, assessment tools, strategies, and threat and intelligence information-sharing products. TSA is in close alignment with CISA and coordinates on both a tactical and strategic level to raise the cybersecurity baseline across the transportation systems sector.

Under the proposed CISA Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) rule published on April 4, 2024, all entities within the TSS—that are currently required to report to TSA—will also be required to report to CISA. The proposed rule is in line with TSA's SDs and security programs that require certain transportation entities to report cybersecurity incidents, as defined by TSA, to CISA within 24 hours of identification. Regulated entities complying with TSA's requirements do not need to make a duplicate report to CISA; all TSA reporting requirements are satisfied via CISA's web-based incident reporting form and CISA shares such reports with TSA. Although CIRCIA requirements do not limit TSA's authority to impose cybersecurity reporting requirements, define reportable incidents more broadly than CISA, or impose a timeframe for reporting that is shorter than the timeframe required by CIRCIA, TSA has ensured that cybersecurity reporting is integrated with the system under development by CISA.

Information and intelligence sharing is a key enabler of TSA's mission to protect the Nation's transportation systems to ensure the freedom of movement for people and commerce. TSA facilitates both classified and unclassified briefings for trade associations, industry executive leadership, and key industry security personnel representatives to ensure full understanding of the evolving threat picture. As previously stated, TSA's commitment to information sharing with industry is strongly supported by two full-time threat intelligence sharing cells—the Aviation Domain Intelligence Integration & Analysis Cell (ADIAC) and the Surface Intelligence Sharing Cell (SISC). Through these entities, TSA shares thousands of threat items, including cyber threat

intelligence with cleared stakeholders. These two intelligence sharing cells are excellent examples of government and industry partnership, and their establishment resulted directly from stakeholder collaboration. Close collaboration with our public and private partners will continue to inform TSA's next steps in the cybersecurity arena.

Finally, we would like to thank Congress and this Subcommittee for your support of TSA's transportation security mission and securing the funding for critical cyber resources in FY 2024. The FY 2025 President's Budget Request, if enacted, will fund specially trained personnel to accelerate cybersecurity inspection and compliance efforts across the entire TSS. TSA will use the funding to emphasize aviation and surface sector resiliency, use of cyber-tools, a trained cyber response staff, a cyber analytical staff, and a regulatory support staff. We recognize the continued need to recruit, train, and retain cybersecurity professionals within TSA. Through recruitment and retention incentives, to include supporting cybersecurity development training opportunities and cybersecurity certifications for personnel, we continue to build our cybersecurity workforce, positioning TSA to effectively tackle the evolving cybersecurity threat as supported by recent budget requests.

Chairman Gimenez, Ranking Member Thanedar, and distinguished Members of the Subcommittee, thank you for this opportunity to share the steps and measures TSA has taken in concert with our stakeholders to strengthen transportation critical infrastructure to address the serious and persistent cybersecurity threat. TSA is committed to ensuring appropriate security measures are in place to increase the cybersecurity defenses of our Nation's most critical transportation systems. I look forward to answering any questions you may have.

**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.

**STATEMENT OF**

**IAN JEFFERIES**

**PRESIDENT AND CHIEF EXECUTIVE OFFICER**

**ASSOCIATION OF AMERICAN RAILROADS**

**BEFORE THE**
**U.S. HOUSE OF REPRESENTATIVES**

**COMMITTEE ON HOMELAND SECURITY**

**SUBCOMMITTEE ON TRANSPORTATION**
**AND MARITIME SECURITY**

**HEARING ON**
**IMPACTS OF EMERGENCY AUTHORITY CYBERSECURITY REGULATIONS ON THE TRANSPORTATION SECTOR**

**NOVEMBER 19, 2024**

**Association of American Railroads**
**425 Third Street SW**
**Washington, DC 20024**
**202-639-2100**

## Introduction

On behalf of the members of the Association of American Railroads (AAR), thank you for the opportunity to testify on how the rail industry works with our government counterparts to address cyber threats and the impacts of emergency authority on those efforts. AAR's members account for the vast majority of North American freight railroad mileage, employees, and traffic.

Freight railroads integrate skilled personnel and ingenuity with technology to keep the network infrastructure safe and the supply chain moving every day. Advanced information and communications technology are helping our employees in every aspect of our operations, including train control, track and equipment inspections, emergency response, dispatching, railcar tracking, locomotive fuel management, predictive performance analysis, employee training, and much more. Cybersecurity is an arms race between attackers and defenders, which is why our highly skilled, highly trained employees work diligently to continually enhance their capabilities and guard against cyberattacks that threaten the safety and integrity of our operations.

For 25 years, railroads have maintained a dedicated coordinating committee focused on cyber threats, effective risk mitigation practices, and engagement with appropriate government entities. Railroads leverage a strong mix of private and public capabilities to effectively prevent and respond to malicious cyber activity. As threats evolve, our industry strives to stay agile and innovative to address the dynamic threat landscape.

## A Unified Commitment to Overall Security Preparedness

The rail industry addresses cybersecurity head on through a longstanding industry-wide, risk-based, and intelligence-driven plan. Railroads' highly specialized cybersecurity teams carry

out comprehensive, multi-faceted cybersecurity plans focused on four factors identified by experts as the most likely way to stop cyberattacks: the tactics most commonly used to gain illicit access to computer systems; the vulnerabilities most commonly exploited; illicit activities missed or disregarded in prior analysis but identified after the incident; and protective measures that could have made a difference had they been implemented.

Responsibility for implementing and sustaining cybersecurity plans lies with two specialized industry coordinating bodies. First, the Rail Security Working Committee includes senior law enforcement and security officials focused on countering domestic and international terrorism. Second, the Rail Information Security Committee (RISC) is comprised of chief information security officers and information assurance leaders from major North American railroads. The RISC was established in 1999 and is supported by security experts from the AAR and the American Short Line and Regional Railroad Association (ASLRRA). Together, these committees form the Rail Sector Coordinating Council (RSCC), the rail industry's primary channel for communication and coordination with government agencies on cybersecurity initiatives.

The rail industry's security plan does not just sit on a shelf. It is a living document, continuously evaluated and enhanced through recurring exercises and frequent consultations with government and private-sector security experts to ensure maximum sustained effectiveness supported by a strong working relationship with the federal government.

**Information Sharing is Vital for Success**

For railroads, cyber awareness is a fundamental component of their day-to-day operations, but even the best cybersecurity plans and practices will falter if useful information on cyber threats is not shared. Information sharing allows organizations to learn from one another,

reduce their vulnerabilities, and quickly adapt to changing conditions. Insights gained from risk assessments and threat advisories, along with experience gained in drills, enable railroads and industry organizations to incorporate effective safeguards and protective measures into their own systems.

For this reason, railroads and industry organizations prioritize proactive engagement with government partners, including the Transportation Security Administration (TSA) and the Cybersecurity and Infrastructure Security Agency (CISA), to share information on cyber threats and effective countermeasures. These open lines of communication are maintained through frequent calls and meetings between AAR, its members, and TSA, ensuring our federal government partners are aware of how rail operations interact with cybersecurity measures.

**Noticed of Proposed Rulemaking (NPRM)**

Earlier this month, TSA issued a lengthy NPRM that builds upon existing cybersecurity requirements previously issued through security directives. While the industry was pleased to see TSA issue this rule through the regulatory process and allow for robust public comment, the NPRM would have greatly benefited from earlier discussions with industry about potential requirements in a more informal setting like negotiated rulemaking. The industry is still digesting the very lengthy proposal and will provide robust comments. There are a few long-standing concerns for the railroads that the NPRM does not fully address.

For example, the NPRM would require railroads to report an incident within 24 hours of it occurring. Congress specifically set the timeframe for reporting incidents at 72 hours under the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). Not only does this lack of harmonization create confusion, the 24-hour window is impractical. Within 24 hours, an attack could still be occurring, the information about the incident will be less complete, if not

inaccurate, and railroads would be pulling resources and manpower away from responding to the attack and towards complying with reporting requirements. The railroads would have to then supplement the initial report as their information becomes available or changes.

Similarly, the NPRM also requires that a railroad's security coordinator be a U.S. citizen, which the railroads have flagged with TSA as a major concern for several years. Two large railroads in the U.S. are headquartered in Canada and employ Canadian citizens in high-level cybersecurity roles. Prohibiting these highly skilled senior level employees from representing their companies as security coordinators serves no clear security benefit and makes it extremely difficult for these Canadian railroads to comply.

**Use of TSA Emergency Authority**

AAR was pleased that TSA finally issued this NPRM. For several years, the industry was operating under security directives issued under TSA's emergency authority. We recognize the importance of TSA having the appropriate authority to act quickly in the face of an emergency. However, following the Colonial Pipeline attack in 2021, TSA used its emergency authority to issue security directives aimed at freight railroads and other modes of critical infrastructure mandating specific requirements effective immediately. AAR was unaware of, nor was it made aware of, any prevailing freight rail emergency conditions that would require use of emergency authority, and the security directives circumvented the notice and comment period that allows for industry feedback to improve regulations. The broad mandates TSA issued also treated every mode as if they were starting from scratch with developing a cybersecurity plan when railroads had been properly monitoring their network for decades. The decision by TSA to issue the recent NPRM and move away from security directives and towards the normal rulemaking process is a welcome one that will make these regulations more effective.

**Other Areas for Improvement**

AAR has identified two other areas where our work with TSA and other agencies could be improved. First, the lack of analysis of cyber incidents by the government can leave railroads and other modes unaware of future threats or how to reduce susceptibility to future attacks. Further analysis of an attack or other incidents by the government can inform railroads' decisions about strengthening our network. Second, the government's focus on the cybersecurity risks of transportation companies overlooks the importance of ensuring the security of suppliers to the industry. Suppliers play a critical role in various aspects of railroad operations, and the government should consider how best to directly address their vulnerability to cyber incidents.

**Conclusion**

The railroad industry, TSA, and CISA share a common purpose: ensuring that effective, up-to-date, and sustainable measures are in place to mitigate risk in the face of evolving cyber threats. Railroads have a proven track record of cooperative engagement with federal agencies, and they firmly believe that collaborative effort is the best way to achieve this goal. Railroad operations are resilient thanks to years of proactive and extensive efforts by highly skilled railroad employees to develop, implement, and continuously improve plans, practices, and measures for cybersecurity as threats and security concerns emerge. Cybersecurity is always evolving, and real-time adaptation is essential to reduce risk. Railroads and their employees will continue to work cooperatively with private and public entities to ensure that our nation's rail network and the people, firms, and communities we serve remain safe, efficient, and secure.