Interstate Natural Gas Association of America

Testimony of Maggie O'Connell
Director of Security, Reliability, and Resilience
Interstate Natural Gas Association of America

Before the House of Representatives Oversight and Accountability Subcommittee on Cybersecurity, Technology & Innovation

Hearing on Enhancing Cybersecurity by Eliminating Inconsistent Regulations

July 25, 2024

Chairwoman Mace, Ranking Member Connolly, members of the Subcommittee, I am Maggie O'Connell, the Director of Security, Reliability, and Resilience with the Interstate Natural Gas Association of America (INGAA). I currently lead all aspects of INGAA's cybersecurity, physical security, and emergency response policy. I represent INGAA and our members on the Oil and Natural Gas Subsector Coordinating Council (ONG SCC) and, in my prior role, I served on the Executive Committee for the Chemical Sector Coordinating Council (CSCC). I also led the coalition of ONG subsector association commentators on the Office of the National Cyber Director's (ONCD) Request for Information (RFI) on *Opportunities For and Obstacles To Harmonizing Cybersecurity Regulations*[1]. Thank you for inviting me to address you today and share the perspectives of both natural gas pipeline operators and the broader oil and natural gas (ONG) subsector on cybersecurity regulatory harmonization.

INGAA is the trade association that advocates to federal U.S. policymakers the regulatory and legislative priorities of the domestic interstate natural gas pipeline industry. INGAA's 27 members represent the majority of interstate natural gas transmission pipeline companies in the U.S. and are leaders in the reliable transportation of gas throughout the country. Some of our members also operate other energy facilities and services including liquified natural gas (LNG) import and export facilities, utilities, dams, nuclear facilities, hazardous liquid pipelines, terminals, gas production and storage facilities, and refineries. Through the diversity of their assets, INGAA members operate a significant portion of the U.S. oil and natural gas value chain and are, as a result, some of the most regulated entities in the nation.

The ONG subsector understands the importance of regulations to ensure the safe, secure, and reliable provision of goods and services. Our primary purpose is to keep energy moving. Which is precisely why our operators apply a risk-based "defense-in-depth" approach to cybersecurity, just as they do with other enterprise-wide risks including safety hazards, changes in laws and regulations, geopolitical forces, changes in market demand or competition, or other systemic financial risks. Defense-in-depth is a comprehensive strategy that aims to protect the entire enterprise, rather than each individual business unit, from various threats. The strategy includes physical and network security, administrative, antivirus, and behavioral controls. It entails robust governance, systematic risk-based management, and multi-dimensional programs based on industry-recognized standards and frameworks. Most importantly, these defense-in-depth approaches are based on the organization's risk tolerance and acceptance.

[1] 88 FR 55694 (August 16, 2023).

To that end, security regulations should not be promulgated simply for the sake of doing so. They must be based on risk, focused on outcomes, and informed by threats, with the goal of safeguarding those elements that enable the secure provision of energy services, protection of personal data, and of the essential functions that support the country's economy and national security. It is equally critical that any new requirements are developed in consultation with the impacted community and harmonized with existing regulations to ensure that there are no unintended consequences or impacts to reliability and safe operations. When agencies seek prescriptive measures or fail to closely examine existing or proposed regulations which aim to address similar objectives, it can lead to conflicting regulatory requirements. Conflicting, duplicative, or overly burdensome cybersecurity requirements may force organizations to dedicate key resources to compliance, rather than using those resources to strengthen, mature, and advance their security programs. Conversely, if regulations are risk-based and outcome-focused, then even divergent requirements will converge when the common outcome is achieved.

Within the energy sector, there are a myriad of agencies with oversight or authorities over cybersecurity to include, the Federal Energy Regulatory Commission (FERC), the North American Electric Reliability Corporation (NERC), the United States Coast Guard (USCG), the Cybersecurity and Infrastructure Security Agency (CISA), the Transportation Security Administration (TSA), the Securities and Exchange Commission (SEC), the Nuclear Regulatory Commission (NRC), and state public utility commissions. In practice, managing compliance obligations with disparate regulations and across agencies may in fact harm the cybersecurity posture of organizations, particularly where limited resources are allocated to compliance activities over managing risk, maturing capabilities, and creating effective security programs. Efficient and appropriate regulatory regimes that are harmonized and streamlined to ensure that organizations are able to focus on hardening their defenses are a top priority for the energy sector.

We understand that there is no single formula to achieve regulatory harmonization, and that it is certainly an uphill battle. Harmonization can be best understood as alignment across multiple federal agencies and related regulations to determine a common set of requirements that achieve a desired security outcome. Undoubtedly, the key driver for harmonization is efficiency for compliance and the circumvention of duplicative or conflicting requirements. However, when undertaking this effort, the federal government – which is best positioned to facilitate harmonization – should focus on understanding the risk within each critical infrastructure sector, the number of agencies with existing cybersecurity requirements within each sector, and the varying purposes of each of the cybersecurity regulations, be they for national security, safety, or consumer and investor protection.

The oil and natural gas industry believes there are three main considerations for the federal government when determining how to harmonize cybersecurity regulations.

- First, when considering new regulatory requirements, regulators should engage in robust consultation processes with industry, other regulatory bodies with authorities in that sector, and the regulators of sectors with direct dependencies to the sector for which the cybersecurity regulations are under development (*i.e.* ONG is dependent on chemical, water, electric, financial, and telecommunications, among others).

- Second, if proactive efforts cannot be made to harmonize or rectify the disparate requirements placed upon owners/operators when developing cybersecurity regulatory requirements, agencies would be well served to take action to retroactively ensure that regulatory requirements applicable

to entities regulated by multiple agencies are harmonized in a reciprocating manner. Doing so would reduce the regulatory burden on industry owners and operators and would allow the federal agencies administering these requirements to streamline their efforts.

- Third, Congress and ONCD should consider whether a single entity, such as CISA, could facilitate the harmonizing role to ensure consistent standards and requirements across jurisdictions covering cybersecurity. Different regulators with various requirements create redundancies, which increases the risk for cybersecurity gaps. A single entity to provide management and oversight of the multitude of cybersecurity regulations would enhance overall cybersecurity and ease compliance efforts.

Consultation

It is critical that any new requirements are harmonized with existing regulations to avoid unintended consequences or impacts to reliable, safe operations. For example, in early iterations of the TSA Pipeline Security Directives (SDs), TSA hastily promulgated overly prescriptive mitigation measures including patching cadence, password changes, daily anti-virus scans – which is both impossible with existing technologies and would have resulted in the industry being less secure – as well as other reactive cyber controls without regard to the impact on system operability, product warranties, and patch effectiveness. Proactive controls, such as multifactor authentication, were required without regard to legacy system capabilities, and rip-and-replace alternatives were directed without considering cost or supply constraints.

Following a months-long consultative process with industry and interagency partners, such as the Pipeline and Hazardous Materials Safety Administration (PHMSA) and CISA, TSA reissued Security Directive Pipeline 2021-02 (SD02) with an eye toward outcome-based requirements wherein operators have greater authority to prioritize their "Critical Cyber Systems" based on their organization's risk tolerance. This collaborative approach proved invaluable to the success of TSA's program and was lauded in the Biden Administration's National Cybersecurity Strategy as one that "produce[d] regulatory requirements that are operationally and commercially viable and will ensure the safe and resilient operation of critical infrastructure.[2]"

Federal agencies considering cybersecurity regulations should leverage these lessons learned and proactively discuss how their proposals may impact existing regulations in the safety, security, and operational space. The more the federal government can consistently develop and apply regulations, the more operators will be able to understand and implement those requirements, definitions, and objectives, which will allow them to focus more effectively on addressing cyber threats and mitigations.

In that regard, consultation with regulators of sectors with direct dependencies to the sector for which the cybersecurity regulations are under development will drive better cybersecurity outcomes for the nation. This is where harmonization can be most effective and beneficial to the regulated community. The interdependencies of critical infrastructure, and notably the use of similar operational technology equipment or vendors, can often suggest that an incident impacting one sector may also impact or have downstream impacts to another. In fact, recent telecommunications outages have proven to be a real-time exercise for ONG operators throughout the country when a lack of communications or visibility into their operations

[2] *See* https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf at pg. 7.

tests the resiliency of their back-up systems. Consequently, where cybersecurity regulations exist among these interdependent systems, harmonized sets of requirements can draw down risk across multiple sectors.

Reciprocity

Reciprocity is particularly pertinent given the increasing number of mutually exclusive and inconsistent federal regulations impacting the oil and natural gas sector emanating from a single federal department. The Department of Homeland Security contains three agencies (CISA, TSA, and USCG) with cybersecurity regulatory authority over the ONG sector. While not necessarily conflicting, especially at the federal level, these regulations are certainly duplicative, burdensome from a compliance perspective, and are inconsistently enforced.

In addition to an overall misuse of government and industry resources, when distinct agencies have purview over the same information technology (IT) and operational technology (OT) systems, the potential of operational complications and associated cost overruns is compounded as multiple reporting regimes require and audit against different mitigations that cover the same outcome (*e.g.* different patching timelines in the OT environment). In that regard, if an operator is already implementing a preexisting regulatory framework, satisfaction with those requirements should be deemed sufficient to meet the requirements of another regulatory program if the same, or substantially similar, risk reduction outcomes are achieved. This approach would ensure that any new requirements would neither compete nor conflict with existing requirements, while supporting a constructive and efficient regulatory oversight program.

For example, TSA has issued two Pipeline SDs, currently on versions Security Directive Pipeline 2021-01D[3] (SD01D) and SD02D[4], as the agency works towards releasing a Notice of Proposed Rulemaking (NPRM)[5], related to pipeline and liquified natural gas (LNG) facilities' cybersecurity processes.SD01D requires covered pipeline and LNG facilities to report cybersecurity incidents to CISA; designate at least two cybersecurity coordinators available to TSA and CISA at all times for the purpose of coordinating with the agencies in the event of a cybersecurity incident; and review their current activities against TSA pipeline cybersecurity recommendations to assess cyber risks, identify gaps, develop remediation measures, and report those results to TSA and CISA.

SD02D requires covered pipeline and LNG facilities to establish and implement a TSA-approved Cybersecurity Implementation Plan (CIP) outlining specific cybersecurity measures, along with a schedule for meeting outcomes designated by TSA; develop and keep current a Cybersecurity Incident Response Plan (CIRP) aligned with TSA requirements; develop and submit for TSA-approval a Cybersecurity Assessment Plan detailing how the effectiveness of their cybersecurity measures will be assessed and how vulnerabilities will be identified and resolved; and submit an annual report describing their Cybersecurity Assessment Plan (CAP) results from the prior year.

Additionally, CISA's Chemical Facility Anti-Terrorism Standards (CFATS)[6] program requires any facility that manufactures, uses, stores, or distributes chemicals of interest (COIs) at or above a screen threshold quantity to report those holdings to CISA within 60-days of coming into possession of those chemicals.

[3] *See* https://www.tsa.gov/sites/default/files/sd-pipeline-2021-01d.pdf (May 29, 2024).
[4] *See* https://www.tsa.gov/sites/default/files/tsa-sd-pipeline-2021-02d-w-memo_07_27_2023.pdf (July 26, 2023).
[5] At the time of this written testimony, TSA's NPRM for Enhancing Surface Cyber Risk Management had not yet been published in the Federal Register; however, the 2024 Spring Unified Regulatory Agenda noted a target date of July 2024.
[6] *See* https://www.cisa.gov/resources-tools/programs/chemical-facility-anti-terrorism-standards-cfats.

High-risk, tiered facilities are also required to submit a Security Vulnerability Assessment and a Site Security Plan, or an Alternative Security Program, that meets 18 defined RBPS[7] intended to address security issues, including cybersecurity[8]. Prior to Congress' failure to reauthorize CFATS, a widely supported and internationally recognized chemical security program, CISA was developing an NPRM expected to include additional cybersecurity requirements for covered facilities.

Notwithstanding the potential inclusion of additional cybersecurity requirements, INGAA would be remiss if we did not underscore our call for Congress to swiftly reauthorize CFATS, so that the operators of these high-risk chemical facilities have the continuity required for their multi-year security programming. Every day, week, and month that passes without CFATS authority in the current domestic and geopolitical environments is a threat to national security.

Lastly, ONG facilities regulated by the USCG under the Maritime Transportation Security Act (MTSA)[9] are similarly required to assess, document, and remediate computer system or network vulnerabilities in their Facility Security Assessments (FSAs) submitted to the USCG, and document how those vulnerabilities have been addressed in the required Facility Security Plans (FSPs). USCG issued an NPRM in February 2024 on *Cybersecurity in the Maritime Transportation System*[10]. As currently written, USCG would require certain prescriptive mitigation measures that are arbitrary, developed without consulting the impacted communities, could impact operational reliability, and are scoped uniformly to include barges, offshore drilling, refineries, LNG facilities, and other marine transportation system (MTS) entities, each with their own unique operational environments.

In our joint comment letter[11] with the American Petroleum Institute (API), the American Gas Association (AGA), the National Ocean Industries Association (NOIA), and the Offshore Operators Committee (OCC), the trades urge USCG to leverage lessons learned from the challenges TSA experienced following the issuance of first iteration of SD02. The consultative process that TSA undertook yielded an outcome-based, risk and threat-informed regulatory program that improves cybersecurity for the pipeline community, which should be used as a model for other segments of the ONG subsector.

Nevertheless, these three agencies have made little effort to harmonize these efforts, leading to increased administrative burdens for coordinating with, and meeting the requirements of, these respective agencies. In INGAA's supplemental comment letter[12] on USCG's proposed requirements, filed jointly with AGA, our organizations recommend, in the spirit of cybersecurity regulatory harmonization and reciprocity, that facilities already covered by TSA's requirements not be required to comply with this proposed rule. At a minimum, the TSA-approved CIP submitted as part of SD02D should be considered sufficient for compliance with USCG's proposed requirements.

---

[7] *See* https://www.cisa.gov/resources-tools/programs/chemical-facility-anti-terrorism-standards-cfats/cfats-risk-based-performance-standards.
[8] *See* https://www.cisa.gov/resources-tools/programs/chemical-facility-anti-terrorism-standards-cfats/cfats-risk-based-performance-standards-rbps/rbps-8-cyber.
[9] 46 U.S.C. Chapter 701 (2002).
[10] 89 FR 13404 (February 22, 2024).
[11] *See* USCG-2022-0802-0079.
[12] *See* USCG-2022-0802-0073.

Single Oversight Agency

Nonetheless, a significant challenge for regulatory harmonization and reciprocity are the silos in which agencies exist. Each agency sees its mission as unique and independent from others, despite the common goal of strong cybersecurity for critical infrastructure systems. To that end, a single agency, such as CISA, could serve as an arbiter and facilitator for cybersecurity regulatory harmonization.

As the nation's cyber defense and risk management agency, CISA is well positioned to lead this effort. Furthermore, in their new capacity as National Coordinator under the National Security Memorandum on Critical Infrastructure Security and Resilience (NSM-22),[13] CISA's visibility into and responsibility for coordinating cross-sector risk can help ensure that regulations are informed by the unique threats to each sector, the cyber maturity levels of each sector, are outcome-based, and align with existing and proposed regulations across dependent sectors. The agency has already undertaken significant work in fostering a collaborative interagency process among the pipeline community through the Joint Cyber Defense Collaborative's (JCDC) Pipeline Campaign Plan and can build upon these efforts to break down these agency silos to enable synchronized, harmonized cybersecurity regulatory planning and implementation across all critical infrastructure sectors.

Congressional Action

ONCD's Summary of the 2023 Cybersecurity Regulatory Harmonization Request for Information reaffirms many of the challenges laid forth and underscores that these concerns are not unique to the energy sector. INGAA is pleased that in light of ONCD's 2023 RFI responses, the White House has begun to explore a pilot reciprocity framework to be used in "a critical infrastructure subsector."[14] Reciprocity, as discussed above, is an extremely helpful tool alongside harmonization, and should be considered where harmonization cannot be achieved or where regulations exist from different agencies under the same Department, such as is the case with DHS within the energy sector. However, as Nick Leiserson, Assistant National Cyber Director for Cyber Policy and Programs commented in his written testimony before the Senate Committee on Homeland and Government Affairs on June 5, 2024[15], ONCD's work toward harmonization and reciprocity cannot be fully achieved without congressional action.

Last week, Senate Homeland Security and Government Affairs Committee Chairman Gary Peters introduced a bill[16] to establish a committee to harmonize cybersecurity regulatory regimes. This effort aims to tackle the cross-sector interdependency challenges by bringing together all federal agencies, including independent agencies, with authority to issue cybersecurity requirements to develop a regulatory framework for harmonization. Despite the irony of crafting regulation to harmonize regulation, INGAA is largely supportive of this concept. However, we cannot underscore enough the importance of consulting with the regulated community in any undertaking involving regulation. As drafted, Senator Peters' bill does not invite the participation of representatives of the critical infrastructure sectors in the harmonization committee. The critical infrastructure operators are the ones who are most capable of speaking to their sector-specific risks, systems, risk tolerance, existing regulations, and the challenges associated with

[13] *See* https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/ (April 30, 2024).
[14] *See* https://www.whitehouse.gov/wp-content/uploads/2024/06/Cybersecurity-Regulatory-Harmonization-RFI-Summary-ONCD.pdf (June 2024) at pg. 4.
[15] https://www.hsgac.senate.gov/library/files/testimony-leiserson-2024-06-05/testimony-leiserson-2024-06-05/.
[16] https://www.congress.gov/bill/118th-congress/senate-bill/4630/text?s=1&r=28.

compliance with multiple cybersecurity requirements across the federal government so that a harmonization framework is operationally appropriate and actually reduces compliance burdens.

Regardless of the framework the government moves to establish for cybersecurity regulatory harmonization and reciprocity, the security of the information provided to federal agencies must be protected. The government's collection and aggregation of sensitive security and operational information from operators to meet security requirements prevents critical infrastructure operators from achieving their security goals. The recent DHS CISA cyber incident in which the Chemical Security Assessment Tool (CSAT) was compromised, potentially exposing highly sensitive data and site security information for CFATS facilities, reaffirms that effective oversight and enhanced security on our own federal systems is essential for the confidence of critical infrastructure operators and the protection of national security.

Conclusion

Operators take an enterprise-wide, risk-based approach to security. They do not separate security across their business units; rather they prioritize resources based on risk and assume that an incident impacting one area of a business could easily occur in another. Prescriptive regulatory requirements can restrain a company's ability to respond to changing threats in a nimble and responsive way. Operators must be able to ensure that needed resources can be deployed when it is determined that risks need to be addressed without the need to submit changes to their cybersecurity plans across multiple agencies. Regulation may require operators to apply certain risk mitigation controls to their critical cyber systems, but operators often apply those same controls across the enterprise.

Harmonization can be most useful when promulgating new regulations across agencies or interdependent sectors, where regulators can align on a common taxonomy or set of requirements. Reciprocity is best served where regulations that exist or are under development across the same sector seek to achieve the same outcome. As additional agencies seek to expand their oversight and authorities to include cybersecurity, harmonization and reciprocity will be essential to ensure that operators can continue to mature their security programs without overly burdensome compliance obligations. It is imperative that the federal government and operators work cooperatively toward our overall defense rather than compliance. If regulation is our pathway to defense, we will absolutely fall short.