Statement for the Hearing Record
Subcommittee on Cybersecurity, Information Technology, and Government Regulations
Committee on Oversight and Accountability
U.S House Representatives

Enhancing Cybersecurity by Eliminating Inconsistent Regulations

July 25, 2024

The American Gas Association (AGA) is well-positioned to provide feedback on harmonization of cybersecurity regulatory requirements for natural gas utilities. A harmonized, outcome-focused, and risk-based approach to cybersecurity regulations should be the foundation for future regulations, and reciprocity should be the goal for existing regulations.

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 77 million residential, commercial, and industrial natural gas customers in the U.S., of which 96 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.

Natural gas utilities interact with a wide range of federal and state government entities with cybersecurity oversight responsibilities for the same informational technology (IT) and operational technology (OT) systems. While natural gas utilities have adapted to multiple regulatory regimes, there are potential operational complications when these regimes require, and audit against, different mitigation strategies that cover the same outcome (*e.g.,* different patching timelines in the OT environment). When cybersecurity requirements conflict, are duplicative, or are overly burdensome, owners/operators are often led to dedicate key resources to compliance activities rather than to strengthening, maturing, and advancing their cybersecurity programs.

The majority of cyber regulatory requirements with implications to natural gas utilities are administered by federal agencies under the purview of the Department of Homeland Security. However, little effort has been made across DHS to harmonize disparate requirements. In our experience, while federal government entities ostensibly welcome the concept of harmonization, they do not currently demonstrate a willingness to concede their own individual approaches to implement an overall harmonized cybersecurity regulatory approach.

To the extent a natural gas operator is already implementing a preexisting cybersecurity regulatory framework, such measures should be considered satisfactory for similar requirements in another regulatory program if the same mandated risk reduction outcomes are achieved. In so doing, new requirements would neither compete nor conflict with existing requirements, while constructively introducing regulatory oversight as appropriate.

Conflicting requirements occur when regulatory bodies seek to implement prescriptive cybersecurity measures. In contrast, if cybersecurity requirements are risk-based and outcome-focused, then even divergent requirements will converge when a common outcome is achieved. Effective cyber risk management cannot be implemented in a vacuum; it *must* be part of an overall risk management program. Boards of Directors and senior executives establish an organization's acceptable level of risk mitigation to address all hazards, including cybersecurity threats. Cybersecurity regulations must address prohibitive costs and support outcome-focused, flexible requirements. Organizations must be allowed to apply risk-informed controls to achieve certain cybersecurity requirements and manage risks in a way that is efficient and effective for their unique individual systems.

Industry's federal cybersecurity oversight and regulatory partners are urged to reframe how they view cybersecurity criticality. To remain effective, they need to move away from the silos of IT and OT functionality – as is commonly distinguished now in the cybersecurity regulatory environment – and instead evaluate industry cyber capability based on whether there is impact to the safe and reliable delivery of a commodity or service. Furthermore, Congress should consider authorizing a single federal entity to play the harmonizing role of ensuring consistent standards and requirements across various agency jurisdictions that cover cybersecurity for every critical infrastructure sector. This authority should cover existing standards and inform any new cybersecurity regulatory process.

Finally, when developing new cybersecurity regulatory requirements, regulators should be required to consult with other regulatory bodies with authorities in a particular critical infrastructure sector, regulators of other sectors with direct ties to the sector for which new cybersecurity regulations are under development, and owners/operators subject to the requirements being drafted. It is critical that agencies take action to ensure harmonization and reciprocity among existing regulatory requirements, and any new cybersecurity requirements are harmonized with all other relevant existing regulations to ensure there are no unintended consequences or impacts to reliable and safe industry operations. Engaging in this process will reduce the cybersecurity regulatory burden on industry owners/operators and streamline, clarify, and improve the federal government's overall cybersecurity authorities and capabilities.

The American Gas Association appreciates the opportunity to share this statement for the hearing record and we look forward to working with the Subcommittee on Cybersecurity, Information Technology, and Government Regulations as it further studies the details of cybersecurity regulatory harmonization.