Kimberly Denbow
Managing Director, Security & Operations
American Gas Association

Testimony before the House Homeland Security Committee Subcommittee on Cybersecurity, Infrastructure Protection, & Innovation

"Cyber Incident Reporting for Critical Infrastructure Act of 2021"

September 1, 2021

Chairwoman Clarke, Ranking Member Garbarino, and Members of the Subcommittee, I am Kimberly Denbow, Managing Director of Security & Operations, of the American Gas Association (AGA). I have led AGA's security policy and technical program for nearly two decades. Also relevant to this hearing, I am a former voting member of the Transportation Security Administration (TSA) Surface Transportation Security Advisory Committee for which I helped stand up and co-chaired the Cybersecurity Subcommittee. I also helped stand up and presently co-chair the Cybersecurity Working Group for both the Oil & Natural Gas Sector Coordinating Council and the Pipeline Sector Coordinating Council. Thank you for inviting me to share my perspectives on the *Cyber Incident Reporting for Critical Infrastructure Act of 2021* and AGA's general approach to cybersecurity.

Founded in 1918, AGA represents more than 200 local energy companies that deliver clean and affordable natural gas throughout the United States. There are more than 76 million residential, commercial, and industrial natural gas customers in the U.S., of which 95 percent — more than 72 million customers — receive their gas from AGA member utilities. Natural gas is a necessary fuel for a clean and secure energy future, providing benefits for the economy, our environment, and our energy security. Alongside the economic and environmental benefits and opportunities natural gas offers our country comes the great responsibility to protect our distribution pipeline system network from cyber compromise.

Technological advances over the last 30 years have made natural gas utilities more cost-effective, safer, and better able to serve our customers via web-based programs and tools. Unfortunately, the opportunity cost of a more connected and more efficient industry is that we have grown to be an attractive target for increasingly sophisticated cyber criminals and terrorists. The cyber threat landscape is evolving at an alarming rate comparable to biological virus mutations. This said, America's investor-owned natural gas utilities are meeting the threat daily via skilled personnel, robust cybersecurity system protections, an industry commitment to security, and a successful ongoing cybersecurity partnership with the Federal government.

Safety and security are core values for America's natural gas utilities. AGA and its member companies are committed to investing in leading security technologies, utilizing best practices and training, and promoting an industrywide vigilant security culture to help fortify our security defenses.

Cyber Incident Reporting for Critical Infrastructure Act of 2021

Effective cybersecurity incident reporting is essential to dampening widespread cybersecurity compromise. AGA supports the *Cyber Incident Reporting for Critical Infrastructure Act of 2021*, which establishes the criteria AGA members argue is necessary for a workable incident reporting framework. A few provisions of particular interest and which have industry's support include report timing, supplemental reporting clarity, recognition of existing reporting requirements, Information Sharing & Analysis Centers (ISACs), and liability protections. Additional details are outlined below:

- Incident Report Timing. Providing covered entities 72 hours after confirmation to report on cybersecurity incidents appropriately recognizes that owners/operators need a reasonable amount of time to not just identify but also to verify the validity of a cybersecurity incident before reporting. This minimizes the reporting of non-credible incidents, which can be excessive and resource-intensive with negligible value-add.

- Supplemental Reporting. The latest draft of this legislation helpfully clarifies what qualifies as supplemental reporting and offers the Department of Homeland Security (DHS) Cybersecurity & Infrastructure Security Agency (CISA) Director (and covered entities) the useful option of a flexible reporting timeline so as not to specifically "prioritize incident response efforts over compliance." This synchronizes the efforts of CISA with the operator, ensures incident investigation is prioritized, and eliminates unnecessary supplemental information submission.

- Information Sharing and Analysis Organizations. We appreciate the latest draft bill's increased reliance on industry Information Sharing & Analysis Centers (ISACs) for government-private sector outreach as well as incident reporting. Permitting owners/operators to leverage existing mechanisms through third-parties, such as AGA's Downstream Natural Gas ISAC, strengthens the function of these entities to the benefit of all stakeholders, since such organizations have sector-specific threat analysts who can provide additional perspectives to CISA.

- Harmonizing Reporting Requirements. AGA's member natural gas utilities are among the most regulated in the country at the state, federal, and local level. Complicating matters, well over 50% of AGA members are combination natural gas-electric utilities with separate electric sector requirements. As such, we appreciate efforts to reduce potential conflicting mandates by harmonizing the cyber incident reporting requirements with preexisting cyber reporting requirements.

- Industry Legal Protections. We appreciate the inclusion of reasonable information disclosure rules, liability protections for reporting entities (familiar to industry as they mirror those in the Cybersecurity Act of 2015), and regulatory protections in the legislation. Without these provisions, it would be hard to imagine the sort of streamlined and trusted public-private incident reporting partnership this legislation contemplates.

While the draft legislation sets a strong foundation for moving forward, there are a few policy areas where we recommend some expansion and/or clarification. Not surprisingly, most of our suggestions surround additional private sector involvement in the overall process, per below:

- Rulemaking Detail [SEC .2220A(d)(1) In General]. This section outlines the incident reporting rulemaking process. While we appreciate that "appropriate stakeholders" will be able to comment on the interim final rule, we strongly recommend greater specific outreach to critical infrastructure organizations (Sector Coordinating Councils, ISACs, individual covered entities, industry organizations, etc.) in developing the rule. Private sector engagement from the beginning will ensure the rule will be reasonable, credible, and based on vital critical infrastructure experience and operational capabilities.

- Who are the Covered Entities? [SEC .2220A(d)(2) Covered Entities]. The list of covered entities should be flexible and updated regularly (or as necessary) as companies change operations. DHS should be able to accommodate such changes. To help determine covered entities, we recommend: (1) consulting with the private sector, (2) utilizing preexisting government lists that identify critical facilities, (3) a periodic review and update of covered entities, and (4) a process that allows critical infrastructure entities to appeal their inclusion on the list.

- Ensuring CISA has the Tools it Needs. [SEC .2220A(d)(6) Responsibilities of Covered Entities]. This subsection focuses on industry's coordination with CISA personnel. This coordination will only be effective and efficient if CISA has the staffing and sector-specific cybersecurity expertise necessary to communicate with private companies in vastly different business sectors. As such, we recommend adding language to ensure that *"CISA will coordinate with SRMAs" (or similar).*

- Director Authority. [SEC .2220A(e)(1) Authorized Activities]. This subsection lists the exceptions under which the Director may disclose information provided to the Office. The discretion allotted the Director in the first two exceptions (A and B) are overly broad, which could lead to literally ANY "cybersecurity purpose" as a reason to disclose sensitive company information. AGA recommends adding clarifying language to each exception (A) and (B) specifying "*to circumvent national security or national economic harm.*"

Cybersecurity incident reporting, framed properly, can be the difference between pivoting against our adversaries in an effective manner and minimizing impact, or fumbling to our adversaries' advantage. *Cyber Incident Reporting for Critical Infrastructure Act of 2021* provides the structure while also delivering agility. With slight alterations, it can be even stronger.

Natural Gas Utility Cybersecurity Management: An Endless Evolution

America's natural gas delivery system is the safest, most reliable energy delivery system in the world. This said, industry operators recognize there are inherent cyber vulnerabilities with employing web-based applications for industrial control and business operating systems. Gas utilities employ multiple mechanisms to support a robust cybersecurity program, including participating in an array of government and industry cybersecurity initiatives. The most important resource is the existing cybersecurity partnership between the federal government and industry operators. This partnership fosters the exchange of vital cybersecurity information which helps stakeholders adapt quickly to dynamic cybersecurity risks. That partnership should continue to be supported by Congress.

The Immeasurable Value of Authentic Partnership

For nearly two decades, AGA favored effective partnership above cybersecurity regulations, which we felt served as a ceiling that stifled robust cybersecurity management. We valued the structured oversight model conceived by TSA, our federal regulator for pipeline security. Though the model was unconventional by federal government standards, it achieved something the traditional 'stick-and-carrot' approach could not – constructive information exchange and at a level of confidence and cooperation not typically available to regulators. The TSA "Pipeline Security Guidelines"[1] (Guidelines) coupled with the trust fostered between industry and government advanced pipeline security by orders of magnitude over the years. Whereas regulations serve as a ceiling to which operators rise but are not incentivized to exceed, Guidelines serve as the floor upon which an operator's program may be built and continuously improved based on the operator's system-specific risks and applicable counter measures.

A Shared Common Goal

Some have suggested cyber compromise in the pipeline industry is a direct consequence of the structured oversight model. TSA has been criticized for not doing more prior to the recent issuance of the pipeline security directives. For the record, TSA Surface Transportation did more with less and on a shoestring budget. The TSA Pipeline Group has been the epitome of innovation – leveraging the infrastructure subject matter expertise of pipeline operators, partnering with CISA and Idaho National Labs for in-house industrial control system cybersecurity knowledge, and collaborating with the Department of Transportation's Pipeline and Hazardous Materials Safety Administration (PHMSA) on cybersecurity reviews of control centers. AGA helped champion the CISA/TSA Pipeline Cybersecurity Initiative[2] and promoted effortlessly the Pipeline Validated Architectural Design Reviews[3]. The quality output has been the result of the dedication of TSA and CISA staff, in partnership with pipeline operators, towards a shared common goal – pipeline security.

[1] https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf
[2] https://www.cisa.gov/pipeline-cybersecurity-initiative
[3] https://us-cert.cisa.gov/resources/ncats#Validated%20Architecture%20Design%20Review%20(VADR)

Driving Change

Over the past few years, more than 70 organizations, including TSA, CISA, PHMSA, the Department of Energy (DOE), Federal Energy Regulatory Commission, National Institute of Standards & Technology (NIST), trade associations, and numerous pipeline operators, worked on revising a standard managed by the American Petroleum Institute (API) for control system cybersecurity. The revision was designed to align with existing cybersecurity Guidelines, the NIST Cyber Security Framework[4], and prominent industry cyber standards. This recently updated consensus-based standard, API 1164 version 3, "Pipeline Control Systems Cybersecurity"[5] (API 1164 version 3), helps the operator manage cyber-risks associated with control system cybersecurity environments by providing requirements and guidance for proper isolation of control system environments from non-control system environments. It also addresses enhanced protections at critical connection points along the supply chain.

Walking the Talk

The AGA Board of Directors continues to be forward leaning on multiple fronts – with security at the forefront. Actions and activities include:

- Creation of the Downstream Natural Gas ISAC, which facilitates the sharing of threat information within the natural gas industry and across sectors by providing analysis, coordination, and summarization of threat indicators and other relevant information to its members – a community of nearly 100% of our nation's natural gas utilities and transmission companies;

- Membership-wide adoption of the *AGA Commitment to Cyber and Physical Security*[6] to demonstrate dedication to ensuring the natural gas pipeline infrastructure remains resilient to the growing and dynamic cyber and physical security threats; and

- Development of a three-point Cybersecurity Action Plan which encompasses enhancing cyber standards for gas utility operations, collaborating with CISA for the enhancement of a cybersecurity verification tool, and developing an operator accountability mechanism. The roadmap includes the progression from guidelines to regulations.

Recently, the AGA Board passed a resolution in support of reasonable cybersecurity regulations. Such regulations would be characterized by four critical components:

1. a risk-based methodology,
2. a framework organized by the functions Identify, Protect, Detect, Respond, and Recover,
3. operator flexibility to pivot to a constantly evolving cyber threat landscape, and
4. alignment with natural gas industry cybersecurity guidelines and standards for operational technology.

These four critical components are satisfied by API 1164 version 3.

[4] https://www.nist.gov/cyberframework
[5] API Standard 1164, 3rd edition
[6] https://www.aga.org/sites/default/files/sites/default/files/media/commitment_to_cyber_and_physical_security_sep2016.pdf

An Effective & Timely Transition

As TSA, in collaboration with CISA, transitions from issuing pipeline security directives to issuing cybersecurity regulations, the federal government is encouraged to leverage API 1164 version 3 which reflects practical, attainable, sustainable, and measurable state-of-the-art cybersecurity protections tailored specifically to pipeline operations. Given the imminent threat that prompted issuance of the pipeline security directives, incorporating this standard by reference will be the federal government's most efficient way to put effective pipeline cyber regulations in place.

A Commitment to America – A Commitment to the Communities We Serve

America's natural gas utilities are cognizant of enduring cyber threats and the continued need for vigilance through cybersecurity protection, detection, and mitigation mechanisms. There is no single solution for absolute system protection. Through a combination of cybersecurity processes and timely and credible information-sharing amongst the government intelligence community and industry operators, America's natural gas delivery system remains protected, safe, and reliable, and will remain so well into the future.