Kimberly Denbow
Vice President, Security & Operations
American Gas Association

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

"Sector Down: Ensuring Critical Infrastructure Resilience"

June 27, 2024

Chairman Garbarino, Ranking Member Swalwell, and Members of the Subcommittee, I am Kimberly Denbow, Vice President of Security & Operations, at the American Gas Association (AGA). I have led AGA's security policy and technical program for nearly three decades. Also relevant to this hearing, 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 authored comments on behalf of AGA in response to the Federal Insurance Office's "Potential Federal Insurance Response to Catastrophic Cyber Incidents[1]." Thank you for inviting me to share my perspectives on the natural gas utility experience with cyber insurance, natural gas utility cybersecurity and operational resilience, and opportunities for further and improved security-related coordination with the federal government.

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.

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 cyber actors. This said, America's natural gas utilities are combatting the threat daily via:

- skilled personnel,
- robust cybersecurity system protections,
- an industry commitment to security,

[1] Potential Federal Insurance Response to Catastrophic Cyber Incidents" as published in the Federal Register on September 29, 2022, at 87 FR 59161 *et seq.* 2022-21133.pdf (govinfo.gov)

- 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.

Safety and Security – 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 security culture of vigilance to help fortify our security defenses and enhance all aspects of safety. To that end, the following provides an overview of AGA member natural gas utility experiences with cyber insurance, natural gas utility cybersecurity and operational resilience, and opportunities to build on existing public/private partnerships.

Cyber Insurance and Natural Gas Utilities

- Insurance Coverage Availability & Effectiveness

  In the gas utility sector's experience, the number of insurance providers willing to write cyber insurance policies has been limited. While capacity appears to be improving, the relatively unpredictable scale and cost of a successful cybersecurity compromise of critical operations unsurprisingly has limited the scope of coverage. Actuarial data in the industry continues to be in short supply and may be ineffective as a predictor given the rapid changes in cyber threats. As a result, some existing cyber insurance programs are unnecessarily restrictive in terms of coverage.

  For example, gaps in insurance coverage resulting from cyber incidents leave an owner/operator uncovered when a cyber event results in physical impacts. Such impacts generally do not fall under the cyber policy, and while they may be pieced together under a property policy or through a specialty product designed to bridge this gap, this is a disincentive to an owner/operator obtaining cyber insurance.

  Another common issue is most insurance policies limit or eliminate coverage if the cyberattack is conducted as part of an "act of war" or carried out by nation states or their affiliates. The terms of these exclusions vary widely and are difficult for our owners/ operators to evaluate. Some versions of these exclusions may place the owner/operator in the position of not only having to demonstrate the impact of the cyber incident but also to identify the origin and motive of the adversary – the latter action is beyond the practical scope of natural gas utility cybersecurity programs and sometimes even beyond the capability of our federal partners.

  These issues are indicative of an overall need for simpler, more streamlined cyber policy terms and the applications required to purchase such insurance. It is difficult for many

operators, particularly smaller ones, to understand what is actually covered under cyber insurance policies where important limiting coverage terms are often buried in places like policy definitions.

- Federal Backstop

  AGA members plan for potential disruptions caused by successful cyber incidents on their systems and services and may procure insurance to offset associated potential financial losses. Given that a disruption of energy systems can lead to significant economic impact, AGA members have a vested interest in ensuring that a healthy cyber insurance market exists, including one that can adequately offset so-called "catastrophic" losses.[2] An appropriately structured federal backstop is needed to stabilize the cyber insurance market. It would cap potential losses and allow insurers to assess and quantify risks without the fear of a devastating loss event.[3] Additionally, it could help address persistent cybersecurity shortfalls if the federal backstop is made contingent on the standardization of insurance cyber policy language/definitions and applications. An owner/operator adherence to cybersecurity best practices that are risk-based[4] or regulatorily prescriptive may further help advance security.

  Creating a federal backstop for the cyber insurance market is proactive, practical, and cost-effective way to protect consumers and manage growing cyber risks.

- "Safe Harbor" Statutes

  Federal "safe harbor" statutes encourage companies to take forward-leaning cybersecurity measures to bolster their own cybersecurity as well as the cybersecurity of their peers. Two relevant examples that could be woven into any catastrophic-type cyber insurance program would be the DHS SAFETY Act program as well as the cyber threat information sharing programs established in the Cybersecurity Information Sharing Act of 2015 ("CISA 2015").

  - SAFETY Act

    The program offers companies the ability to minimize or even eliminate specific types of tort liability following cyberattacks when companies can demonstrate they have implemented robust and effective security programs. Linking the obtainment and maintenance of SAFETY Act protections to cyber insurance would be highly

[2] AGA comments to Federal Insurance Office (FIO) "Potential Federal Insurance Response to Catastrophic Cyber Incidents" as published in the Federal Register on September 29, 2022, at 87 FR 59161 *et seq.*
[3] Axio comments to FIO "Potential Federal Insurance Response to Catastrophic Cyber Incidents" as published in the Federal Register on September 29, 2022, at 87 FR 59161 *et seq.*
[4] Policies consistent with risk-based security measures could include encouraging companies to adopt defense-in-depth strategies, least-privilege access security model, and/or controls supporting the NIST Cyber Security Framework key functions of govern, identify, detect, protect, respond, and recover.

useful in promoting effective cybersecurity as well as limiting the economic losses associated with catastrophic cyberattacks.

Linking the SAFETY Act to any catastrophic cyber insurance program could offer companies that have received a SAFETY Act award – and thus have demonstrated that they offer a cybersecurity technology program effective in deterring, defeating, responding to, or mitigating cyberattacks – a specific path to receiving expanded catastrophic cyberattack coverage and/or more favorable premiums.

- CISA 2015

  Congress sought to promote greater sharing of threat information amongst companies and with their partners within DHS. Participation in information sharing programs (e.g., the DNG-ISAC) helps break down barriers to effective threat intelligence analysis. Moreover, active participation in public-private cyber information sharing regimes and/or ISACs should be considered part of any possible requirement for owners/operators to obtain access to any future federal cybersecurity insurance backstop.

Natural Gas Cybersecurity and Operational Resilience

- Cybersecurity

  AGA members have been at the forefront of cybersecurity investment and are continually seeking ways to raise 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 the Transportation Security Administration (TSA) to help strengthen and add value to the pipeline Security Directives (SDs)[5] and reduce risk for the industry. Overall, risk-based cybersecurity aligns with the National Security Memorandum on Critical Infrastructure Security and Resilience[6].

  AGA member natural gas utilities engage in a variety of cybersecurity enhancement programs, including, but not limited to:

  - AGA cybersecurity peer-to-peer program, in which operators evaluate their respective company cyber policies, procedures, and practices.

[5] Security Directive Pipeline 2021-01 (May 28): *Enhancing Pipeline Cybersecurity* (SD1), and Security Directive Pipeline 2021-02 (July 19): *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.

[6] National Security Memorandum on Critical Infrastructure Security and Resilience | The White House

- AGA Biennial Cyber Metrics Survey, which helps benchmark cybersecurity maturity across the natural gas utility community.
- Natural Gas Exercise (NGX), which is a national tabletop exercise of physical security, cybersecurity, and business continuity. NGX-2024 will be a hybrid exercise intended to drill operators' cyber incident response plans and "test" provisions within the Natural Gas Policy Act of 1978, which have been suggested by the Department of Energy to permit the federal government to redirect natural gas from transmission pipelines in times of emergency without regard to contractual agreements.
- Network monitoring technology, which tracks network traffic for unusual cyber activity.
- The DNG-ISAC (stood up by AGA and its members over a decade ago), which provides the natural gas industry[7] with a secure platform for the trusted exchange of physical and cyber threat information and analytics. Given the interdependence between the natural gas and the electric subsectors, there is also a great deal of coordination with the Electric Information Sharing & Analysis Center.
- Energy Sector Cyber Mutual Assistance Program administered by the Edison Electric Institute.

It should be noted that while the threat landscape can appear similar across most critical infrastructure sectors, natural gas utility operations are increasingly needing to address new (and unintentional) cybersecurity risks introduced by federal and state government actions intended to address pipeline safety. For example, because federal pipeline safety policies now mandate the installation of remotely operated valves, natural gas cyber professionals must now plan accordingly to address new cyber vulnerabilities associated with this new electronic equipment. Further, as state regulators evaluate requiring operators to make detailed pipeline operations information publicly available, consideration must be given to the potential increased risk of adversaries leveraging such information to strategically disrupt natural gas systems.

- Operational Resilience

The operational characteristics of the natural gas transportation network in combination with the physical properties of natural gas effectively minimize the likelihood and severity of widespread service disruptions.

- Operators manage the internal pressure of the delivery system by controlling the amount of natural gas that enters and leaves the system; this process of increasing and decreasing pressure happens relatively slowly because of the compressibility

[7] Members of the DNG-ISAC include AGA member natural gas utilities, transmission pipeline members of the Interstate Natural Gas Association of America, and utility and transmission members of the Canadian Gas Association. Additionally, governmental members include Fusion Centers, DHS Intelligence & Analysis, select State threat offices and law enforcement groups.

of natural gas. Industrial control systems are used to help monitor and, in some cases, operate the pipelines and their components that move the gas.

- Critical electronics generally have mechanical fail-safes and can be operated manually, if necessary.
- Natural gas physically moves slowly through a pipeline at an average speed of 15-20 miles per hour, further allowing time for pipeline operators to manage the flow and adjust operations in the unlikely event of a disruption. Outages are rare, and when they occur, they tend to be localized due to the interconnected nature of the transportation network.
- Few pipelines in the U.S. are single-sourced and those that are single-sourced have back-up supply contingency plans, which may include utilizing underground natural gas storage, liquified natural gas, and/or other mechanisms to support system resilience.

Enhanced Public/Private Partnerships: Improving Regulations and Strengthening Engagement

AGA and its member utilities engage actively in public/private partnership opportunities that add measurable value, while also advancing cybersecurity. These opportunities include direct participation with the Department of Homeland Security (DHS), which has several cybersecurity-related initiatives and programs across its portfolio of agencies that regulatorily or voluntarily affect natural gas utilities. DHS entities of particular relevance to natural gas utilities include the:

- TSA,
- Cybersecurity & Infrastructure Security Agency (CISA) – specifically, the Chemical Facility Anti-Terrorism Standards (CFATS) and the Joint Cyber Defense Collaborative (JCDC) Pipelines Cyber Defense Planning Effort, and
- United States Coast Guard.

Each entity/program has helped in varying degrees to move the needle on natural gas utility cybersecurity. For example,

- On the regulatory-front, TSA continues to coordinate with pipeline owners/operators to improve risk-based cybersecurity requirements and achieve predetermined cybersecurity outcomes while promoting flexibility. Despite the challenges associated with the first generation of pipeline Security Directives (SDs) in 2021, the credibility established between TSA and owner/operators prior to the issuance of the SDs helped promote the improvements to subsequent SDs. Particularly noteworthy, TSA's leadership regularly hosts Inspection Forums to garner feedback from owners/operators regarding ways to strengthen the SDs and ensuing cyber regulations.

- On the voluntary-front, the JCDC Pipeline Effort continues to lead an interactive community of government, oil & natural gas pipeline owner-operators, and industrial control system vendors – all driving towards a shared common goal of robust pipeline sector cybersecurity. The inaugural product of this collaboration was a Pipeline Reference Architecture tool and accompanying principles to serve as a voluntary model to guide cybersecurity investment, planning, and operations as pipeline operators work to better segment their networks and mitigate intrusion campaigns.

While cybersecurity regulation harmonization and zero trust reporting appear to be the latest concepts of choice across the federal government, government action (and inaction) can hinder their implementation. The Cyber Incident Reporting for Critical Infrastructure Act's (CIRCIA) Proposed Reporting Requirements and the recent CISA Chemical Security Assessment Tool (CSAT) cybersecurity breach are indicative of the challenges that government must resolve in order to be a reliable industry partner. The challenges are described as follows.

- Harmonization

  While the CIRCIA proposed reporting requirements speak of harmonization between the federal agencies, CISA does not have the authority to require cross-agency harmonization. As a result, the burden is on the owners/operators to determine gaps between agency cybersecurity authorities. For a natural gas utility that operates natural gas, electric, water, coastal facilities, and nuclear, the operator must sort through cyber incident reporting requirements of TSA, the North American Electric Reliability Corporation, the Environmental Protection Agency, the USCG, and the Nuclear Regulatory Commission. It is incumbent on CISA to ensure that its overall cybersecurity reporting requirements account for and harmonize with similar cybersecurity reporting schemes required by sector specific federal agencies as much as possible in order to improve efficiency and reduce costs to the covered entities.

- Zero Trust

  While the federal government is driving itself to a zero trust[8] approach, the government's collection and aggregation of security and operational-related information from critical infrastructure to meet security requirements prevent critical infrastructure owners/operators from achieving zero trust. This is evidenced by the recent DHS CISA cyber incident in which the Chemical Security Assessment Tool (CSAT), which contains industry reporters' detailed security vulnerabilities and plans,[9] had been compromised for multiple days before being recognized by CISA.

[8] Zero Trust Architecture | GSA

[9] 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 necessity for government accountability in the collection, aggregation, and protection of sensitive operations information. The inadequate cybersecurity measures that resulted in the breach underscore the need for the government to have stringent safeguards and robust incident response protocols on the systems the government relies on to store critical infrastructure information. Furthermore, the lack of communication from the responsible agencies exacerbated the situation, leaving operators without crucial information to effectively mitigate the damage. It is not sufficient for agencies to express regret; there must be a concerted effort to prevent recurrence and ensure operators are not left to bear the brunt of the consequences. Effective oversight and enhanced security frameworks on the government's own networks are essential to restore public confidence and protect national security interests.

Ensuring the proper security and handling of sensitive operational information submitted by industry to government partners supports mutually beneficial collaboration. AGA and its member companies value government partnership, while also seeking to limit the vulnerabilities introduced by demonstrated government cybersecurity performance.

In Closing

America's natural gas utilities recognize their attractiveness as a vector and target for nefarious cyber actors. AGA member utilities combat the threat daily by leveraging a cybersecurity management portfolio of wide-ranging tools to include cybersecurity insurance, risk-based cybersecurity measures, participation in the DNG-ISAC, and active engagement in value-add public/private initiatives that advance cybersecurity.

AGA encourages the government to learn from the successes of TSA and JCDC in their genuine collaboration with owners/operators – to earnestly work **with** the owners/operators to seek solutions that are risk-based, outcome-focused, and elevates security above compliance to achieve a commonly shared mission. Additionally, harmonization of government-imposed cybersecurity requirements should not be the burden of owners/operators but rather the responsibility of the government agencies. Lastly, the federal government should hold itself to sensitive information security standards and incident reporting at least as high as required of owners/operators. This is particularly significant given the government's aggregation of our nation's most critical infrastructure operational information.