Natural Gas Utility Cybersecurity Initiatives

The American Gas Association’s (AGA) members are committed to delivering natural gas safely, reliably, cost-effectively and in an environmentally responsible way. Domestic natural gas transportation depends on control systems and business networks to help ensure reliability and safety. AGA and its membership recognize that cyber vulnerabilities are inherent to the application of such systems and that these systems continue to be targets of cyber attacks. As such, AGA member natural gas utilities are involved in cybersecurity initiatives with the understanding that industry cybersecurity effectiveness lies in the diversity of individual company operating systems, and that a one-size-fits-all preventive approach has grave potential to increase system vulnerability.

Natural gas utilities actively engage in cybersecurity risk management, with the primary objectives of minimizing cyber vulnerabilities and increasing a system’s ability to detect malicious cyber traffic and mitigate impact, while implementing security measures that do not disrupt the safe and reliable delivery of natural gas to customers. In general, operators across the industry use the “defense in depth” strategy and a variation of mechanisms to protect their control systems.

AGA actively engages in public-private partnerships with various Federal government entities, including but not limited to the U.S. Department of Homeland Security (DHS); U.S. Department of Energy (DOE); U.S. Department of Transportation; DHS Transportation Security Administration (TSA); DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT); the National Security Agency; White House National Security Staff; Federal Bureau of Investigation; U.S. Secret Service; and others to share information, work through threat scenarios, and develop and implement strategies that help reduce and mitigate the impacts of a cyber attack. AGA member gas utilities also participate in working sessions and classified meetings with the Federal government intelligence community; officials from DHS have met with the AGA board of directors and member companies to review and assess threats. Further, AGA member companies take advantage of the cybersecurity tools available through our partnerships.

The following list provides a sampling of leading cybersecurity initiatives AGA member gas utilities have been or continue to be engaged in within the industry or through the public-private partnership model.

**AGA Chairs Oil & Natural Gas Sector Coordinating Council Cybersecurity Working Group**

The Oil & Natural Gas Sector Coordinating Council (ONG SCC) is an operators’ forum supported by DOE, in coordination with DHS, to promote effective security strategies and activities, policy and communication across the oil and natural gas (ONG) sector to achieve the nation’s homeland security mission. The ONG SCC set up the Cybersecurity Working Group (CSWG) to serve as the subject matter expert body. AGA chairs this working group, which is a joint effort of the Pipeline and Chemical sectors as well due to overlapping cybersecurity interests. The CSWG efforts are designed to increase cybersecurity education and awareness for the sector; to promote engagement between operators and the Federal Government regarding the development of regulations, guidelines and programs that may impact sector cybersecurity activities; and to align physical and cyber infrastructure initiatives.
AGA Leads Collaboration with DOE Cybersecurity Capability Assessment Model
As the chair of the CSWG, AGA is facilitating the participation of ONG operators in the DOE-led development of the cybersecurity assessment tool, the Oil and Natural Gas Cybersecurity Capability Maturity Model (ONG C2M2). This highly-regarded model originated with the electric sector. C2M2 allows operators to assess their cybersecurity capabilities and prioritize their actions and investments.

Coordination of Federal Government Risk Assessment Programs
AGA proactively coordinated meetings of the DOE, TSA, and DHS intelligence community in an effort to encourage all government entities to align their various cybersecurity risk assessment programs, compare/contrast the programs, and identify where synergies could be made. As a result of the meetings, DOE is developing a single page chart that may be referenced by the owner/operator to determine which program would best suit their cyber risk assessment needs.

Recommendation to Develop Downstream Natural Gas Information Sharing & Analysis Center
AGA is leading an effort to establish the Downstream Natural Gas ISAC (DNG ISAC) for the timely reporting, sharing, and analysis of cyber and physical incident information related to natural gas utilities. The DNG ISAC would be tied into the National Council of ISACs and have a bidirectional information sharing conduit with the electric sector ISAC to share threat intelligence, incident information and tools.

TSA Cybersecurity Assessment and Risk Management Approach
AGA co-chaired an initiative facilitated by the TSA to develop a cooperative, national-level approach to cyber risk management, known as Cybersecurity Assessment and Risk Management Approach (CARMA) for the ONG pipeline sector. The purpose of the project was to help industry develop an organization-independent, prioritized list of risks to pipeline sector business functions from cyber attacks and a prioritized list of activities the pipelines would consider undertaking or have already put in place to address such risks. This initiative played a significant role in the technical sessions with the DHS Integrated Task Force (ITF) in the identification of cyber-dependent critical infrastructure.

Cybersecurity Executive Order - Cyber-Dependent Critical infrastructure & NIST Cybersecurity Framework
Through its role as the CSWG chair, AGA coordinated technical sessions between the DHS ITF and the ONG representatives for the identification of cyber-dependent critical infrastructure. DHS concluded that despite the ONG sector having cyber-dependent critical infrastructure, a cyber-compromise could not result in consequences that would meet the criteria of requirements set forth in the Executive Order Section 9, i.e., catastrophic regional or national effects. AGA looks forward to continuing the evaluation with the ITF in this annual review.

Regarding the NIST Cybersecurity Framework, AGA staff and members have been integrally engaged in the development process to ensure the product is one that can be feasibly applied to natural gas systems without impacting reliability and safety.

Presidential Policy Directive 21 - Revisions to the National Infrastructure Protection Plan
AGA is a leading proponent of the public-private partnership model. The National Infrastructure Protection Plan (NIPP) provides the framework for this model, and AGA is engaged in the rewrite to ensure the public-private partnership model is strengthened and continues to foster collaboration.

AGA Member Company All-Hazards Threat Analysis
AGA conducted an all-hazards threat survey of member company executives and cybersecurity subject matter experts. AGA has identified those threats and risks which have a cyber-component and require further attention, and is evaluating opportunities to help gas utilities bolster their cyber defenses through increased awareness and/or training.