EEI Edison Electric Institute
Power by Association℠

AGA
American Gas Association

October 10, 2014

Ms. Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

RE: Experience with the Framework for Improving Critical Infrastructure Cybersecurity

Dear Ms. Honeycutt:

On behalf of our members, the American Gas Association ("AGA"), and the Edison Electric Institute ("EEI") are pleased to submit this response to the Request for Information: "Experience with the Framework for Improving Critical Infrastructure Cybersecurity," which the National Institute of Standards and Technology ("NIST") published in the Federal Register on Tuesday, August 26, 2014.

AGA, founded in 1918, represents more than 200 local energy companies that deliver clean natural gas throughout the United States. There are more than 71 million residential, commercial, and industrial natural gas customers in the U.S., of which 94 percent — over 68 million customers — receive their gas from AGA members. AGA is an advocate for natural gas utility companies and their customers and provides a broad range of programs and services for member natural gas pipelines, marketers, gatherers, international natural gas companies and industry associates. Today, natural gas meets more than one-fourth of the United States' energy needs.

EEI is the association of the nation's shareholder-owned electric utilities and its affiliates world-wide. EEI's U.S. members serve more than 98% of the ultimate customers of electricity in the shareholder-owned segment of the industry and represent about 70% of the U.S. electric power industry. Protecting the nation's electric grid and ensuring a safe and reliable supply of power is the electric power industry's top priority. Thus, managing cybersecurity risk is a top priority.

We appreciate the ongoing effort by NIST to support a broad, cross-sector cybersecurity framework to reduce cybersecurity risk to critical infrastructure. The approach taken by NIST in the *Framework for Improving Critical Infrastructure Cybersecurity* ("Framework") in outlining the core elements of an effective cybersecurity risk management program, and recommending that their application be tailored to reflect each organization's unique business requirements, risks, risk tolerance, and resources provides useful guidance and flexibility that is essential to risk management.

Cybersecurity risk management is not new to our members

Our members already use a number of sector specific standards, guidelines, and practices, which align with the Framework. Examples include the mandatory and enforceable North American Electric Reliability Critical Infrastructure Protection ("NERC CIP") Cybersecurity Standards, the voluntary Department of Energy (“DOE”) Electricity and Oil and Natural Gas Subsector Cybersecurity Capabilities and Maturity Models, the voluntary *Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry*, the Transportation Security Administration ("TSA”) *Pipeline Security Guidelines*, and the voluntary NIST *Guidelines for Smart Grid Cyber Security* (NISTIR 7628). DOE, the Department of Homeland Security (“DHS”), NERC, trade organizations, and asset owners and operators of the Energy Sector have each devoted significant resources to improving cyber risk management.

DOE and industry invested over $9 billion to accelerate the introduction of newer, smarter technologies to the electricity subsector. Funding for these projects required implementation of a cybersecurity plan, including evaluation of: cyber risks and mitigation measures, cybersecurity criteria for device and vendor selection, and relevant standards or best practices.   EEI’s Threat Scenario Project identifies threats and practices to mitigate these threats. Identified threats included coordinated cyber attacks, as well as blended physical and cyber attacks. The project established common elements for each threat scenario, including a description, likely targets, potential threat actors, specific attack paths, and likely impacts of a successful attack. The project continues to evolve as the threat landscape changes in order to keep EEI members prepared to identify and defend against emerging cyber threats. Electric power industry representatives also helped DOE, NIST, and NERC to develop the *Electricity Subsector Cybersecurity Risk Management Process* to help tailor cybersecurity risk management processes to meet organizational requirements. This guideline helps utilities incorporate cybersecurity risk considerations into their existing corporate risk management processes.

The AGA Cybersecurity Task Force has been actively engaged in the development of products and programs intended to strengthen the natural gas utility industry’s cybersecurity posture. In particular, the Small Utility Cybersecurity Project leverages AGA’s Small Member Council to advance the cybersecurity threat mitigation capabilities of small utilities through application of the Oil and Natural Gas Cybersecurity Capability Maturity Model (ONG-C2M2). Similar to EEI’s Threat Scenario Project, AGA published the *Natural Gas Utility Threat Analysis Elements & Mitigations Guidance*. This guidance provides a template for AGA member company’s cybersecurity professionals to engage their senior leadership in discussion of leading cyber-based threats to the gas utility industry. Also, recently the Downstream Natural Gas Information and Analysis Center (“DNG-ISAC”) was established to help support the information sharing interests of downstream natural gas utilities. Recognizing the shared customer base and growing interdependency between natural gas and electric power generation, the DNG-ISAC coordinates and collaborates with the Electricity Sector ISAC (“ES-ISAC”) on physical as well as cyber-related intelligence and incident information sharing. Through this concerted effort, the vast majority of electric companies and natural gas utilities across America have improved situational awareness of the security landscape.

In addition to the coordinated public-private efforts with our government partners, efforts by other organizations, including the National Association of Corporate Directors and the National Association of Regulatory Utility Commissioners have also contributed to raising executive awareness. Although the Framework did not introduce cybersecurity risk management to our members, it has helped to encourage more comprehensive and mature, enterprise-wide approaches to cybersecurity. As a result, many of our members now make regular reports to their board of directors on cybersecurity posture and risk.

Strong member awareness of the Framework

AGA, EEI, and our members actively and consistently engaged with NIST throughout the development of the Framework, supporting the development of a flexible, voluntary tool that leverages existing cybersecurity approaches. We continue to support NIST's efforts by raising awareness of the Framework through a variety our member committees and conferences focused on cybersecurity, through the Electricity Subsector Coordinating Council ("ESCC") and the Oil and Natural Gas Sector Coordinating Council ("ONG SCC"), and in cross-sector venues. Our awareness efforts have focused on different member functions—including regulatory, business continuity, cybersecurity, risk management, and legal professionals—and staffing levels—including security analysts, managers, directors, and executive officers.

AGA also hosted a series of webinars on control system cybersecurity and application of the ONG-C2M2. AGA is also working with small utilities to develop robust cybersecurity programs. This summer, upon member request, EEI established new information sharing and work groups focused on cybersecurity: Cybersecurity Law Group, Enterprise Risk Management Task Force, and a Supply Chain Cyber Integrity Working Group.

The Electricity Subsector is also regulated and subject to mandatory and enforceable cybersecurity standards, the NERC CIP cybersecurity standards. The Federal Energy Regulatory Commission ("FERC" or "the Commission") approves and enforces these standards, on which utilities are formally audited every three years. In April, the Commission held a technical conference to discuss the latest order approving version five of the mandatory cybersecurity standards. A panel during this conference discussed the functional differences between the Framework and the NERC CIP cybersecurity standards. At this conference, EEI stressed the voluntary nature of the Framework, which leverages existing cybersecurity approaches and allows flexible implementation to address specific organizational needs.[1]

Experiences with the Framework are just beginning

Since the NIST Cybersecurity Framework was released in February, EEI and AGA members coordinated through the ESCC, ONG SCC, and DOE, our sector-specific agency ("SSA"), to develop energy sector-specific guidance for using the Framework. *The Energy Sector Cybersecurity Framework Implementation Guidance* ("Implementation Guidance") aligns existing, publicly available sector-specific cybersecurity standards, tools, and processes with the Framework so that entities can continue to or start to use these customized tools to implement the Framework. A key tool used in this guidance is the C2M2, which helps our members assess their cybersecurity capabilities and prioritize their investments to enhance cybersecurity. The Implementation Guidance is currently being finalized by DOE after a 30 day public comment period. Although our members may be waiting for the Implementation Guidance to be finalized

[1] *See* Edison Electric Institute, Prepared Statement of Melanie Seader, Senior Cyber & Infrastructure Security Analyst (April 29, 2014), available at http://www.ferc.gov/CalendarFiles/20140429091439-Seader,%20EEI.pdf.

before considering whether they have “implemented” the Framework, many are focused on using the C2M2, either the ES-C2M2, ONG-C2M2, or generic C2M2.

AGA and EEI members are adapting various risk-based methodologies and cybersecurity approaches to implement the Framework. Some are using control-based approaches such as NIST’s *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST SP 800-53), others are using the C2M2, and some are integrating these and other approaches. The Framework and its alignment with the C2M2 is helpful in encouraging further and more in-depth use of the C2M2 and other cybersecurity approaches. The primary use of the Framework so far has been as an internal tool to help identify strengths and opportunities for improvement of existing cybersecurity practices. However, other uses of the Framework by members include:

1. As an internal communication tool to raise cybersecurity awareness and help integrate cybersecurity risk management into enterprise risk management
2. As an external communication tool to facilitate cybersecurity discussions with domestic and international partners

Initial use of the Framework introduced new challenges

One challenge in developing an industry practice, such as the Implementation Guidance, is that many member utilities belong to multiple critical infrastructure sectors, including Commercial Facilities; Chemical; Communications; Dams; Energy (electricity and oil and natural gas subsectors); Nuclear Reactors, Materials, and Waste; Transportation Systems; and Water and Wastewater Systems. Members encouraged DOE to focus on the Energy Sector and work with DHS and the other SSAs to align the Implementation Guidance with other sector efforts. In addition to coordinating with government partners to develop the Implementation Guidance, DOE also developed the C2M2, a generic version of the ES-C2M2 and ONG-C2M2[2] for use in other sectors, which NIST may want to consider in efforts to improve upon the Framework. Due to interdependencies, the ESCC and ONG SCC have also begun coordinating with other critical sectors to focus on cybersecurity information sharing, tools and technologies, and incident response. AGA also chairs the Joint Cybersecurity Work Group supporting the Oil and Natural Gas, Pipeline, and Chemical Sector Coordinating Councils.

Another challenge is getting suppliers to view cybersecurity as a feature of their products. EEI established a cross-function team of information technology, cybersecurity, sourcing, risk management, and legal professionals to focus on this challenge as well as cyber supply chain integrity risk. Similarly, AGA has set up a task group to address this risk. We are building upon the work of the Energy Sector Control Systems Working Group’s *Cybersecurity Procurement Language for Energy Delivery System*s and the Framework to increase member awareness and partner with our suppliers to improve cybersecurity and cyber supply chain integrity through procurement to build cybersecurity into systems.

[2] See DOE’s Cybersecurity Capability Maturity Model Program at: http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program.

We greatly appreciate the NIST efforts to develop the Framework, listen to and incorporate our feedback, and seek comments from stakeholders on awareness and experiences using the Framework. AGA, EEI, and our members look forward to future collaboration with NIST and our other government partners to improve the cybersecurity of critical infrastructure.

Sincerely,

Scott I. Aaronson
Senior Director, National Security Policy
Edison Electric Institute

Jim Linn
Managing Director, Information Technologies
American Gas Association