April 10, 2017

National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

To Whom It May Concern:

On behalf of our members, the American Gas Association ("AGA") and the Edison Electric Institute ("EEI") are pleased to submit this response as part of the public comment period for the Cybersecurity Framework Draft Version 1.1 ("Draft Framework"), which the National Institute of Standards and Technology ("NIST") published on its website on Tuesday, January 10, 2017.

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 that represents all U.S. investor-owned electric utilities and its affiliates worldwide. Our members provide electricity for 220 million Americans and operate in all 50 states and the District of Columbia, accounting for approximately 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 ability to maintain flexibility, while sufficiently detailing program components to provide substantive guidance is essential to risk management. The voluntary, high-level nature of the Framework has been critical to its successful deployment throughout industry, and has continued to strengthen the trusted partnership between NIST and private industry.

We believe NIST did an excellent job soliciting input and feedback during the initial drafting of the Framework, during which the Energy Sector was an active participant. As supporters of the NIST process, we appreciate the opportunity to provide the following comments and recommendations on the Draft Framework. We ask that NIST continue to maintain the Framework as a voluntary baseline tool. The Framework should be informative and high level, not prescriptive, and should not take positions in conflict with existing enforceable industry standards. More specific comments to the questions posted by NIST in the Draft Framework, and redline comments on the Draft Framework itself, are included in the attached documents. We look forward to participating in the May workshop.

The Framework should remain a voluntary baseline tool that identifies existing, cross-sector critical infrastructure cybersecurity standards and guidance

Cybersecurity capabilities vary by sector and entity. As noted during the initial drafting of the Framework, reducing the nation's cyber risk requires bringing the cybersecurity of critical infrastructure from all 16 sectors up to a minimum baseline level. This level will not be achieved in the same way for each sector, nor will it be achieved homogenously by organizations within each sector as they all have different critical infrastructure risk profiles. Anything further should continue to be addressed at the sector level through additional guidance in coordination with Sector-Specific Agencies ("SSA").

Strong member use and promotion of the Framework

After the NIST Cybersecurity Framework was released, AGA and EEI members worked with their SSA, the Department of Energy, to align existing cybersecurity risk management programs and tools with the Framework, ultimately producing the *Energy Sector Cybersecurity Framework Implementation Guidance* ("Implementation Guidance"). AGA and EEI members adapted various control-based approaches such as NIST's *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST SP 800-53), others used DOE's Cybersecurity Capability Maturity Model ("C2M2"), and some have integrated these and other approaches. The Framework and its alignment with C2M2 is helpful in encouraging further and more in-depth use of the C2M2 and other cybersecurity approaches. The Implementation Guidance will be updated to incorporate the new additions to the Framework, once finalized.

AGA, EEI, and our members continue to support NIST's efforts by raising awareness of the Framework through a variety of means, including outreach to our member committees and conferences focused on cybersecurity, through the Electricity Subsector Coordinating Council ("ESCC") and the Oil and Natural Gas Subsector Coordinating Council ("ONG SCC"), and in cross-sector venues. Though our members have already employed various cybersecurity risk management activities, the Framework has helped to encourage more comprehensive and mature, enterprise-wide approaches to cybersecurity.

Cybersecurity risk management is a top priority of our members

In addition to the Framework, our members continue to use a number of sector specific standards, guidelines, and practices. Examples include the mandatory and enforceable North American Electric Reliability Corporation Critical Infrastructure Protection ("NERC CIP") Cybersecurity Standards, DOE's voluntary 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). These existing requirements and guidelines provide comprehensive guidance that help electricity asset owners and operators to assess, develop, and improve their cybersecurity capabilities. 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.

Minimize duplication of efforts, and avoid conflicting with existing rules and standards

In July 2016, the Federal Energy Regulatory Commission ("FERC") issued an order directing the NERC to "develop a forward-looking, objective-driven Reliability Standard that provides security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations." [1] The NERC CIP standard, *CIP-013-1 – Cyber Security – Supply Chain Risk Management* ("NERC CIP-013-1"), is currently in draft form. Publishing an updated Framework prior to the release of this mandatory, enforceable standard will be inherently problematic for combination gas-electric companies. NIST should avoid taking a position in opposition to this standard, as it will discourage entities required to implement NERC CIP-013-1 from also implementing version 1.1 of the NIST Cybersecurity Framework. NIST should work to harmonize the Framework updates with the approved version of NERC CIP-013-1 to avoid a counterproductive duplication of efforts.

Supply Chain Risk Management is an ongoing challenge

We view the addition of supply-chain risk management as a substantial improvement to the original Cybersecurity Framework, provided that it aligns with the aforementioned NERC CIP-013-1. We ask, however, that NIST review the updated text and appendices for relevance to operational technology (OT) in addition to information technology (IT), which appears to be the current focus of the draft language. Industry already has taken a number of steps to work with suppliers on viewing 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. Both AGA and EEI members are involved in DOE's supply Energy Sector Critical Manufacturers Working Group (ESCMWG), which works to bring together utilities and the vendor community to address supply chain risks.

The updated Framework should continue to be informative and voluntary guidelines, but not prescriptive

Determining what is prescriptive may be difficult due to the volume of input received by NIST from various stakeholders who have different experience, expertise, and perspective. A foundational characteristic of the Framework is that it remains a voluntary guide and is not an auditable standard. Drafters should be careful not to introduce prescriptive and directive language into the Framework, which creates risk for companies and may lead to reduced implementation of the updated Framework. Some of the newly proposed language, particularly in Section 4.2, "Types of Cybersecurity Measurement" is too prescriptive and points to specific technologies, creating applicability problems across the 16 sectors. Given the rapid evolution of tools and capabilities, the Framework and subcategories should continue to be outcome/objective focused to remain technology neutral. Avoiding specific technical solutions enables asset owner and operators to select the practices to reduce risk as well as the appropriate security controls and technologies to be used.

[1] Revised Critical Infrastructure Protection Reliability Standards, Order No. 829 156 FERC ¶ 61,050 at P 4 (July 21, 2016).

Framework methodology should be tailored to improving critical infrastructure cybersecurity while protecting individual privacy and civil liberties

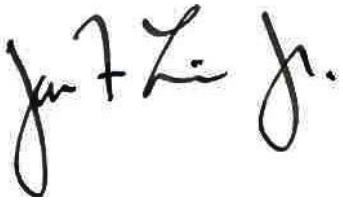
Section 7(c) of Presidential Executive Order 13636 specifies that "[t]he Cybersecurity Framework shall include methodologies to identify and mitigate impacts of the Cybersecurity Framework and associated information security measures or controls on business confidentiality, and to protect individual privacy and individual liberties."[2] Protecting customer privacy and civil liberties is important, and issues regarding those matters raised during the initial drafting of the Framework remain. However, we are concerned that instead of focusing on means to limit the privacy impacts of the Framework, the methodology appears to recommend independent privacy protections unrelated to the protection of critical infrastructure. Similar to risk management, the scope of privacy and civil liberty protections are beyond that of cybersecurity. The purpose of the framework is to "help owners and operators of critical infrastructure identify, assess, and manage cyber risk."[3] The methodology provided should be tailored to the purpose of the Framework: to improve critical infrastructure cybersecurity. Additionally, it is critical that the privacy methodology is clear and actionable. The existing language does not readily allow companies to discern how to use the methodology or determine whether current practices already incorporate its elements.

Consider who is providing input to the Draft Framework process

Finally, we recommend that NIST consider who is providing the input when updating the Framework and determining how to use the input. We recognize and support NIST's efforts to encourage feedback from critical infrastructure owners and operators and cybersecurity staff, specifically those who have operational, managerial and policy experience and responsibilities for cybersecurity, technology and/or standards development for critical infrastructure companies.

We greatly appreciate the NIST efforts to update the Framework, as well as to listen to and incorporate our feedback. AGA, EEI, and our members look forward to continued collaboration with NIST and our other government partners to improve the cybersecurity of critical infrastructure.

Sincerely,



Scott I. Aaronson
Executive Director, Security & Business Continuity
Edison Electric Institute

Jim Linn
Managing Director, Information Technology
American Gas Association

---

2 The President, Executive Order 13636—Improving Critical Infrastructure Cybersecurity, February 19, 2013, http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

3 Executive Order 13636, Improving Critical Infrastructure Cybersecurity Sec. 7(b).

With the release of the Cybersecurity Framework Draft Version 1.1, NIST requested answers to the following questions:

Are there any topics not addressed in the draft Framework Version 1.1 that could be addressed in the final?

- No additional topics should be addressed in Version 1.1. However, the discussion of metrics in the new section "4.0 Measuring and Demonstrating Cybersecurity" could be expanded with the addition of additional practical guidance.

How do the changes made in the draft Version 1.1 impact the cybersecurity ecosystem?

- There is a greater emphasis on supply chain, though unfortunately the focus is largely on compliance-oriented controls. These types of controls may have some value but they often are not preventive. Reference to industry-standard certifications should be considered. For operational technology, there should be a greater recognition of the role of vendor involvement in system design and configuration.
-

For those using Version 1.0, would the proposed changes impact your current use of the Framework? If so, how?

- We do not see substantial impact. The added language would provide additional support for third-party security review programs, however, NIST should recognize that under the current way SCRM has been incorporated in the Draft Framework, companies may not be able to identify as "Adaptive" if its suppliers are not SCRM compliant.

For those not currently using Version 1.0, does the draft Version 1.1 affect your decision to use the Framework? If so, how?

- Many of our members currently use the Framework. We anticipate that following the publication of version 1.1, the changes to the Framework will be reviewed for use by our members.

Does this proposed update adequately reflect advances made in the Roadmap areas?

- No opinion.

Is there a better label than "version 1.1" for this update?

- No opinion.

Based on this update, activities in Roadmap areas, and activities in the cybersecurity ecosystem, are there additional areas that should be added to the Roadmap? Are there any areas that should be removed from the Roadmap? Comments:

- The next revision of the Framework should focus on challenges associated with operational technology (as compared to IT) and the emerging Internet of Things (IoT).