



January 19, 2018

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 Draft 2 of the Cybersecurity Framework Version 1.1 (“Draft Framework”), which the National Institute of Standards and Technology (“NIST”) published on its website on Tuesday, December 5, 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 companies. Our members provide electricity for 220 million Americans, and operate in all 50 states and the District of Columbia. As a whole, the electric power industry supports more than 7 million jobs in communities across the United States. 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 effort by NIST to continue supporting a broad, cross-sector Cybersecurity Framework to reduce cybersecurity risks 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 is directly related to its successful deployment by industry, which strengthens the trusted partnership between NIST and private industry.

NIST continues to excel at soliciting input and feedback on updates and changes to the Framework, and the Energy Sector will continue to be an active participant. As supporters of the NIST process, we appreciate the opportunity to provide comments and recommendations on both Draft 1 and 2 of the Draft Framework version 1.1. 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 or regulations. More specific comments and suggested changes to the proposed edits in the Draft Framework are included in the attached document.

The Framework should remain a voluntary baseline tool

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 DOE’s Cybersecurity Capability Maturity Model (“C2M2”). AGA and EEI members are currently engaged in a working group to update the C2M2 to reflect the changes in the Framework for version 1.1. 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 also 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 facilitated more comprehensive and mature, enterprise-wide approaches to cybersecurity.

Align with existing, cross-sector critical infrastructure cybersecurity standards and guidance

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, and the Transportation Security Administration (“TSA”) *Pipeline Security Guidelines*. These existing requirements and guidelines provide comprehensive guidance that help electricity asset owners and operators assess, develop, and improve their cybersecurity capabilities.

Maintain harmony with existing rules and standards to sustain use of the Framework

We view the addition of supply-chain risk management as a substantial improvement to the original Cybersecurity Framework. 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 awaiting FERC approval. Once this standard is approved by FERC, electric sector entities required to implement NERC CIP-013-1 and the other related supply chain requirements will be focused first on implementing these new regulations, which may delay their implementation of version 1.1 of the NIST Cybersecurity Framework. The Framework and mandatory requirements cannot be the same due to the voluntary nature of the Framework and the need to enforce the mandatory requirements. However, maintaining harmony between the Framework and mandatory requirements will be important to sustaining the use of the Framework by electric companies.

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

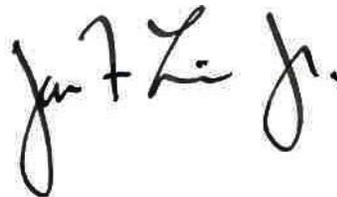
Determining what is prescriptive may be difficult due to the volume of input received by NIST from various stakeholders who have different experience, expertise, and perspective. A foundational characteristic of the Framework is that it remains a voluntary guide and is not an auditable standard. We appreciate NIST’s concerted effort to remove much of the prescriptive and directive language that was included in Draft 1. The Framework and subcategories should continue to be outcome/objective focused to remain technology neutral.

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 strengthen the cybersecurity of critical infrastructure.

Sincerely,



Scott I. Aaronson
Vice President, Security & Preparedness
Edison Electric Institute



Jim Linn
Chief Information Officer
American Gas Association

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