December 13, 2013

Information Technology Laboratory
ATTN: Adam Sedgewick
National Institute of Standards and Technology
10 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930

RE: Request for Comments on the Preliminary Cybersecurity Framework

Dear Mr. Sedgewick,

On behalf of the American Gas Association (AGA), American Public Power Association (APPA), Edison Electric Institute (EEI), Electric Power Supply Association (EPSA), GridWise Alliance (GWA), Large Public Power Council (LPPC), National Rural Electric Cooperative Association (NRECA), Utilities Telecom Council (UTC), and our members I am pleased to submit the following comments to help the National Institute of Standards and Technology (NIST) finalize the Cybersecurity Framework as required by Executive Order 13636, *Improving Critical Infrastructure Cybersecurity* (EO).

We appreciate the effort by NIST to develop a broad, cross-sector Cybersecurity Framework to reduce cybersecurity risk to critical infrastructure. We recognize the substantial challenge inherent in an effort to draw program components in sufficient detail to provide substantive guidance, while remaining sufficiently flexible to apply across sectors of the economy with very diverse cybersecurity risk profiles. The general approach taken b NIST in outlining the core elements of an effective program, and recommending that their application be tailored to reflect each organization's unique business requirements, risks, risk tolerance, and resources makes sense, as it simultaneously provides useful guidance and essential flexibility.

As active participants in the NIST process, we appreciate the opportunity to provide the following comments and recommendations based on our observations from participation in all five NIST workshops and reviewing the Preliminary Cybersecurity Framework (Framework). Although these comments use numbered bullets, each is important and we expect them to be weighted equally by NIST. Many of us and our members representing the Energy Sector have also submitted more detailed comments and recommendations.

For follow-up questions about our comments, we encourage you to contact:

Jim Linn, AGA (202-824-7272, jlinn@aga.org)
Nathan Mitchell, APPA (202-467-2925, nmitchell@publicpower.org)
David Batz, EEI (202-508-5064, dbatz@eei.org)

Jack Cashin, EPSA (202-628-8200, Jcashin@epsa.org)
Ladeene Freimuth, GWA (202-550-2306, ladeene@freimuthgroup.com)
Jonathan Schneider, LPPC (202-728-3034, JSchneider@stinson.com)
Barry Lawson, NRECA (703-907-5781, barry.lawson@nreca.coop)
Nadya Bartol, UTC (202-833-6809, nadya.bartol@utc.org)

KEY ENERGY SECTOR RECOMMENDATIONS

1. Section 3.0 of the Framework should support sector-level coordination to develop implementation guidance

Efforts to improve cybersecurity are not new to the Energy Sector. The Sector already uses a number of sector specific standards, guidelines, and practices, which can be aligned with the Framework. Examples include the North American Electric Reliability Critical Infrastructure Protection Standards (NERC CIP Standards), the Electricity Subsector Cybersecurity Capabilities and Maturity Model (ES–C2M2), and the Electricity Subsector Cybersecurity Risk Management Process (RMP). As a result, DOE, DHS, NERC, trade organizations, and asset owners and operators of the Energy Sector, have already devoted significant resources towards reducing cyber risk.

To encourage critical infrastructure owner and operator use of the Framework, we recommend that NIST support the sector-level effort as described by Section 8 (b) of the Executive Order in the Framework's Section 3.0, How to Use the Framework. In Section 3.0, NIST should encourage the sectors to coordinate with their Sector-Specific Agencies, through their Sector Coordinating Councils to review the Cybersecurity Framework and develop implementation guidance to integrate existing and future efforts "to address sector-specific risks and operating environments."[1] This will enable the Energy Sector to leverage and integrate cybersecurity improvements already underway into the Framework. Also, at the sector-level, cybersecurity risk management can be tailored to unique sector characteristics, and through existing partnerships be equipped to leverage expertise from across the sector to increase efficiency and properly leverage resources to use the Framework to reduce cyber risk to critical infrastructure.

NIST's support of sector-level coordination to develop implementation guidance will also improve the likelihood of the success of the Program DHS is tasked with establishing "to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure."[2] Sector-level coordination can also be used to sustain the Framework engagement and involvement of all 16 critical infrastructures, which can be leveraged in developing future Framework versions based on sector progress and environmental changes (e.g., threat, technology).

[1] Executive Order 13636, Improving Critical Infrastructure Cybersecurity Sec. 8(b).
[2] Executive Order 13636, Improving Critical Infrastructure Cybersecurity Sec. 8(a).

2. The focus of the Framework should be limited to the systems and assets essential to critical infrastructure functions and this focus should be made clear throughout the Framework and the appendices

The scope of risk management is beyond cybersecurity. Organizations must consider a number of business risks (e.g., compliance, financial, operational, and reputational) for business continuity. Risk management is important in understanding and addressing cybersecurity; however, the purpose of the Framework is to "Reduce Cyber Risk to Critical Infrastructure" and not to reduce all broader business risks that an organization might face.[3] Therefore the scope of the Cybersecurity Framework should be clearly limited to cybersecurity for critical infrastructure, the purpose of Executive Order 13636.

To "provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach"[4] the Framework's focus must be on the systems and assets essential to critical infrastructure functions. This focus helps ensure that available resources are targeted at reducing critical infrastructure cybersecurity risk. We support the Framework definition of Critical infrastructure[5] in the Introduction and Glossary. However, the scope of the Framework in other sections and the appendices appears to be broader and thereby the focus of the Framework is unclear.

The Framework Core is particularly confusing as it references "business purposes," "business needs," "business objectives," and other similar business-mission focused language rather than focusing on the systems and assets essential to critical infrastructure functions. Critical infrastructure is not defined by the business missions of each of the 16 sectors identified in PPD-21, but is specific to the operation of the systems and assets critical to the national economy, health, safety, and security. Not all systems and assets within each entity of the 16 critical infrastructure sectors are critical to the nation's economy, health, safety, and security and therefore not all systems and assets should be the focus of the Framework.

The existing, broad business scope will reduce the focus on critical infrastructure and may result in organizations devoting limited resources to systems and assets that are not essential to critical infrastructure functions. As a result, the EO efforts to improve critical infrastructure cybersecurity will be diluted. A risk-based approach focused on the systems and assets essential to the critical infrastructure function enables organizations to identify and prioritize the protection, detection, response, and recovery activities that will help improve critical infrastructure

[3] Executive Order 13636, Improving Critical Infrastructure Cybersecurity, February 12, 2013.

[4] *Ibid*., Sec. 7(b).

[5] Critical infrastructure is defined as the "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." EO 13636 Sec. 2, Patriot Act of 2001.

cybersecurity. Organizations that do not have critical infrastructure can still use the Framework to improve their cybersecurity posture by focusing on the systems and assets that are essential to their organizational or business functions.

3. How the Framework Core, Profiles, and Implementation Tiers can be used together to reduce cyber risk to critical infrastructure should be made clear in Section 3.2

The Framework Core (Core) includes the cybersecurity practices that are common across all of the critical infrastructure sectors. This Core provides a baseline set of practices that can be leveraged by organizations to build or improve upon their existing cybersecurity program. The Framework Profile is intended to be "a tool to enable organizations to establish a roadmap for reducing cybersecurity risk."[6] However, the Framework is unclear regarding how the profiles are built using the Core; the Implementation Tiers focus on the maturity of an organization's risk management process rather than implementation of the Core practices.

A risk-based approach requires a cybersecurity risk assessment to prioritize these risks, which can be addressed through specific cybersecurity practices. Risk assessment and prioritization is addressed under the Identify function of the Core and the other Core functions address best practices that can be used to respond to cybersecurity risk. Therefore, a possible approach to clarifying the use of the Core Profiles, and Implementation Tiers is:

- Step 1: Integrate cybersecurity into an existing or new risk management process to address the applicable categories and subcategories of the Identify Function

- Step 2: Based on the risk assessment and prioritization created by the implementation of a risk management process (Step 1), implement the applicable practices found in the categories and subcategories of the Core functions Protect, Detect, Respond, and Recover. During this implementation step, profiles can be created to establish a roadmap and track progress toward reducing cybersecurity risk.

- Step 3 (ongoing): Once integrated, the risk management process can be periodically reviewed against the Implementation Tiers to mature the process. This is an ongoing process that will require assessing risk, reprioritizing, and making changes to the applicable cybersecurity practices found in the Core.

[6] Preliminary Cybersecurity Framework, lines 282-283.

4. The subcategory language should be edited to reduce redundancy, focus on clear outcomes, and relate to the risk management process

We greatly appreciate NIST's recent efforts toward improving the subcategory language in the Framework Core. Non-prescriptive language at the cross-sector level is appropriate because diverse users can select the appropriate controls and technologies to meet the cybersecurity outcomes described in the Core. However, in some areas of the core, the subcategory language is redundant and vague, which may lead to inconsistent interpretations within and across the 16 critical infrastructure sectors.

Regarding redundancy and vagueness, many of these details will be addressed by individual entities providing comments using the NIST template. As a vagueness example, several subcategories use "managed," "protected," or "secured." It is unclear what these terms mean and how they differ from each other. Each subcategory should be managed under the risk management process, but determining whether an asset is protected or secured is uncertain as the organizations' risk environments vary and change over time. Therefore relating these terms in the subcategory language to the risk management process will add the needed clarity.

5. The body of the Framework should make it clear that the use or applicability of the subcategories may vary by organization

Although the introductory text in Appendix A, the Core, mentions that the Core is not exhaustive and is extensible, this direction is not foun in the body of the Framework. The use of subcategories will vary by organizations within and across the 16 critical infrastructure sectors depending on their particular critical infrastructure systems, assets, and risk. For example, the Energy Sector not only includes organizations of various size and ownership structures, but also organizations that are a part of other critical infrastructures. Establishing new protective cybersecurity technological or procedural controls can also undermine existing protections if not executed in a thoughtful, coordinated manner.

Not all subcategories, therefore, may be applicable and some categories may need to be added during implementation to address a specific risk to a particular sector or organization. Therefore it should be made clear in the body of the Framework (including Sections 1.1, 2.0, and 3.0) that the use or applicability of the subcategories may vary by organization. This will help to encourage organizations to make well-reasoned, risk-based cybersecurity decisions.

6. Appendix B should be revised to focus on protecting privacy and civil liberties implicated by critical infrastructure cybersecurity activities

Section 7(c) of the Executive Order 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." Protecting the customer privacy and civil liberties is important. However, we are concerned that, instead of focusing on means to limit the privacy impacts of the Framework, Appendix B 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."[7] The methodology in Appendix B should be revised to tailor the methodology 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 Appendix B does not readily allow companies to discern how to use the methodology or determine whether current practices already incorporate its elements. We observe that Harriet Pearson, as a "result of discussions of representatives from a variety of industry sectors," provided NIST with an alternative to Appendix B[8] that presents concepts and principles that are more actionable and process oriented than the existing Appendix B. NIST should view this alternative to Appendix B as a strong reference for improving the methodology to protect privacy and civil liberties implicated by critical infrastructure cybersecurity activities.

7. The definition of Framework adoption has not obtained general consensus

In the December 4, 2013 "Update on the Development of the Cybersecurity Framework" (Update), NIST described that "general consensus" was developed based on discussion at the November Raleigh Workshop for a definition of Framework adoption.[9] However, we did not observe such a consensus, but we did observe that the Workshop audience did not generally accept the term or clearly understand the definition of adoption. The definition provided by NIST in the Update was proposed by DHS for discussion specific to the Voluntary Critical Infrastructure Cybersecurity Program (Program), but has not yet received general consensus. An organization would not "comply" with the Framework but use it to achieve a goal. We recommend that NIST simplify the adoption definition[10] to: an

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

[8] December 5, 2013, Harriet P. Pearson. http://csrc.nist.gov/cyberframework/framework_comments/20131205_harriet_pearson_hoganlovells.pdf

[9] NIST, Update on the Development of the Cybersecurity Framework, December 4, 2013, http://www.nist.gov/itl/upload/nist_cybersecurity_framework_update_120413.pdf.

[10] "An organization adopts the framework when it uses the Cybersecurity Framework as a key part of its systematic process for identifying, assessing, prioritizing, and/or communicating: cybersecurity risks, current approaches and efforts to address those risks, and steps needed

organization adopts the framework when it voluntarily uses the framework as a part of its risk management process or strategy to protect critical infrastructure.

We appreciate the opportunity to submit these comments to NIST and look forward to continuing to collaborate with NIST to finalize the Framework; the Department of Energy (DOE), our Sector-Specific Agency, to develop sector-specific implementation guidance; and the Department of Homeland Security (DHS) and DOE to provide Energy Sector input for the establishment of and support participation in the Voluntary Critical Infrastructure Cybersecurity Program (Program).

Sincerely,

Edward H. Comer

Vice President & General Counsel
Edison Electric Institute

to reduce cybersecurity risks as part of its management of the organization's broader risks and priorities." *Ibid*.