Electric Power Industry Views on the
Framework for Improving Critical Infrastructure Cybersecurity

February 23, 2016

On behalf of our members, the American Public Power Association, the Edison Electric Institute, the Electric Power Supply Association, the Large Public Power Council, the National Rural Electric Cooperative Association, and the Utilities Telecom Council, submit these comments in response to the December 11, 2015 National Institute of Standards and Technology (NIST) Request for Information (RFI).

The American Public Power Association (APPA) is the national service organization representing the interests of non-profit, state and locally-owned electric utilities. More than 2,000 public power systems provide over 15 percent of all kilowatt-hour sales to ultimate customers and operate in every state except Hawaii and provide electricity to U.S. territories such as Puerto Rico, Guam, and American Samoa. Collectively, public power utilities serve 48 million Americans.

The Edison Electric Institute (EEI) is the association that represents all U.S. investor-owned electric companies. Our members provide electricity for 220 million Americans, operate in all 50 states and the District of Columbia, and directly employ more than 500,000 workers. With $100 billion in annual capital expenditures, the electric power industry is responsible for millions of additional jobs. Safe, reliable, affordable, and clean electricity powers the economy and enhances the lives of all Americans.

The Electric Power Supply Association (EPSA) is the national trade association representing leading competitive power suppliers, including generators and marketers that are active participants in physical commodity markets with related commercial hedging activities. These suppliers account for nearly 40 percent of the installed generating capacity in the United States and provide reliable and competitively priced electricity from environmentally responsible facilities. EPSA seeks to bring the benefits of competition to all power customers. The comments contained in this filing represent the position of EPSA as an organization, but not necessarily the views of any particular member with respect to any issue.

The Large Public Power Council (LPPC) is an association of 26 of the nation's largest municipal and state-owned utilities, located in eleven states in all regions of the nation. LPPC speaks for the larger, asset-owning members of the public power community, representing 34,000 miles of transmission and 90% of the transmission investment owned by non-Federal public power entities in the United States.

The National Rural Electric Cooperative Association (NRECA) is the national service organization dedicated to representing the national interests of cooperative electric utilities and

the consumers they serve. NRECA is the national service organization for more than 900 not-for-profit rural electric utilities that provide electric energy to over 42 million people in 47 states or 12 percent of electric customers. Kilowatt-hour sales by rural electric cooperatives account for approximately 11 percent of all electric energy sold in the United States. NRECA members generate approximately 50 percent of the electric energy they sell and purchase the remaining 50 percent from non-NRECA members. The vast majority of NRECA members are not-for profit, consumer-owned cooperatives. NRECA's members also include 65 generation and transmission ("G&T") cooperatives, which generate and transmit power to 668 of the 838 distribution cooperatives. The G&Ts are owned by the distribution cooperatives they serve. Remaining distribution cooperatives receive power directly from other generation sources within the electric utility sector. Both distribution and G&T cooperatives were formed to provide reliable electric service to their owner-members at the lowest reasonable cost.

The Utilities Telecom Council (UTC) is a global trade association that focuses on information and communications technology (ICT) challenges for utilities and other critical infrastructure industries. UTC's members range from large investor-owned utilities to small rural electric cooperative utilities and municipal utilities. UTC members also include providers delivering ICT products and services to utilities. UTC has been an active participant in the NIST Cybersecurity Framework process. In addition to contributing to the Framework itself, we have continuously made our membership aware of the Framework's benefits and have worked with UTC members to use the NIST Framework to establish, assess, or improve their cybersecurity programs.

Summary

Our members generate, transmit, and/or deliver electricity to residential, commercial, and industrial consumers and therefore our comments are specific to the electric power industry. As an industry that already has significant regulations for reliability and cybersecurity of the Bulk Electric System (BES), our comments and experiences may not be applicable to the other critical infrastructure subsectors and sectors.

In developing the Cybersecurity Framework (the Framework), we believe that NIST did an excellent job with a challenging task in facilitating and consolidating industry input with transparency and active stakeholder engagement. The Framework is being used by our members in a variety of ways. Our experience with the Framework has shown that it provides a beneficial educational and communication tool for enterprise-wide cybersecurity efforts. Many other regulations, standards, best practices, and tools have been used by our members and are in many instances linked to the Framework to provide further technical guidance to our members. We encourage NIST not to make changes to the Framework at this time, but pursue further guidance in other efforts that can be linked to the Framework (e.g., Framework implementation workshops). This approach would allow NIST to continue to govern the Framework, while enabling different guidance and tools to be leveraged to enhance cybersecurity efforts.

I. Use of the Framework and Sharing Information

We strongly support the voluntary model of the Framework. However, cybersecurity and reliability for our most critical assets, our generation and transmission facilities, are already regulated by the Federal Energy Regulatory Commission (FERC). Therefore, despite the intended voluntary nature of the Framework, it is important to recognize that it can still have a regulatory impact on our members. For example, in April 2014, just two months after the release of the Framework, during a technical conference on the Critical Infrastructure Protection (CIP) Cyber Security Standards, among the issues addressed by FERC was "how the CIP version 5 Standards could be adjusted to address any concern or weaknesses," whether the approaches identified in the "NIST Cyber Security Framework are more appropriate," for "comparisons between the CIP version 5 Standards security controls and the security controls" of the Framework, and "identification of specific security controls or control objectives that should be considered in future revisions of CIP standards." Therefore the Framework as well as any other cybersecurity standard, regulation, or practice is likely to be reviewed and evaluated by FERC to determine if there are gaps in our cybersecurity regulatory requirements.

The electric power industry is in the process of concluding a significant effort to implement version 5 of the CIP standards. CIP version 5 is a comprehensive set of ten mandatory and enforceable cybersecurity standards (CIP-002-5.1 through CIP-011-1), which are focused on identification, protection, detection, response, and recovery efforts, an approach consistent with the Framework. CIP version 5 brings thousands of new generation and transmission systems and facilities under regulatory scope.

However, despite the resource intensive CIP version 5 implementation effort, our members use the Framework. For assets that fall under CIP version 5, we have leveraged industry association efforts such as the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection Committee (CIPC) to map these requirements to the Framework. Our members have also benefited from use of the Framework beyond mapping to our regulatory requirements.

Prior to the release of the Framework we worked closely with our sector specific agency, the Department of Energy (DOE) to develop the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2). Many of our members have found this tool more useful in providing more technical and sector-specific guidance. Therefore through the Electricity Subsector Coordinating Council (ESCC), we worked with DOE to develop Framework implementation guidance, which included an approach that leverages the ES-C2M2. The Smart Grid Interoperability Panel (SGIP) has also been working with the industry to create detailed Framework implementation guidance.

Many members use a blended approach that combines the NIST Framework, ES-C2M2, NIST SP 800-53, and other tools. For example, members may use ES-C2M2 assessments to

baseline, identify, prioritize, and address gaps among various business units, enterprise-wide; and NIST Special Publication (SP) 800-53 to conduct system assessments. NRECA has also developed guidance tailored to electric cooperatives which can be downloaded from: https://groups.cooperative.com/smartgriddemo/public/CyberSecurity/Pages/default.aspx. Some of our members use Governance, Risk, and Compliance (GRC) that have incorporated the NIST Framework as well as CIP requirements, standards, practices, and guidelines into such tools.

Also, members use the Framework as a basis for improving data protection and as a communication tool. It also helps to facilitate communications regarding security posture and requirements to our members' leadership, suppliers, and other partners. For example, we referenced the Framework in the development of the *Cybersecurity Procurement Language for Energy Delivery Systems*.[1]

II. Possible Framework Updates and the Future Governance of the Framework

Changes to the Framework at this time, even incremental ones, could negatively impact the balance between the Framework and our industry specific cybersecurity efforts. The electric power industry has devoted significant resources to map cybersecurity regulations, standards, guidance, best practices, and tools to the Framework. Framework changes would require updating these mappings as well as related risk assessments. Also, although many baseline cybersecurity risk assessments have been conducted, many of our members are beginning to conduct follow-up assessments to gauge progress towards reaching their targeted profiles. If the Framework is updated before this is done, baseline assessments may need to be redone, which will impede rather than enhance progress. As a result, we do not currently support changes to the Framework or transitioning the Framework to the private sector for further updates. The real value of the Framework to our industry is that it aligns various cybersecurity practices to provide a view of cross-sector practices and enables sector-specific practices to be aligned to help us identify efficiencies and gaps.

Instead of updating the Framework, we suggest evaluating the need for additional implementation resources specific to particular users such as information and communication technology manufacturers and service providers. Possible implementation resources could include: a data protection implementation guidance leveraging the Framework and implementation guidance specific to particular needs such as information and communication technology (ICT) manufacturers, other suppliers, and service providers.

Also, FERC has recently proposed to create supply chain risk management requirements for electric power utilities, which are likely to require user utilities to leverage their contracting processes to encourage industrial control system suppliers and service providers to improve their

[1] Energy Sector Control Systems Working Group, *Cybersecurity Procurement Language for Energy Delivery Systems*, April 2014, available at: *http://www.energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf*.

supply chain security practices. Instead of electric power industry specific requirements, NIST could develop a cross-sector supply chain risk management resource focused on the acquisition and delivery stages of the supply chain life cycle. For such a resource to be useful, it needs to be easy to use and applicable to all the critical infrastructure sectors as well as the manufacturers, suppliers, and service providers of ICT.

NIST could also facilitate discussions between different stakeholders regarding risk management decision making and risk impacts. There are currently many resources for improving cybersecurity but there is not a resource available to guide the process of balancing the value of risk mitigation with the risk impact for various stakeholders. Such discussions would be helpful in evaluating the benefits of emerging capabilities and technologies and the related risks they introduce to critical infrastructure.

Conclusion

We greatly appreciate the NIST efforts on the Framework, including listening to and incorporating feedback from stakeholders. APPA, EEI, EPSA, LPPC, NRECA, UTC, 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
Managing Director, Electric Sector and National Infrastructure Protection
Edison Electric Institute
(202) 508-5481
saaronson@eei.org

Nadya Bartol, CISSP, CGEIT
Vice President of Industry Affairs and Cybersecurity Strategist
Utilities Telecom Council
(202) 833-6809
nadya.bartol@utc.org

Jack Cashin
Director of Regulatory Affairs
Electric Power Supply Association
(202) 628-8200
jcashin@epsa.org

John DiStasio
President
Large Public Power Council
(202) 298-3723
John@lppc.org

Barry R. Lawson
Associate Director, Power Delivery & Reliability
National Rural Electric Cooperative Association
(703) 907-5781
barry.lawson@nreca.coop

Nathan Mitchell, PE
Sr. Director, Electric Reliability Standards & Security
American Public Power Association
(202) 467-2925
nmitchell@publicpower.org