April 8, 2013

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

RE: NIST Docket No. 130208119-3119-01
Comments of the Electric Trade Associations in Response to NIST's Request for Information on "Developing a Framework to Improve Critical Infrastructure Cybersecurity."

Dear Ms. Honeycutt:

The American Public Power Association ("APPA"), Large Public Power Council ("LPPC"), National Rural Electric Cooperative Association ("NRECA"), and Transmission Access Policy Study Group ("TAPS") (collectively the "Electric Trade Associations") jointly on behalf of their respective members submit these comments in response to the notice and request for information ("RFI") on "Developing a Framework to Improve Critical Infrastructure Cybersecurity," issued on February 26, 2013 by the National Institute of Standards and Technology ("NIST").[1;2]

The Electric Trade Associations represent entities within the electric subsector that will be asked to adopt any voluntary industry standards, methodologies, procedures and processes that are developed pursuant to the final Cybersecurity Framework that is to be published by the Director of NIST, pursuant to the President's February 12, 2013 Executive Order on Improving Critical Infrastructure Cybersecurity ("EO").[3] All of our respective members operate in the electric subsector.

[1] NIST RFI, Docket No. 130208119-3119-01, 78 Fed. Reg. 13,024–28 (Feb. 26, 2013).

[2] Each of the Electric Trade Associations are participants in the April 8, 2013 Comments on the NIST RFI submitted by the "Electric Power Sector Coalition."

[3] ''Executive Order 13636—Improving Critical Infrastructure Cybersecurity," 78 FR 11739 (February 19, 2013).

Our respective member electric utilities provide highly reliable and affordable electric service to their customers. Our members have a long history of reliability excellence and a proven commitment to maintaining high standards as technology evolves. Cybersecurity is central to the day-to-day operations of our member utilities across the country, each of which manages cybersecurity programs tailored to its unique operations, assets and communications networks. Each of our members is committed to working with their respective suppliers of equipment, fuel and other inputs to the electricity supply chain and with their electricity end-use customers to enhance the protection and resiliency of the nation's critical infrastructure from cyber attack.

The Electric Trade Associations vigorously support the provisions in the EO furthering information sharing by government agencies with critical infrastructure owners and operators. We welcome the EO's directive to the Secretary of Homeland Security and the Attorney General to establish a process providing for the rapid dissemination of unclassified and classified information relevant to cyber vulnerabilities, along with information available under the Cybersecurity Services program, to critical infrastructure entities. In the past, much of this information has been shielded from entities seeking to manage cyber vulnerabilities. Establishing strong public-private information sharing practices between federal government agencies charged with ensuring domestic security, the intelligence community and industry is essential in protecting critical assets from intrusion and disruption. The Electric Trade Associations are confident that the provision of actionable information on cyber threats and vulnerabilities, along with the provision of associated technical information, will assist critical infrastructure owners and operators to develop and implement necessary protective measures to address existing and emerging threats and vulnerabilities.

Further, the Electric Trade Associations welcome NIST's development of a broad, cross-sector Baseline Framework to reduce cybersecurity risk to critical infrastructure.[4] An appropriately structured framework will provide the potential for meaningful improvement in national security, as common procedures and processes are implemented across sectors. Our members are fully committed to assisting in developing the Framework and participating in ensuing refinements.

In support of these comments, we provide the following brief descriptions of each of the Electric Trade Associations:

APPA is the national service organization representing the interests of not-for-profit, publicly owned electric utilities throughout the United States. More than 2,000 public power utilities provide over 15 percent of all kilowatt-hour sales of electricity to ultimate customers, and do business in every state except Hawaii.

LPPC represents 26 of the largest state and municipal-owned utilities in the nation. Together, LPPC's members represent 90 percent of the transmission investment owned by non-federal public power entities.

[4] EO at section 7.

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 approximately 67 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.

TAPS is an association of transmission-dependent utilities ("TDUs") in more than 35 states, promoting open and non-discriminatory transmission access. As TDUs, TAPS members are users of the bulk power system, highly reliant on the reliability of facilities owned and operated by others for the transmission service required to meet TAPS members' loads.

Notices and communications regarding these comments may be addressed to:

AMERICAN PUBLIC POWER ASSOCIATION
Allen Mosher
Vice President of Policy Analysis
and Reliability Standards
1875 Connecticut Ave. NW, Suite 1200
Washington, DC 20009
(202) 467-2944
amosher@publicpower.org

Nathan Mitchell
Director, Electric Reliability Standards and Compliance
1875 Connecticut Ave. NW, Suite 1200
Washington, DC 20009
(202) 467-2925
nmitchell@publicpower.org

LARGE PUBLIC POWER COUNCIL
Jonathan D. Schneider
Jonathan P. Trotta
STINSON MORRISON HECKER LLP
1775 Pennsylvania Ave. NW, Suite 800
Washington, DC 20006-4605
(202) 728-3034
jschneider@stinson.com
jtrotta@stinson.com

Counsel for Large Public Power Council

NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION
Laura Marshall Schepis
Senior Director, Legislative Affairs
(703) 907-5829

TRANSMISSION ACCESS POLICY STUDY GROUP
John Twitty
Executive Director
TAPS

laura.marshallschepis@nreca.coop

Barry R. Lawson
Associate Director, Power Delivery & Reliability
(703) 907-5781
barry.lawson@nreca.coop
4301 Wilson Boulevard
Mailcode GR11-253
Arlington, VA 22203

4203 E. Woodland St.
Springfield, MO 65809
(417) 838-8576
835consulting@gmail.com

Cynthia S. Bogorad
Rebecca J. Baldwin
SPIEGEL & MCDIARMID LLP
1333 New Hampshire Ave., NW
Washington, DC 20036
(202) 879-4000
cynthia.bogorad@spiegelmcd.com
rebecca.baldwin@spiegelmcd.com

The Electric Trade Associations provide the following general comments on the Framework, and answers to certain specific RFI questions below. We have also encouraged our members to respond individually to the RFI, to the extent they have facts and circumstances that are essential for NIST's consideration.

I. GENERAL COMMENTS ON THE FRAMEWORK

A. The Framework Should Encompass, and Not Conflict With, Existing Critical Infrastructure Protection ("CIP") Standards Promulgated by Independent Regulatory Agencies.

As electric utilities which own or operate facilities that are part of the Bulk Electric System and subject to Section 215 of the Federal Power Act ("FPA"), 16 U.S.C. 824o, many of the Electric Trade Associations' members are subject to applicable reliability standards developed by the North American Electric Reliability Corporation ("NERC") and approved by the Federal Energy Regulatory Commission ("FERC"). These NERC Critical Infrastructure Protection ("NERC CIP" or "Cyber") standards were developed through an exhaustive industry consensus-based standards development process accredited by the American National Standards Institute ("ANSI").

The Electric Trade Associations see significant value in the NIST RFI proposal to develop and publish a cross-sector Cybersecurity Framework to establish a voluntary baseline for cyber risk mitigation across all critical infrastructure sectors, but strongly counsel NIST to recognize the breadth and depth of NERC's existing CIP standards, and ensure that the NIST Framework steers clear of conflict or duplication, either of which would lead to confusion and compromise security and reliability.

Unlike the cybersecurity program described in the EO that may be developed pursuant to a final NIST Cybersecurity Framework, NERC CIP reliability standards impose mandatory and enforceable requirements on owners and operators of the Bulk Electric System, as set forth in the applicability sections of these standards. Compliance with NERC CIP standards is enforceable by NERC, subject to FERC oversight and approval. Enforcement actions may entail the

imposition of financial penalties of up to one million dollars per violation per day, as well as NERC remedial action directives to ensure immediate changes to cybersecurity practices and procedures.

The NERC CIP standards are prescriptive and comprehensive, covering both cybersecurity and the physical security of cyber systems that are used to control the Bulk Electric System. Currently effective Version 3 of the NERC CIP standards are grouped as follows:

- CIP-002-3 – Critical Cyber Asset Identification
- CIP-003-3 – Security Management Controls
- CIP-004-3 – Personnel & Training
- CIP-005-3 – Electronic Security Perimeters
- CIP-006-3 – Physical Security of Critical Cyber Assets
- CIP-007-3 – Systems Security Management
- CIP-008-3 – Incident Reporting and Response Planning
- CIP-009-3 – Recovery Plans for Critical Cyber Assets

Version 4 of the NERC CIP standards, scheduled to become mandatory and enforceable on April 1, 2014, retains the specific security controls developed and approved as Version 3, while imposing specific "bright line" criteria for the identification of Critical Bulk Electric System Assets to which these security controls apply.

Version 5 of the NERC CIP standards, filed with FERC on January 31, 2013, will supersede Version 4 once and as approved by FERC. As NERC explains in its response to the RFI, proposed Version 5 of the CIP Standards reflects existing NIST guidelines (SP800-53)[5] by scaling the level of needed security controls to identified risks and in providing for ongoing monitoring, assessments and corrections of controls. Version 5 of the NERC CIP standards also proposes to add two standards to the NERC CIP family, fashioned from pre-existing requirements:

- CIP-010-1 – Configuration Change Management and Vulnerability Assessments
- CIP-011-1 – Information Protection

The Electric Trade Associations are encouraged that the EO expressly states that the NIST Framework "shall incorporate voluntary consensus standards and industry best practices to

[5] NIST Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, updated May 1, 2010, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

the fullest extent possible."[6] Further, the RFI states that "[t]he Framework would be designed to be compatible with existing regulatory authorities and regulations."[7]

The potential for conflict or duplication would certainly be minimized if, as recommended here, the Framework embodies recommendations for the development and implementation of goals and processes, and steers away from prescribing specific methodologies and technologies. As well, a specific statement indicating that the recommendations embodied in the Framework are not intended to conflict with existing law, regulatory authorities or regulations would provide a clear signal that no conflict is intended.

B. The Framework Should Focus on Developing Broad, Cross-Sector Goals and Processes, Focused on A Risk-Based Approach, While Remaining Flexible and Technologically Neutral.

The Electric Trade Associations recommend that NIST develop the Cybersecurity Framework as a set of principles establishing goals and processes for critical infrastructure, and steer away from prescribing specific methodologies or technologies. Further, the Electric Trade Associations urge NIST to structure the Framework such that it provides a flexible path for organizations to improve their security protocols, and not a set of rules for which a passing or failing grade is assessed. A flexible, process-oriented approach to the Framework is counseled first by the constantly evolving nature of cyber threats and vulnerabilities. An overly prescriptive approach would result in guidelines destined to be outdated in short order, as the nature of threats and vulnerabilities evolve. Further, because the Framework is intended to apply to a large number of highly diverse critical infrastructure sectors, each of which is faced with varied challenges, vulnerabilities and consequences, a detailed model would be difficult to develop and inevitably confusing to apply.

As a frame of reference for a sensible approach, the Electric Trade Associations commend to NIST's attention the Department of Energy's ("DOE") Electricity Subsector Cybersecurity Capability Maturity Model ("ES-C2M2"),[8] and its companion Risk Management Process ("RMP") guideline.[9] The ES-C2M2 Model establishes ten core "domains," or areas of competence, each providing a contribution to a secure environment. The domains are broad and appeal to common sense, comprising: (1) Risk Management; (2) Asset, Change, and Configuration Management; (3) Identity and Access Management; (4) Threat and Vulnerability Management; (5) Situational Awareness; (6) Information Sharing and Communications; (7) Event and Incident Response, Continuity of Operations; (8) Supply Chain and External

[6] EO, Section 7.

[7] NIST RFI at 13025.

[8] DOE, Electricity Subsector Cybersecurity Capability Maturity Model, ES-C2M2, Version 1.0 (May 31, 2012), available here: http://energy.gov/oe/downloads/electricity-subsector-cybersecurity-capability-maturity-model-may-2012.

[9] DOE, Electricity Subsector Cybersecurity Risk Management Process Guideline, DOE/OE-0003 (May 2012), available here: http://energy.gov/oe/downloads/cybersecurity-risk-management-process-rmp-guideline-final-may-2012.

Dependencies Management; (9) Workforce Management; and (10) Cybersecurity Program Management. For each, the model calls for the evaluation of responsible entities based on the maturity of the resources allocated to the different domains, evaluated on a four-tiered basis, with level 0 reflecting no resources allocated to that domain; level 1 reflecting the initiation of useful practices; level 2 reflecting a degree of performance including program documentation, stakeholder involvement, resource commitment and reliance on standards or guidelines; and level 3 reflects a fully managed program, exhibiting organized governance, periodic review, lines of responsibility and authority, and a determination that involved personnel are fully competent. The allocation of resources is based on the risk evaluation conducted by the utility. Not all domains require equal allocation of resources. Resources need to be allocated in proportion to the risk. The ES-C2M2 framework gives the utility flexibility to evaluate its risk and allocate resources based on this risk informed evaluation.

Similarly, DOE's RMP provides a valuable organizational tool for the management of cyber risks, addressing Organization (Tier 1), Business Processes (Tier 2) and the selection, procurement and monitoring of cybersecurity safeguards and countermeasures addressed to information technology and control systems (Tier 3). As with the Maturity Model, the RMP provides space for organizations to evaluate risks, and scale their programs to provide an appropriate response.

The combination of the ES-C2M2 Model and the RMP are comprehensive and substantive, without being so prescriptive that they ignore the evolving nature of cyber threats and vulnerabilities, or create inadvertent barriers to needed technological innovation and widespread adoption of improved practices. Equally important, these tools enable responsible entities to scale protective measures to their size and scale of assets and operations, and to the nature of cyber risks as the threat and vulnerability landscape evolves over time. The Electric Trade Associations encourage NIST to incorporate similar features into the Framework.

II. THE ELECTRIC TRADE ASSOCIATIONS' RESPONSES TO NIST RFI QUESTIONS

A. NIST RFI Section 1: Current Risk Management Practices.

- **<u>Question 1:</u> What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?**

The Electric Trade Associations believe the most immediate need is for the provision of timely, actionable information regarding existing and emerging threats and vulnerabilities, and sound input regarding appropriate responses. Due to the critical nature of the service it provides, the electric utility sector has been on the front line of emerging cybersecurity threats. Utilities recognize the need for, and the benefits that can be gained from, a clearinghouse for timely information about threats, vulnerabilities and responses. This type of clearinghouse has been developed within the utility subsector, but needs to be expanded to include other business sectors and, most importantly, the federal government and its intelligence services. Accordingly, the Electric Trade Associations place high on the list of challenges the need for information sharing between the federal government, intelligence community and the private sector, and the timely

dissemination of actionable information on emerging threats and vulnerabilities as well as responses. This information includes the granting of additional, and in some cases higher-level, security clearances for electric utility representatives.

As a model for this framework, the Electric Trade Associations point to NERC's Electricity Sector - Information Sharing and Analysis Center ("ES-ISAC"). We have found this program to be a valuable source of reliable information often not available elsewhere. The ES-ISAC has also substantially improved the efficacy of its communications infrastructure and made major strides to reach a greater number of large and small entities across the electricity subsector. However, much more can be done to improve the content of the information provided by the subsector's federal partners to the ES-ISAC and to begin more effective informational exchange across critical infrastructure sectors. The effectiveness of the process can be improved as more actionable intelligence is shared by federal agencies with the electricity sector, particularly when such information can be redacted on a timely basis to allow classification of such information as non-public, For Official Use Only ("FOUO"). Only then will private sector entities be able to leverage knowledge into effective risk-based cybersecurity practices.

The Electric Trade Associations also note that provisions of various state statutes and regulatory agency rules often do not shield cybersecurity information from disclosure requirements under public records/government in the sunshine laws. This concern is particularly problematic for state and publicly owned electric utilities. Beyond that, the waiver provision of the Freedom of Information Act poses problems for federal agencies and entities.

- **Question 2: What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?**

As discussed in the Electric Trade Associations' general comments above, a cross-sector framework must be sufficiently flexible to enable varied organizations to be agile in responding to ever-evolving threats and vulnerabilities, and a wide range of risks. The Framework must be flexible, goals-based and process oriented, and it must avoid overly prescriptive approaches or technologies that risk becoming antiquated, and are not scalable to a realistic evaluation of risk. Too rigid a Framework would risk establishing perverse incentives to develop and stick with programs and practices that fail to respond appropriately to evolving risks.

- **Question 3 – *N/A***

- **Question 4 – *N/A***

- **Question 5: How do organizations define and assess risk generally and cybersecurity risk specifically?**

For electric utilities, risk is generally defined as a function of the likelihood that the reliable real-time delivery of electric power will be disrupted, particularly if such disruptions occur on a wide-area basis or result in damage to equipment that may cause outages for an

extended period of time. Reflecting this basic concept, DOE's RMP guideline – developed in conjunction with NIST, NERC and the electric subsector – defines "Cybersecurity Risk" as:

> [t]he risk to organizational operations (including mission, functions, image, reputation), resources, and other organizations due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or [information technology] and [industrial control systems].[10]

- **Question 6 – *N/A***

- **Question 7: What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?**

Electric subsector critical infrastructure owners and operators are obligated to comply with applicable mandatory NERC CIP standards. In addition, useful work has been done by DOE in outlining essential capabilities and organizational tools through the ES-C2M2 Maturity Model and the RMP, discussed in general comments above. Further, most of the electric subsector's rural electric cooperatives are subject to mandatory Electric System Emergency Restoration Plan ("ERP") regulations through the Department of Agriculture's Rural Utility Service ("USDA RUS"). In addition, NRECA's Cooperative Research Network ("CRN") is proactive in developing cybersecurity tools for electric distribution utilities. APPA has developed a "Cyber Security Essentials" guide for its members that builds upon the NERC CIP standards and the September 2011 DOE "Roadmap to Achieve Energy Delivery Systems Cybersecurity."

1. NERC CIP Standards

Electric subsector critical infrastructure owners and operators are subject to applicable mandatory NERC CIP standards, including prescriptive standards addressing both cybersecurity and physical security. The body of CIP standards was developed by NERC in a cooperative process with the electric industry, approved by FERC pursuant to FPA Section 215, and currently is mandatory and enforceable, carrying with it potential financial penalties of up to $1 million per day, per violation. The Electric Trade Associations urge NIST to be mindful of the comprehensive protections woven into the current regulatory regime, including the CIP standards, and to ensure that any Framework ultimately developed does not inadvertently undermine existing cybersecurity controls that apply to the electric subsector.

2. DOE ES-C2M2 and RMP

Discussed above, the Electric Trade Associations commend to NIST's attention DOE's ES-C2M2 Maturity Model, along with the RMP, developed by DOE in collaboration with NIST, NERC, the Department of Homeland Security ("DHS") and the electric industry. The Maturity

[10] DOE RMP guideline at 66.

Model was designed to support ongoing development and measurement of cybersecurity capabilities within the electric subsector by: (a) strengthening the subsector's cybersecurity capabilities; (b) enabling utilities to effectively and consistently evaluate and benchmark cybersecurity capabilities; (c) sharing information and best practices within the subsector as a means of improving cybersecurity capabilities; and (d) enabling electric utilities to prioritize actions and investments to improve cybersecurity. Also discussed above, the RMP provides an organizational framework for addressing risk, counseling the use of organizational and technical tools scaled to each responsible entity's evaluation of risk. Because these models do not endorse particular methodologies or technologies, they are sufficiently flexible to enable organizations to respond to evolving threats and vulnerabilities, while scaling their programs to an evaluation of risk. The models do not reflect a checklist approach to particular tools or technologies, which would ultimately be counterproductive in inhibiting the agility needed to respond to an always changing environment.

3. USDA RUS ERP Regulations and NRECA CRN Cyber Security Tools

Beginning in October 2004, the USDA RUS ERP regulations (7 CFR Part 1730) required each electric cooperative borrower to perform a vulnerability and risk assessment and to develop emergency recovery plans regarding physical and cyber incidents.[11] In addition, cooperative borrowers are also required to annually exercise their ERP.

NRECA's CRN has been proactive in developing cybersecurity tools targeting distribution utilities, which typically are not subject to NERC standards compliance because their operations do not impact the bulk electric system. These tools are beneficial to utilities of all sizes. Electric cooperatives are at the forefront of smart grid deployment and therefore are very much aware of the need to comprehensively address the security of any new telecommunications-enabled devices.

As part of its fulfillment of a $68 million smart grid demonstration program under the American Reinvestment and Recovery Act, CRN developed cybersecurity plans for 23 participating electric cooperatives. That effort led to the development of a tool that compiles thousands of pages of industry and government guidance on cybersecurity into a digestible, deployable plan. This plan is publicly available, and anecdotal evidence indicates it is in use at many utilities, including some that are outside the cooperative network.[12] CRN now leads training sessions on the plan and cybersecurity best practices, which are open to all segments of the electric industry.

- **<u>Question 8:</u> What are the current regulatory and regulatory reporting requirements in the United States (e.g. local, state, national, and other) for organizations relating to cybersecurity?**

[11] http://www.gpo.gov/fdsys/pkg/FR-2011-08-04/pdf/2011-19661.pdf

[12] The NRECA CRN Cybersecurity Plan is available here: http://www.nreca.coop/bestbets/cybersecurity.

FPA section 215 provided for FERC's certification in 2006 of NERC as the nation's Electric Reliability Organization ("ERO"). FPA section 215 further requires users, owners and operators of the bulk power system within the U.S. to comply with mandatory and enforceable reliability standards developed by NERC and approved by FERC, including the body of CIP standards which, as noted above, prescribe a core set of mandatory baseline protocols for protection of critical cyber and physical assets. As part of this reliability framework, NERC has legal authority to monitor and enforce compliance with FERC-approved reliability standards, and to assess penalties and sanctions. In addition, FERC maintains independent authority under the statute to monitor and enforce the reliability standards.

- **Question 9: What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?**

The electric subsector shares certain interdependencies with cyber assets in the communications, information technology, and transportation sectors. Among other things, critical assets in the electric subsector that are potentially interdependent on the communications and transportation sectors include industrial control systems, energy marketing and management systems, as well as generation, transmission and distribution systems. However, to a substantial degree, electric utilities own and/or operate independent, dedicated communications networks, which may justify a different type of protection (no need for encryption, e.g.) than would otherwise be applicable to common carrier networks. Specific electric subsector entities have close interdependencies with the dam, water and waste water sectors.

- **Question 10: What performance goals do organizations adopt to ensure their ability to provide essential services while managing cybersecurity risk?**

NERC's CIP Standards provide certain Key Performance Indicators measuring the efficacy of cybersecurity practices, while audits of NERC's CIP standards require evidence of performance to demonstrate compliance. As well, NERC's Emergency Operations Planning ("EOP") reliability standards address operational resilience and restoration in the electric subsector through requirements for, among other things, backup and recovery of energy systems. The Electric Trade Associations' members to which these standards apply must be fully compliant.

- **Question 11: If your organization is required to report to more than one regulatory body, what information does your organization report and what has been your organization's reporting experience?**

The Electric Trade Associations' members must comply with applicable NERC standards. These standards have embedded within them various reporting requirements with regard to disturbances or unusual occurrences, suspected or determined to be caused by sabotage

(*i.e.*, CIP-001-2), as well as cybersecurity incidents related to critical cyber assets (*i.e.*, CIP-008-3).

Specifically, CIP-001-2 calls on organizations subject to the standard to report to relevant government and regulatory bodies disturbances or unusual occurrences that are suspected or determined to be caused by sabotage. The standard, too, requires those entities to establish communications contacts with local Federal Bureau of Investigation officials, and to develop reporting procedures.

In addition, NERC standard CIP-008-3 prescribes requirements for identification, classification, response and reporting of cybersecurity incidents related to critical cyber assets. Among other things, the standard requires entities subject to the standard to develop, maintain and implement a cybersecurity incident response plan, which includes processes and procedures for classifying events as reportable cybersecurity incidents, reporting such incidents to the ES-ISAC, and retaining documents relevant to any such reportable incidents.

NERC Standard EOP-004-1, Disturbance Reporting, requires applicable entities to report cyber and physical attack on their systems. Failure to report within 24 hours of an incident may be determined a violation of the standard and subject an entity to financial penalties.

Cyber and physical attack and outage reporting is further required under Form DOE-OE-417[13] for incidents including actual physical attacks, actual cyber-attack, complete operational failure, or electrical system separation. Timely reporting of this outage data is already mandatory under Section 13(b) of the Federal Energy Administration Act of 1974. There are civil and criminal penalties for violation of that Act. In addition, electric emergency incidents and disturbances must be reported under Form EIA-417.[14] Data submitted through EIA-417 is used by DOE to gather current information regarding emergency situations on electric energy supply systems.

Finally, the Nuclear Regulatory Commission ("NRC") has in place cybersecurity regulations which require existing nuclear power reactor licensees, and those corporations applying for new reactor licenses, to submit a new cybersecurity plan and an implementation timeline for NRC approval. Those cybersecurity plans must demonstrate how the facility has or would identify critical digital assets, and describe its protective strategy, among other requirements.[15] In a January 2010 Regulatory Guide, NRC provided guidance to the nuclear industry on acceptable ways to meet these cybersecurity requirements, in addition to recommended best practices from NIST, the International Society of Automation, and the Institute of Electrical and Electronics Engineers, as well as guidance from DHS.[16]

---

[13] Form DOE-OE-417 is available here: http://www.oe.netl.doe.gov/oe417.aspx.

[14] Form EIA-417 is available here: ftp://ftp.eia.doe.gov/pub/pdf/electricity/insteia417.pdf.

[15] 10 C.F.R. § 73.54.

[16] *See* DHS Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities (Jan. 2010), available here: http://pbadupws.nrc.gov/docs/ML0903/ML090340159.pdf.

- **Question 12: What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?**

In the electric subsector, NERC currently plays a key role in overseeing and enforcing industry compliance with CIP standards through well-established processes and procedures rooted in FPA Section 215. These standards apply internationally in Canada and in a portion of northern Mexico. In addition, NERC and the electric subsector actively develop and refine mandatory cybersecurity standards aimed at threat and vulnerability identification, and protection of key physical and cyber assets. As NERC points out in its comments, the CIP standards create a baseline for stakeholders to adopt security best practices and resources into their organizations, while remaining sufficiently flexible to account for the dynamic nature of technology and emerging threats and vulnerabilities. NERC and the ES-ISAC facilitate this process by providing tools and information to industry which are essential to the electric subsector's ability to effectively assess new threats and vulnerabilities.

The Electric Trade Associations endorse NERC's work in this area and urge NIST, in developing the Framework, to draw on NERC's substantial technical expertise and knowledge of critical infrastructure cybersecurity assessment, monitoring, standards development, and oversight.

B. NIST RFI Section 2: Use of Frameworks, Standards, Guidelines and Best Practices.

- **Question 1: What additional approaches already exist?**

As NIST moves forward to develop a uniform cyber Framework, the Electric Trade Associations' members see much value in five existing approaches in the electric subsector: (1) the NERC CIP standards; (2) DOE's ES-C2M2 Maturity Model; (3) DOE's RMP guideline; (4) NERC and regional Critical Infrastructure Protection Committees ("CIPC"); and the (5) the ES-ISAC alert process.

Discussed above, the CIP standards focus on cybersecurity and physical security of cyber assets. The DOE ES-C2M2 model, developed in collaboration with NIST, NERC, DHS and the electric industry, is designed to support ongoing development and measurement of cybersecurity capabilities within the electric subsector, while the companion DOE RMP guideline is intended to provide a viable risk management process that is tailored to the needs of electric subsector organizations. The Electric Trade Associations' members endorse these three approaches.

The existing NERC and regional CIPC groups provide valuable industry input to the development of guidelines and best practices. These groups will provide the needed resources in the form of subject matter expertise.

The ES-ISAC provides real-time threat information to the electric subsector.

NERC has also developed and implemented a "NERC Alert System" that categorizes risks to the bulk electric system based on severity. Cybersecurity risks are within the scope of the NERC Alert System. NERC's NIST RFI comments in response to Question 8 on Specific Industry Practices is excerpted below:

> The Electricity Sub-sector broadly implemented and continues to maintain threat response level plans based on the NERC model initially released in 2002. Cyber-specific guidance in the model included progressive threat level action planning. Further formalization of cyber incident handling continues with NERC CIP standards, which includes required reporting for more significant compliance matters to the ES-ISAC along with voluntary non-compliance reporting. The NERC Alert System addressing such matters has been implemented and formalized across the industry for registered entities. As defined by NERC Rules of Procedure, alerts are divided into three distinct levels:
>
> 1. Industry Advisory - Purely informational, intended to alert registered entities to issues or potential problems. A response to NERC is not necessary.
> 2. Recommendation to Industry - Recommend specific action be taken by registered entities. Require a response from recipients as defined in the alert.
> 3. Essential Action - Identify actions deemed to be "essential" to bulk power system reliability. Requires NERC Board of Trustees approval prior to issuance. Similar to recommendations, essential actions also require recipients to respond as defined in the alert.
>
> Each alert contains specific information including:
>
> - List of Electricity Sub-sector functional entities the alert was distributed to
> - Reporting requirements and details (if applicable)
> - A set of "primary interest groups" within the receiving organization who may benefit most from the alert
> - Background information for the genesis of the alert (generally a description of a disturbance event or particular information about a cyber or physical vulnerability)
> - Specific, actionable observations, recommendations, or essential actions
> - Contact information for the appropriate NERC staff
> - Label indicating the sensitivity of the information contained in the alert

- **<u>Question 3:</u> Which organizations use these approaches?**

Under FPA Section 215, FERC (and thus NERC) has jurisdiction over "users, owners, and operators" of the bulk power system. The NERC CIP standards, and indeed the entire body of NERC reliability standards, apply to the functional entities set out in the applicability section

of each standard, excluding those entities that do not have a material impact on the reliability of the bulk power grid, as defined in the NERC Statement of Compliance Registry Criteria.[17]

Both the DOE ES-C2M2 and companion RMP guidelines are electric subsector-wide documents that list core capabilities, and outline organizational tools for assessing and managing cyber risks.

All electric subsector entities are eligible to participate in the ES-ISAC. The NERC Alert program applies formally to NERC registered entities.

- **Question 4: What, if any, are the limitations of using such approaches?**

Each of the above-described approaches establishes foundational practices for cybersecurity. However, due to the number of frameworks and guidelines that have been developed to address a multitude of needs, conflicts emerge regarding controls and a varying degree of requirements that vastly complicate wholesale adoption of guidelines. At times, no universal set of conformity assessment practices exist which would allow for a repeatable, objective review of effectiveness. Often, the use of guidance must be tempered to mitigate conflict, particularly in those sectors subject to mandatory, enforceable cybersecurity standards such as the electric subsector. Further, the continually-evolving nature of cybersecurity threats and vulnerabilities – which typically occur at a much faster rate than development of standards and guidance – make it essential that the appropriate level of actionable threat and vulnerability information is available to critical infrastructure owners and operators, to ensure that selected practices and controls are meeting the objective of reducing risk. In addition, timely access to actionable threat and vulnerability information will go far to ensure organizations are more agile both in their ability to respond to emerging threats, and to adjust their control selections ahead of formal guidance.

- **Question 5: What, if any, modifications could make these approaches more useful?**

As noted, Bulk Electric System owners, operators and users participate in NERC's ES-ISAC alert system. This program may be substantially enhanced when, as directed by the EO, federal agencies coordinate the release of timely information possessed by the government regarding existing and emerging threats. The ES-ISAC program invites participation by all electric sector organizations.

- **Question 6: How do these approaches take into account sector-specific needs?**

Both the NERC CIP standards and the DOE ES-C2M2 Model were developed with the specific needs and requirements of the electric subsector in mind. The NERC standards are developed using an ANSI-accredited standards development process, the core of which is a

[17] *See* NERC Rules of Procedure, Appendix 5B, Statement of Compliance Registry Criteria, available here: http://www.nerc.com/files/Appendix_5B_RegistrationCriteria_20130305.pdf ,

consensus-based approach to standards development which draws on the technical expertise and experience of the electric industry stakeholders. The CIPC and the ES-ISAC are limited to the electricity sector only.

- **Question 7: When using an existing framework, should there be a related sector-specific standards development process or voluntary program?**

The Electric Trade Associations note that the NERC reliability standards are mandatory. There is a role for supplemental voluntary practices, needed to respond flexibly to emerging threats and vulnerabilities, however the Electric Trade Associations caution against the creation of a second set of potentially conflicting standards and standards development processes.

- **Question 8: What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?**

Sector-Specific Agencies ("SSAs") and related Sector Coordinating Councils play a critical role in this effort through clear, effective outreach and communication with industry regarding current and emerging threats and vulnerabilities. Both SSAs and the Coordinating Councils are closely aligned with the operations of their respective sectors and, therefore, are uniquely positioned to work with industry to develop case studies regarding Framework adoption and implementation, which will go far to promote uniformity within those sectors. SSAs and Sector Coordinating Councils, too, intimately understand the uniqueness of their sectors and can assist to develop risk-based measures to ensure adoption of the Framework is commensurate with risk and operations of sector organization.

SSAs and Sector Coordinating Councils should work closely to support the ISACs, and should prioritize improvement of timely, actionable threat information sharing; define roles and responsibilities of sector organizations; provide resources and support for cross-sector information sharing through the ISACs; and engage with industry to encourage sector threat and response analysis.

Question 9: What other outreach efforts would be helpful?

As noted by NERC in its RFI comments, additional outreach efforts by the SSA, Government Coordinating Council and Sector Coordinating Council for each sector is essential. Specifically, these groups should be involved in developing and sponsoring a collaborative, comprehensive outreach effort, which informs sector stakeholders on key structures, policies, priorities and approaches employed within that sector. SSAs, too, should ensure that proper resources are devoted to sector priorities, and be sure to disseminate and publish as much outreach content as possible. The Electric Trade Associations offer to disseminate any outreach materials to our members through our existing communication channels.

C. NIST RFI Section 3: Specific Industry Practices.

As a general matter, the Electric Trade Associations' members note that the nine industry practices identified by NIST[18] are widely used throughout the electric subsector, and are reflected within the body of NERC's currently-effective CIP standards, CIP-002 through CIP-009. In this regard, the Electric Trade Associations endorse NERC's position that these CIP standards outline specific actions to be undertaken by asset owners and operators to protect critical cyber assets necessary for electric system reliability.

The Electric Trade Associations agree with NERC that a key implementation challenge faced by the electric subsector is ensuring that entities adequately secure their operational systems (*e.g.*, control systems, SCADA, etc.) from potential threats and vulnerabilities introduced by an increased reliance on interoperable operating systems and networks without compromising the efficiencies and reliability benefits offered by those systems.

III. CONCLUSION

The Electric Trade Associations support the work NIST has undertaken to develop a Cybersecurity Framework consistent the EO, and asks that these comments be reflected in the shape of that Framework.

Respectfully Submitted,

AMERICAN PUBLIC POWER ASSOCIATION

/S/
Allen Mosher
Vice President of Policy Analysis
and Reliability Standards
Nathan Mitchell
Director, Electric Reliability Standards and Compliance
1875 Connecticut Ave. NW, Suite 1200
Washington, DC 20009
(202) 467-2944

LARGE PUBLIC POWER COUNCIL

/S/
Jonathan D. Schneider
Jonathan P. Trotta
STINSON MORRISON HECKER LLP
1775 Pennsylvania Ave. NW, Suite 800
Washington, DC 20006-4605
(202) 728-3034
jschneider@stinson.com
jtrotta@stinson.com

Counsel for Large Public Power Council

[18] The nine specific industry practices identified by NIST in the RFI are these: (1) separation of business from operational systems; (2) use of encryption and key management; (3) identification and authorization of users accessing systems; (4) asset identification and management; (5) monitoring and incident detection tools and capabilities; (6) incident handling policies and procedures; (7) mission/system resiliency practices; (8) security engineering practices; and (9) privacy and civil liberties protection. *See* NIST RFI at 13,027–28.

amosher@publicpower.org
nmitchell@publicpower.org

NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION

/S/

Laura Marshall Schepis
Senior Director, Legislative Affairs
(703) 907-5829
laura.marshallschepis@nreca.coop

Barry R. Lawson
Associate Director, Power Delivery & Reliability
(703) 907-5781
barry.lawson@nreca.coop
4301 Wilson Boulevard
Mailcode GR11-253
Arlington, VA 22203

TRANSMISSION ACCESS POLICY STUDY GROUP

/S/

Cynthia S. Bogorad
Rebecca J. Baldwin
SPIEGEL & MCDIARMID LLP
1333 New Hampshire Ave., NW
Washington, DC 20036
(202) 879-4000
cynthia.bogorad@spiegelmcd.com
rebecca.baldwin@spiegelmcd.com