701 Pennsylvania Avenue, N.W. | Washington, D.C. 20004-2696 | www.eei.org
202.508.5615 | Fax: 202.508.5673 | Mobile: 202.258.2909 | ecomer@eei.org

Power by Association℠

Edward H. Comer
Vice President, General Counsel & Corporate Secretary

April 8, 2013

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

RE: Request for Information: Developing a Framework to Improve Critical Infrastructure Cybersecurity

Dear Ms. Honeycutt:

On behalf of our members, the Edison Electric Institute (EEI) is pleased to submit the attached comments responding to the Request for Information (RFI) that the National Institute of Standards and Technology (NIST) published in the Federal Register on Tuesday, February 26, 2013.

Our sector has a long history of providing safe, adequate, low-cost and reliable electric service. The sector achieves this service through investments to assure the security and resilience of our electric system, including mutual assistance and cooperation. Electric companies work to maintain the reliability and the security of the computers, control systems, and other cyber assets that help electric companies operate the electric grid. The sector employs threat mitigation actions focused on preparation, prevention, response, and recovery in its operations.

As a result of passage of the Energy Policy Act of 2005, the electricity sub-sector in the United States is subject to mandatory, enforceable, cybersecurity standards developed and enforced by the North American Electric Reliability Corporation (NERC), under the jurisdiction of the Federal Energy Regulatory Commission ("FERC"). Considerable resources and much time have been dedicated to the drafting and implementation of these cybersecurity standards. NERC standard development relies heavily on the technical expertise of industry experts to ensure that these mandatory cybersecurity standards are technically and operationally sound, fully responsive to FERC regulatory directives, and do not result in unintended consequences for the reliable operation of the bulk power system.

EEI encourages NIST to develop a Cybersecurity Framework that provides a high-level and flexible tool for critical infrastructure to ensure that the Cybersecurity Framework can be adapted to the Nation's diverse critical infrastructure sectors, without unintended consequences. The Framework should focus on cost-effective risk management and leverage each sector's existing processes, standards and guidance. The Framework development process should not try to develop new cybersecurity standards impacting the electric industry because new standards will likely overlap and duplicate the existing approaches already in use by the electricity and other sectors. The Framework and its implementation should also leverage existing public-private cybersecurity partnerships because improving cybersecurity

requires coordinated efforts among electric companies, the federal government, and the suppliers of critical electric grid systems and components.

EEI looks forward to participating and supporting the NIST Cybersecurity Framework development process. Please contact Mr. David Batz at 202 508 5064, dbatz@eei.org, if you have any follow-up questions about our comments.

Sincerely,

Edward H. Comer
Vice President & General Counsel

Comments of the Edison Electric Institute

On the NIST RFI
Developing a Framework to Improve Critical Infrastructure Cybersecurity
April 8, 2013

The Edison Electric Institute (EEI) is the trade association of U.S. shareholder-owned electric companies. EEI's U.S. members serve more than 98% of the ultimate customers of electricity in the shareholder-owned segment of the industry and represent about 70% of the U.S. electric power industry. EEI is part of a broad coalition of electric power stakeholders focused on cybersecurity. This cybersecurity coalition includes several major trade associations representing the full range of electric generation, transmission and distribution companies in the United States, as well as regulators, Canadian interests and large industrial customers.[1]

Protecting the nation's electric grid and ensuring a safe and reliable supply of power is the electric utility industry's top priority. Thus, our industry takes cyber security threats very seriously. EEI shares the goals of Executive Order 13636 to enhance the protection and resilience of the Nation's critical infrastructure through public-private partnerships. We welcome the opportunity to comment on the NIST Cybersecurity Framework.

The power grid is a complex infrastructure made up of networked generation, transmission, distribution, control, and communication technologies, which can be damaged by natural events such as severe storms as well as malicious events such as a cyber attack. Cybersecurity is not new to the electricity sub-sector—it has been a growing priority over the past decade. The sector employs threat mitigation actions focused on preparation, prevention, resiliency, response, and recovery in its operations. As threats to the grid continue to grow more sophisticated, the sector continues to strengthen its defenses.

As a result of passage of the Energy Policy Act of 2005, the electricity sub-sector has been subject to mandatory, enforceable, cybersecurity standards under the jurisdiction of FERC. The standards drafting process, which is conducted by the North American Electric Reliability Corporation (NERC), relies heavily on the technical expertise of industry experts working in conjunction with federal regulators to ensure that cybersecurity standards are technically and operationally sound and do not result in unintended consequences. Considerable resources and much time have been dedicated to the drafting and implementation of these cybersecurity standards.

Owners and operators of nuclear energy facilities are also subject to extensive regulation by the Nuclear Regulatory Commission (NRC) to ensure cyber protection. The nuclear energy industry implemented a cybersecurity program in 2002 to protect critical digital assets. In 2009, the NRC built upon this program by establishing cybersecurity regulations for U.S. nuclear reactors. A memorandum of understanding and policy statement by the NRC ensure that there is good coordination between NERC and the NRC, so that no gaps in protection exist for nuclear generators.

EEI, our members and others in the electric industry also work with government partners in a variety of voluntary contexts to protect against cyber threats. Through these efforts, we have learned that standards

[1] EEI is also joining this coalition in filing brief comments to the NIST RFI.

enforce good business practices and encourage a baseline level of security, but standards alone are not sufficient because the cybersecurity threat environment is constantly changing and threats and our nation's adversaries evolve rapidly.

Imminent cyber threats require quick action and flexibility. Timely dissemination of threat information and analysis must play an important role in informing protective actions. Therefore, EEI strongly supports the provisions of the Executive Order furthering timely information sharing about cyber threats among the government and owners and operators of critical infrastructure.

Close collaboration between government and industry is needed to truly mitigate cyber risk**.** Just as our industry does not have intelligence gathering capabilities, the government does not have the expertise to operate an electric utility system. Close collaboration with the government is also needed to practice emergency response protocols before a disaster strikes. Both industry and government have roles to play, which require a close working relationship. Our efforts will be vastly improved with better information sharing ability and a clearer understanding of roles among various government agencies, which the Executive Order seeks to achieve.

EEI also agrees with the Executive Order that a Cybersecurity Framework "shall provide a prioritized, flexible, repeatable, and performance-based, and cost-effective approach."[2] To that end, we believe that the framework must:

1. Be high-level and flexible, to ensure that the Cybersecurity Framework can be adapted to the Nation's diverse critical infrastructure sectors, without unintended consequences;
2. Build upon each sector's existing processes, standards and guidance, including sector-specific regulatory standards which already exist in the electric and nuclear industries;[3]
3. Avoid time-consuming and unnecessary duplication of efforts;[4]
4. Preserve and build upon existing public-private partnerships;[5] and
5. Be risk-based and cost-effective.

EEI Responses to NIST RFI Questions

I Current Risk Management Practices

1. What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?

Our greatest challenge is obtaining timely, actionable and currently unavailable cyber threat information. Since the cybersecurity threat environment is constantly changing, the ongoing

---

[2] Section 7(b) of the Executive Order.

[3] This is consistent with Section 7(a) of the Executive Order, which directs that the Framework "incorporate voluntary consensus standards and industry best practices to the fullest extent possible."

[4] This is consistent with Section 10(c) of the Executive Order, which requires agencies to report on duplicative, conflicting or excessively burdensome cybersecurity requirements.

[5] See generally Section 8 of the Executive Order.

dissemination of vulnerability and threat information and analysis is needed to inform protective actions. The federal government has considerable knowledge of these cyber threats while electric companies understand the operations of power systems. We need better mechanisms for the government and industry to provide for ongoing consultation, cooperation and the sharing of information with each other to alert companies to potential threats and provide guidance on mitigation of these threats. Such information is important to improving our risk assessment process since it will enable us to focus resources on likely risks.

Expansion of the Enhanced Cybersecurity Services program to the electricity sub-sector is one mechanism with the potential to improve information sharing between the federal government and the electricity sub-sector. Therefore, we welcome speedy implementation of Section 4 of the Executive Order that directs the government to increase the volume, timeliness and quality of cyber threat information shared with the private sector.

Supply chain security is also a challenge. The software and hardware components that make up the information and control systems used by the electricity sub-sector are manufactured by a very large number of different vendors, who often are either owned or operated internationally. New vendors and service providers, who may be less familiar with the security requirements and operating environments specific to the electricity sub-sector, are also becoming a part of the sector's supply chain. This complex and dynamic supply chain introduces the risk that flaws or malware can be inserted accidently or intentionally into electricity sub-sector information and control system components in a variety of ways.

Individual companies do not have the resources to assess the supply chain integrity of every component – from millions of lines of software code to thousands of hardware components. However, companies are working with each other, the Federal government, and vendors to reduce the supply chain risk through a number of security efforts including: adoption of secure coding practices, application and component testing, improved procurement language, use of supplier monitoring tools and best practices, and analysis of software and hardware.

2. What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical information?

One of the key lessons we have learned as we have worked to advance our own readiness is that while standards encourage good business practices and enforce a baseline level of security, standards alone are not sufficient to address cyber threats. Standards take a long time to develop and can provide a road map for our adversaries to evade security controls. It is extremely important to avoid conflicting or unnecessary standards that divert attention from the need for flexibility and creativity in the security context. The establishment of new, or worse, duplicative standards (even if voluntary) will unnecessarily divert resources and seriously hinder our ability to respond quickly and with agility to real-time cyber threats.

Given this, we believe strongly that the Framework must focus on communications, and existing guidelines and best practices rather than develop or refine detailed standards. The Framework must be flexible, risk-centric, goals-based and process-oriented and avoid an overly prescriptive approach.

3. **Describe your organization's policies and procedures governing risk generally and cybersecurity risk specifically. How does senior management communicate and oversee these policies and procedures?**
4. **Where do organizations locate their cybersecurity risk management program/office?**
5. **How do organizations define and assess risk generally and cybersecurity risk specifically?**
6. **To what extent is cybersecurity risk incorporated into organizations' overarching enterprise risks management?**
10. **What performance goals do organizations adopt to ensure their ability to provide essential services while managing cybersecurity risk?**

We are responding to these questions concurrently because we believe it is important to focus on the main principles, not implementation details. In our experience every organization in our industry operates somewhat differently, but we believe these operational differences are not particularly critical variables in and of themselves. The important thing is that protecting the nation's electric grid and ensuring a reliable supply of power is the electric power industry's top priority and assuring cybersecurity and resilience is part of achieving that priority.

Through EEI, CEOs of our members and other utility associations have personally engaged in multiple discussions of cyber issues and met with various governmental agencies to discuss cyber issues. EEI is conducting several cyber education, best practice and training initiatives as well.

Under the auspices of National Infrastructure Advisory Council (NIAC), several electric industry CEOs now are engaged in an ongoing partnership with the White House National Security Staff and senior officials throughout the government, including Department of Energy (DOE) Deputy Secretary Daniel Poneman and Department of Homeland Security (DHS) Deputy Secretary Jane Holl Lute. This collaboration has resulted in classified briefings to make senior industry executives aware of the full scope of the threats facing the electric grid, as well as a commitment from government representatives to improve the flow of information between the government and industry. Other initiatives for this government-industry partnership include addressing legal, technical, and procedural hurdles associated with the deployment of proprietary government technology on utility networks to improve real-time situational awareness, and a directive to identify roles and responsibilities that will expedite response and recovery should a major power disruption occur.

Further, DOE and DHS, in partnership with the private sector, have undertaken the *Electricity Subsector Cybersecurity Capabilities and Maturity Model* (ES–C2M2) to strengthen the industry's cyber readiness by enabling electric utilities and grid operators to assess their cybersecurity capabilities and prioritize their security investments. Beyond this, many of our members work closely with DHS and the U.S. Secret Service to prepare for events of national significance; they also work with the National Security Agency (NSA) and Department of Defense (DOD) on addressing mission-critical electric power needs "on the ground" at the base level and from the national perspective.

EEI is also coordinating voluntary action by its member companies to vigorously stay ahead of the threats to operation of critical infrastructure. Working with The Chertoff Group, EEI and its members are conducting a "Threat Scenario Project." This project represents an exhaustive effort to provide a self-assessment tool by which EEI members can thoughtfully review a wide range of threats – including, but not limited to, cyber and physical attacks – that might impact their

operations and at the same time evaluate measures to mitigate and expedite recovery from the consequences of these threats. The Threat Scenario Project is designed to explore high-consequence, low-frequency threats facing electric utility companies. The information contained in this tool is enhancing executive awareness and stimulating further consideration of preparedness, prevention, response, and recovery activities.

Another important initiative, which EEI members have undertaken to protect our critical infrastructure, is the Spare Transformer Equipment Program (STEP). This was developed in response to an industry-wide desire to cost-effectively improve reliability, particularly in the event of deliberate destruction of electrical transformers in connection with a terrorist event. STEP was designed to ensure that sufficient spare transformer capacity is available pursuant to a mandatory sharing mechanism to allow an affected participating utility to restore its system following a triggering event with spare equipment from another participating utility. And although a triggering event requiring mandatory sharing is limited to an act of terrorism, STEP provides a ready mechanism for participating utilities to voluntarily share assets in the event of other catastrophic loss. Because of the broad industry participation in STEP, this capacity is geographically dispersed, and enjoys requisite FERC and applicable state commission approval of the transfers contemplated by STEP. Further, this process is not static; pursuant to the STEP agreement at least once each year participants adjust what equipment needs to be made available through STEP based on agreed upon contingencies for a "worst case" scenario. In addition, STEP remains open to any other utility that is not already a participant.

In short, as part of the industry's overall responsibility to assure an extremely high level of reliability to our customers, electric companies work individually, collectively, with NERC and with several different federal agencies to maintain the reliability and the security of the computers, control systems and other cyber assets that help operate the electric grid. We are constantly working to strengthen and improve the security of our cyber systems and to identify and address any vulnerability.

As part of our dedication to reliability, our industry designs our critical systems for resiliency so that there are multiple pathways and options to keep customers in service in the event that any element or interrelated elements of the system are damaged.

Finally, as indicated in response to Question 1, our risk assessment processes will be improved if we can receive timely information from the government about cyber threats because knowledge of specific risks will better enable us to focus resources on such risks.

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

In addition to the NERC and NRC cybersecurity standards, which are described in comments filed by NERC, the electricity sub-sector uses:

- *Electricity Subsector Cybersecurity Risk Management Process* – a cybersecurity risk management guideline developed by DOE, NIST, NERC, and industry subject matter experts;

- NIST SP 800-30, *Guide for Conducting Risk Assessments*;

- NIST 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*; and

- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*.

- NERC Alerts, Section 810 NERC Rules of Procedure

Electric utilities also benefit from the senior-level NIAC engagement discussed earlier and a host of other information-sharing venues. These include the DHS National Cybersecurity and Communications Integration Center (NCCIC) and the NERC Electricity Sector Information Sharing and Analysis Center (ES-ISAC), both of which inform the industry on recommended preventative actions.

8. 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. 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 electricity sub-sector is subject to mandatory NERC Critical Infrastructure Protection (CIP) and NRC cybersecurity requirements. Section 215 of the Federal Power Act and FERC gave NERC authority to develop enforceable cybersecurity standards. The NERC CIP-002 through CIP-009 standards were approved by FERC in 2008, making them mandatory for owners and operators of the bulk power system. Since 2008, the standards have been updated as the threat landscape continues to evolve. The NERC CIP standards are tailored to electricity sub-sector cyber risks and focus on protecting Critical Cyber Assets through a number of security practices that support the reliability of the bulk power system. Version 3 is currently used by the electricity sub-sector. Version 4 will replace version 3 on April 1, 2014 and Version 5 was filed with FERC on February 1, 2013.

The Atomic Energy Act and the NRC created mandatory standards for nuclear power reactor licensees, 10 CFR § 73.54 "Protection of digital computer and communication systems and networks" for nuclear power plants. The regulation requires licensees to submit a comprehensive cybersecurity plan and an implementation timeline for NRC approval. A memorandum of understanding and policy statement by the NRC ensure that there is good coordination between NERC and the NRC, so that no gaps in protection exist for nuclear generators.

Reporting occurs for many different purposes and in many different contexts. The range of reporting obligations stretches from accounting and governance to privacy, operational issues, outages and criminal investigations. Many of these reporting requirements focus on potential impacts of cyber acts and do little to help identify or respond to actual cyber threats.

For example, the SEC requires reporting for information about cybersecurity as it relates to material investor interests; the FTC requires reporting to customers when certain financial information is compromised in a cyber situation (the red flag rule); state utility regulatory commissions may seek justifications for the recovery of costs incurred to protect cybersecurity and may seek information

about cyber events; DOE and EIA collect information about outages, including those relating to cybersecurity, and almost every state requires reporting to affected individuals when a cyber intrusion potentially compromises the privacy of individual confidential financial or other information. These kinds of notices usually do not and should not reveal sensitive information about the nature of the threat or breach that occurred and corrective actions.

We urge NIST to focus, at least initially, exclusively on requirements that share information about cyber threats, intrusions, protective measures and warnings and are sufficiently detailed to be useful to others that could be subjected to similar events.

In the electricity sub-sector, NERC requires the reporting of reliability disturbances to its Regional Reliability Organization and NERC (Standard EOP-004-1); cyber events to the ES-ISAC (Standard CIP 008-3); and sabotage events to "appropriate systems, governmental agencies, and regulatory bodies" (Standard CIP 001-2). The sector also has reporting requirements to DOE through Form OE-417. Cyber events that interrupt electric system operation must be reported to DOE within an hour of the incident (Emergency Alert). Cyber events that could impact the adequacy or reliability of the electric power system must be reported to DOE within 6 hours of the incident (Normal Alert). DOE reporting is also required within 6 hours if more than 50,000 customers lose electric service for an hour or more and when fuel supply emergencies could impact electric power system adequacy or reliability. Cyber events are also reported to state and local law enforcement and the FBI for investigation.

With respect to the ES-ISAC, NERC utilizes an alert system that helps inform electric utilities' response to cyber threats and vulnerabilities. The ES-ISAC developed the following three levels of Alerts to formally notify the industry regarding security issues:

- Level 1 Industry Advisory – These are purely informational and intended to alert registered entities to issues or potential problems.
- Level 2 Recommendation to Industry - Recommends specific action by registered entities. Recipients are required to respond as defined in the Alert.
- Level 3 Essential Action - Identifies actions deemed to be "essential" to bulk power system reliability. Like recommendations, essential actions require recipients to respond as defined in the Alert.

Alerting utilities to potential threats and providing guidance on mitigation of those threats is an example of close industry coordination in defense of the larger system that does not require a formal standard. These Alerts and Notifications are a valuable tool to rapidly provide more detailed and tactical information to all components, assets and functions of the bulk power system. In total, NERC has issued 24 CIP-related Alerts since January 2010 (22 Industry Advisories and two Recommendations to Industry). These Alerts covered items such as Aurora, Stuxnet, Night Dragon, and the reporting of suspicious activity.

Our industry seeks to have an even better situational awareness of cyber events affecting the government and other sectors of the economy to the extent that these can affect the electricity sub-sector as well. Our industry strongly supports the Executive Order as it seeks to address this need.

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 power industry is interdependent with all of the sectors mentioned. –Further coordination with these sectors is needed.

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

    The NERC CIP standards and processes apply to the interconnected grid in both Canada and Mexico and are thus international in nature. It is worthwhile to review international standards to obtain best practices.

II Use of Frameworks, Standards, Guidelines, and Best Practices

1. **What additional approaches already exist?**
2. **Which of these approaches apply across all sectors?**
3. **Which organizations use these approaches?**

A number of approaches to cybersecurity already exist for the electricity sub-sector, including mandatory and voluntary standards, frameworks, guidelines and best practices, many of which are discussed below. While standards may have a role in encouraging a baseline level of security and good business practices, standards alone are not sufficient because the cybersecurity environment is constantly changing and evolves rapidly. EEI strongly believes that the NIST Framework should be a high-level and flexible tool, leverage existing approaches and public-private cybersecurity partnerships and focus on cost-effective risk management. The Framework development process should not try to develop new cybersecurity standards because new standards will likely overlap and duplicate the existing approaches already in use by the electricity and other sectors.

The Electricity and Nuclear Sectors have Mandatory Cybersecurity Standards

The electricity and nuclear sectors are the only critical infrastructure sectors with mandatory and enforceable cybersecurity standards. The Energy Policy Act of 2005 created an Electric Reliability Organization (ERO) to develop and enforce mandatory cybersecurity standards. NERC was designated as the ERO in 2006 and worked with electricity sub-sector experts to develop the NERC Critical Infrastructure Protection (CIP) standards CIP-002 through CIP-009, which were approved by FERC in 2008, making them mandatory for owners and operators of the bulk power system. The NERC CIP standards are tailored to electricity sub-sector cyber risks and focus on protecting Critical Cyber Assets through a number of security practices that support the reliability of the bulk power system. Since 2008, the standards have been updated as the threat landscape continues to evolve. Version 3 is the currently used by the electricity sub-sector. Version 4 will replace version 3 on April 1, 2014 and Version 5 was filed with FERC on February 1, 2013. The Atomic Energy Act and Nuclear Regulatory Commission (NRC) created mandatory standards for nuclear power plants.

The Electricity Sub-sector Also Employs Voluntary Cybersecurity Guidance

The electricity sub-sector recognizes that standards can elevate cybersecurity across a sector by requiring the implementation of minimum security measures that set a baseline for the sector's cybersecurity practices. However, this baseline security is not enough to secure the sector against a dynamic and rapidly evolving threat landscape. Therefore the sector partners with federal agencies, including NIST, the Federal Energy Regulatory Commission (FERC), the Department of Homeland Security (DHS), and the Department of Energy (DOE) to develop cybersecurity practices that improve sector-wide resilience to cyber threats. In addition to the existing frameworks, standards, guidelines, and best practices ("cybersecurity guidance") developed in collaboration with the federal government, there is also cybersecurity guidance that has been developed by non-governmental organizations. Examples of existing cybersecurity guidance that is tailored to and being used by the electricity sub-sector include:

- *Electricity Subsector Cybersecurity Capability Maturity Model* (ES-C2M2) – a model developed by DOE, DHS, and industry subject matter experts to help electric utilities and grid operators to assess their cybersecurity capabilities and prioritize their investments to enhance cybersecurity.

- NISTIR 7628, *Guidelines for Smart Grid Cyber Security* – a framework for assessing Smart Grid cybersecurity risk and applying the security measures to mitigate that risk.

- *Threat Scenario Project* – an ongoing project by EEI, private sector experts, and its member utilities, to identify threats to the electric grid and practices to mitigate these threats. Identified threats include coordinated cyber attacks, as well as blended physical and cyber attacks. The project established common elements for each threat scenario, including a description, likely targets, potential threat actors, specific attack paths, and likely impacts of a successful attack. The project continues to evolve as the threat landscape changes in order to keep the industry prepared to identify and defend against emerging cyber threats.

- *Roadmap to Achieve Energy Delivery Systems Cybersecurity* – a strategic framework for industry, vendors, academia, and government stakeholders to design, install, operate, and maintain a resilient energy delivery system capable of surviving a cyber incident while sustaining critical functions.

- *Vulnerability Analysis of Energy Delivery Control Systems* – an Idaho National Laboratory report, based on assessments performed between 2003 and 2010 that describes common energy sector control system vulnerabilities and recommendations for vendors and asset owners to identify and reduce risks.

- IEEE 1686, *Security for Intelligent Electronic Devices* – standards developed by the Institute of Electrical and Electronics Engineers (IEEE) that set minimum requirements for substation intelligent electronic devices.

- IEC 62351 – series of information security standards for power system control operations developed by the International Electrotechnical Commission (IEC).

Cybersecurity guidance used by the electricity sub-sector, which are applicable to multiple sectors include:

- *Critical Controls for Effective Cyber Defense* – technical measures to detect, prevent, and mitigate damage from the most common and damaging cyber attacks. Formerly named the SANS Top 20 Critical Controls, version 4.1 was released in March 2013 and is available on the SANS website.

- *Cyber Resilience Review* (CRR) – DHS on-site assessment program to measure and enhance the implementation of critical infrastructure cybersecurity programs.

- NIST SP 800-82, *Guide to Industrial Control Systems (ICS) Security* – a guide to control systems threats, vulnerabilities, and mitigation countermeasures.

- NIST SP 800-83, *Guide to Malware Incident Prevention and Handling*.

- NIST SP 800-153, *Guidelines for Security Wireless Local Area Networks (WLANs)*.

- NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations* – best practices in information security, which includes an appendix tailored to security of industrial control systems.

- ISO/IEC 27000-series – information security standards published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

- IT Infrastructure Library (ITIL) – a framework of information technology service management best practices.

- Control Objectives for IT (CobiT) – a framework of policy, process, procedures, and metrics to govern IT operations, which includes risk management.

- *Process Control Domain Security Requirements for Vendors* – outlines specific cybersecurity requirements based on best practices for suppliers of industrial automation and control systems. Developed by WIB, the International Instrument Users' Association.

- ISA99/IEC 62443 – industrial automation and control system security standards developed by the International Society of Automation (ISA), which are being used by the International Electrotechnical Commission (IEC) to produce the IEC 62443 series of standards.

- *Cyber Security Procurement Language for Control Systems* – security principles released by DHS for designing and procuring control systems products and services.

- Defense Information Systems Agency Security Technical Implementation Guide – protection profiles for information assurance products.

In addition to the development and use of cybersecurity guidance, the electricity sub-sector collaborates with federal agencies, state and local agencies, and law enforcement to strengthen its cybersecurity capabilities. Electricity companies also actively participate in a number of cyber defense initiatives with their vendors, each other, and through coordinated industry initiatives.

4. **What, if any, are the limitations of using such approaches?**
5. **What, if any, modifications could make these approaches more useful?**

6. **How do these approaches take into account sector-specific needs?**
7. **When using an existing framework, should there be a related sector-specific standards development process or voluntary program?**
8. **What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?**
9. **What other outreach efforts would be helpful?**

Public-Private Coordination Is Required

Protecting the grid from cyber attacks requires a coordinated effort among electric companies, the federal government, other critical infrastructure sectors the electricity sub-sector depends upon and the suppliers of critical electric grid systems and components. To complement its cybersecurity efforts and to address rapidly changing intelligence on evolving threats, the industry embraces a cooperative relationship with federal authorities to protect against situations that threaten national security or public welfare, and to prioritize the assets which need enhanced security**.** A well-practiced, public-private partnership utilizes all stakeholders' expertise, including the government's ability to provide clear direction and assess threats, while owners and operators of the critical infrastructure develop mitigation strategies that will avoid significant adverse consequences to utility operations or assets.

The NIST Framework should leverage existing public-private partnerships. DHS and sector-specific agencies have worked with the electricity sub-sector during the past decade to improve information sharing, operational resiliency, and emergency response capabilities of critical infrastructure. For example, in 2009, DHS developed the Private Sector Preparedness program (PS-Prep), a voluntary certification program for emergency preparedness.

Focus on Risk Management for Essential Systems to Address Rapidly Evolving Threat and Technology Advances

Developing and implementing cybersecurity guidance to keep pace with rapidly evolving threats is challenging. Standards in particular take time and industry-specific expertise to develop, review, approve, and publish. Such development processes are necessary due to the complexity and uniqueness of various information and control systems used throughout critical infrastructures. Business information and control system implementations vary widely among companies within a sector; therefore sector specific guidance may not even be applicable or necessary to some companies. The variation between companies in different critical infrastructure sectors is even greater. Also, cybersecurity guidance tends to be lengthy, requiring further time for asset owners and operators to review, analyze, and implement the guidance to their specific systems.

To address rapidly evolving threats and technology advancements, the electricity sub-sector supports a risk-based, prioritized approach that identifies assets truly critical to the reliable and safe operation of the electric grid. This ensures the most essential elements of our systems receive the highest level of attention, as well as the resources necessary to secure them. However, to keep pace with threats to the electric grid, rapid and secure sharing of actionable threat information is needed to inform risk management processes.

Threat information must be shared quickly through secure mechanisms within the critical infrastructure sector and between the sector and the federal government. This information must

also be shared rapidly and securely with the vendors and service providers the critical infrastructure sectors rely upon. In turn, these vendors and service providers need guidance for responding to the threat information in a manner that best serves their critical infrastructure customers, pertaining to the services they provide.

The federal government's threat intelligence is often classified, which slows down its sharing with and use by private sectors. Also, the federal government may not have the technical expertise specific to critical infrastructure to determine which threat information is most needed by the sector. Within a critical infrastructure, antitrust laws may inhibit information sharing among companies.

Although privacy is an important concern for the electricity sub-sector (see section III for more on privacy), the threat information the sector needs are digital signatures or fingerprints such as IP addresses and other indicators of compromise left behind by attackers. This threat information is based on analysis of past attacks and does not contain personal information that triggers privacy protections.

EEI supports the measures outlined in section 4 of the Executive Order aimed at increasing the "volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats." Improving information sharing requires establishing trust between and within the federal government, critical infrastructures, vendors, and service providers. The private sector must have confidence that the government will use the information it receives from sector companies for national security purposes and not publicly disclose or use the information to impose regulatory penalties. NIST should be aware that the electricity sub-sector is required by critical infrastructure protection standards to implement and document a security program that identifies, classifies and protects sensitive information associated with critical cyber assets (CIP-003 R4). With strong information protection measures already in place, the sector is well-positioned to work with the federal government to receive and protect sensitive threat information that could allow electric utilities to further strengthen its cybersecurity protections.

Leveraging existing public-private partnerships and relationships are important for improving information sharing. Other challenges to this information sharing include antitrust laws, which may inhibit sharing within and among sectors.

<u>Avoid Unintended Consequences of New Cybersecurity Guidance on Sectors with Established Voluntary and Mandatory Practices</u>

Although new cybersecurity guidance aimed at improving critical infrastructure cybersecurity may work for some critical infrastructure sectors, it could have unintended, negative impacts on sectors such as the electricity sub-sector with existing mandatory and voluntary standards. Mandatory, regulatory standards take priority over voluntary standards and practices because non-compliance is a high risk, especially when substantial monetary penalties are involved (e.g., NERC CIP standards). However voluntary standards also increase risk as non-compliance can create liability and reputational risk. Given the vast number of already existing cybersecurity standards, this becomes difficult and expensive for organizations to manage often due to potentially conflicting or ambiguous standards.

Proving compliance often involves capturing evidence and extensive documentation, which increases compliance costs (resources). These costs to critical infrastructure should be carefully considered before developing or adopting new mandatory or voluntary federal or state cybersecurity guidance. Cybersecurity guidance should be cost-effective. Compliance costs should be proportional to the cybersecurity improvements they bring to critical infrastructure.

To mitigate these unintended consequences, new cybersecurity guidance should be closely aligned with existing guidance and risk management practices. Alignment means that the guidance will not conflict with existing cybersecurity guidelines or create double jeopardy situations. For a voluntary cybersecurity framework to be embraced by the private sector this alignment is particularly crucial for mandatory standards. Tools to facilitate the implementation of a new cybersecurity framework such as checklist summaries, use cases, and a map of the Framework to other sector specific and cross-sector cybersecurity guidance will also help to encourage adoption.

Recognize that Voluntary Cybersecurity Guidance Is NOT Designed for Mandatory Compliance

Voluntary frameworks, standards, guidelines, and best practices are designed to aid critical infrastructure in managing risk and applying the necessary security controls. The processes used to develop voluntary guidance are not designed to produce enforceable guidance. Mandatory standards require developing agreed upon, clear, concise and unambiguous language upon which compliance can be equitably measured against. The NIST Cybersecurity Framework is intended for voluntary use. The voluntary use of the framework should be clearly stated within the document(s) developed by NIST as well as in outreach efforts associated with the Framework. However, the Cybersecurity Framework and other cybersecurity guidance can be used to inform existing regulatory development processes, as described in section 10 of the Executive Order.

Consider that Cybersecurity Guidance Can Help Attackers

Cybersecurity guidance, intended to improve critical infrastructure cybersecurity, can also provide guidance to attackers by giving them a “blueprint” to the security measures a sector is required or encouraged to implement. In developing a framework to improve critical infrastructure cybersecurity, consideration should be given to the fact that this information can also provide knowledge to those looking to compromise our systems. A balance between detailed requirements and the risk of publishing this information should be considered throughout the Framework development process.

Support the Role of DOE and Sector Coordination Councils

DOE is the sector-specific agency for the electricity sub-sector. DOE has already led the development of cybersecurity guidance specific to the electricity sub-sector. In addition, DOE provides incentives for research development and deployment of advanced electricity sub-sector cybersecurity solutions through its Cybersecurity for Energy Delivery Systems program, which is guided by the *Roadmap to Achieve Energy Delivery Systems Cybersecurity* and input from sector subject matter experts. DOE’s operational knowledge of the electricity sub-sector gives it the unique capability to further assist the electricity sub-sector by developing implementation guidance, education, and training for the Cybersecurity Framework developed by NIST.

The sector coordinating councils, the Electricity Sub-sector Coordination Council (ESCC) and the Government Coordinating Council (GCC), should focus on bringing together electricity and government executives to focus on key cybersecurity challenges such as sector-wide incident response to a large-scale cyber event. Working groups such as the Energy Sector Control Systems Working Group (ESCSWG) can be used to implement the coordinating council priorities.

III Specific Industry Practices

The RFI sought information regarding adoption of the following nine practices:

- **Separation of business from operational systems**
- **Use of encryption and key management**
- **Identification and authorization of users accessing systems**
- **Asset identification and management**
- **Monitoring and incident detection tools and capabilities**
- **Incident handling policies and procedures**
- **Mission/system resiliency practices**
- **Security engineering practices**
- **Privacy and civil liberties protection**

1. General Comments to Answer the Questions about these Practices.

The nine practices listed in the RFI are widely used by the electricity sub-sector and are addressed by the NERC CIP standards and the other cybersecurity guidance listed above. The criticality and application of the practice may vary by entity, depending on the operation and information technologies used by an organization's systems and the implementation of these systems. Each poses a unique set of challenges, including implementation, administrative, operational, complexity, and cost. Therefore, a risk management process and a comprehensive strategy incorporating these and other practices for a defense-in-depth approach are needed to address these challenges.

Other practices used by industry include:

- Integration of physical security practices, enterprise IT, and energy control systems
- Robust personnel screening, training and awareness programs
- Threat intelligence and monitoring practices, including information sharing
- Configuration and vulnerability management practices
- Separation of control systems from Internet facing systems
- Removable media control and sanitization
- Change control processes to ensure changes to the IT infrastructure are performed in a controlled and coordinated manner and do not negatively impact cybersecurity
- Procurement protections to ensure products or services of prospective vendors are vetted prior to being approved for use
- Decommissioning practices such as wiping devices/media

- Forensics analysis

Cybersecurity guidance focused on these practices and guided by an organization's risk management process are used for the development of internal cybersecurity policies, standards, and procedures for the protection of IT information and control system assets. During system design, the guidance is used for risk assessment, security by design, and procurement processes. During system operation, the guidance is used for ongoing security efforts, including monitoring, response, and system/asset/user management. As indicated previously, the ES-ISAC provides a three tiered alert system to the electricity sub-sector that reflects the severity of cyber threats. However, more timely sharing of threat information by the federal government is critical to improve our efforts to identify risks for risk assessment and resource allocation purposes.

As EEI indicated in the portion of our comment addressing risk management practices, protecting the nation's power grid and maintaining the reliability of our electricity supply is our top priority. All electric providers devote the resources necessary to satisfy the NERC CIP requirements. In addition almost all providers of transmission and distribution services and many, if not most electric power generators are subject to rate regulation by FERC and state public utility commissions which require a showing that costs of service, including costs of providing cybersecurity are "just and reasonable." As we commented earlier, the more information we have about the full scope of threats facing the electric grid, the better we can allocate resources.

2. Privacy

EEI's members have a long history of protecting the privacy of customer data and respecting the civil liberties of their customers. In view of the development of Smart Grid technologies, the electric industry has had to revisit industry privacy practices and as a result, even stronger privacy standards and practices have been developed, as described below. The electric industry continues to work with federal and state officials (including NIST), as well as other stakeholders to refine and improve its privacy standards and practices. Consequently, EEI's members generally have privacy practices in place based on widely accepted national and international standards and principles. Given that the electric industry is complex and EEI's members face varying state regulatory requirements, utilities have implemented these practices on a company-by-company basis. Therefore, EEI believes that the utility industry should continue to manage risks to privacy and civil liberties through the implementation and refinement of existing privacy practices and principles.

Answers to Selected Questions regarding Privacy

1. Are these practices widely used throughout critical infrastructure and industry?

Protecting customer privacy is an important and well-established priority for EEI's members, virtually all of whom have policies in place to protect access to customer data**.** Traditionally, privacy regulation of customer data has been the responsibility of the states, and virtually all of the states have developed various data privacy, access and disclosure laws governing utility customers. States and the federal government also have consumer protection laws safeguarding the interests of energy consumers.

The deployment of Smart Grid technology has introduced new data collection and information sharing abilities related to customer data, and in recognition of the privacy and data access issues which have

been raised, electric utilities have acted in coordination with state and federal officials (including NIST), stakeholders and privacy experts to update their policies and procedures. Generally, these updated standards and practices are based on Fair Information Practice Principles ("FIPPs"), such as those outlined in the White House Report entitled "Consumer Data Privacy in a Networked World" and the Federal Trade Commission ("FTC") report entitled "Protecting Consumer Privacy in an Era of Rapid Change." Another example of a recent industry standard is NAESB REQ.22, which establishes voluntary Model Business Practices for Third Party access to Smart Meter-based information. Similarly, Volume 3 ("Privacy and the Smart Grid") of NISTIR 7628 provides another example of updated industry guidelines/recommendations based on FIPPs principles. The NIST Cybersecurity Working Group ("NIST/CSWG") continues its work in this area through its Privacy Subgroup. More recently, the industry has been working with the Department of Energy ("DOE") to develop a voluntary code of conduct ("VCC") consisting of the following elements:

- Management and Accountability;
- Notice and Purpose, Choice and Consent;
- Use and Retention; Individual Access;
- Disclosure and Limitations;
- Security and Safeguards;
- Accuracy and Quality;
- Openness, Monitoring, and Challenging Compliance; and
- Enforcement Mechanisms.

2. How do these practices relate to existing international standards and practices?

As noted above, the aforementioned standards and practices are based on FIPPs that are internationally recognized. The Organization for Economic Co-operation and Development ("OECD") Privacy Principles represent an example of similar principles. Internationally, the OECD Privacy Principles provide the most commonly used privacy framework. Existing and emerging privacy and data protection laws reflect OECD Privacy Principles, which continue to serve as a basis for the creation of leading practice privacy programs and additional principles.

6. How are standards or guidelines utilized by organizations in the implementation of these practices?

Standards or guidelines of the kinds identified above provide useful references to EEI members in assessing the adequacy of existing policies and practices, and updating them where needed. EEI members have taken a number of steps individually to implement privacy standards and practices by developing, reviewing, updating and implementing internal privacy policies. Such efforts include creation by some EEI members of a "Privacy Officer" position, charged with overseeing corporate privacy policy issues, as well as monitoring necessary policy changes, and responding to privacy-related concerns and inquiries. Likewise, other EEI members are tasking existing compliance officers with similar responsibilities.

Additionally, some EEI members are forming internal organizations to review customer privacy issues and policies. Utilities are also gathering input and expertise from their legal departments in review of state privacy requirements as applied to customer privacy. Other utilities have developed data access policies, based on the privacy and data access consensus guidelines developed by EEI's members.

9. What risks to privacy and civil liberties do commenters perceive in the application of these practices?

The primary privacy issue related to the deployment of Smart Grid technologies is that the collection, transmittal and maintenance of personally identifiable data related to the nature and frequency of personal energy consumption and production in a more granular form. However, the privacy practices already in place have not proven to be a threat to civil liberties, but rather reflect industry commitment to protect customer privacy. Privacy of customer financial information is covered by multiple consumer protection laws in virtually every state and federal requirements, such as the FTC's red flag rule.

11. How should any risks to privacy and civil liberties be managed?

Risks to privacy and civil liberties in the utility industry should continue to be managed through the implementation and refinement of existing privacy practices and principles.