NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

National Institute of Standards and Technology Request for Information North American Electric Reliability Corporation Response – April 8, 2013

Request for Information (RFI) Overview

This paper constitutes the North American Electric Reliability Corporation's (NERC) responses to the National Institute of Standards and Technology's (NIST) notice and request for information on "Developing a Framework to Improve Critical Infrastructure Cybersecurity" (Docket Number 130208119–3119–01), Fed. Reg. Vol. 78, No. 38 (February 26, 2013) at pp. 13024.

NERC's mission is to ensure the reliability of the North American bulk power system (BPS). NERC is the electric reliability organization (ERO) certified by the Federal Energy Regulatory Commission (FERC) to establish and enforce Reliability Standards for the BPS within the United States in accordance with Section 215 of the Federal Power Act enacted by the Energy Policy Act of 2005. NERC's Reliability Standards are mandatory and enforceable within the United States for the BPS and include Critical Infrastructure Protection (CIP) standards. The bulk power industry has the largest collection of collaboratively developed, mandatory and enforceable standards of any critical infrastructure sector. NERC develops and enforces Reliability Standards to secure the BPS; assesses adequacy annually via a 10-year forecast, and summer and winter forecasts; monitors the BPS; and educates, trains, and certifies industry personnel. In addition, NERC addresses security issues from both a physical security perspective as well as a cybersecurity perspective, engaging with government and industry partners on threats, vulnerabilities, and mitigation strategies. ERO activities in Canada related to the reliability of the BPS are recognized and overseen by the appropriate governmental authorities in that country.

The BPS is highly interconnected, and the owners and operators are highly interdependent in their reliable operation of the grid. The grid is in reality a single, very large machine. Disturbances and off-normal events at one location on the grid can have serious consequences at other, far-removed locations, even crossing international boundaries. At the same time, the asset owners and operators of the electricity industry comprise a numerous and widely diverse group, in terms of size, ownership, business model, and footprint. Within the United States, there are approximately 200 shareholder-owned utilities, 800 electric co-operatives, and more than 2,000 government-owned utilities. The largest may serve several millions of customers and have a footprint that spans several states. The smallest may serve only a few hundred customers in a single municipality. Some are vertically integrated utilities that own and

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

operate generation, transmission, and distribution assets. Others own no assets but have operating control over the transmission assets owned by a number of utilities, in a number of states. Some own and operate only transmission assets; others, only generation.

RFI Questions

Section 1: Current Risk Management Practices

NIST solicits information about how organizations assess risk; how cybersecurity factors into that risk assessment; the current usage of existing cybersecurity frameworks, standards, and guidelines; and other management practices related to cybersecurity. In addition, NIST is interested in understanding whether particular frameworks, standards, guidelines, and/or best practices are mandated by legal or regulatory requirements and the challenges organizations perceive in meeting such requirements. This will assist in NIST's goal of developing a Framework that includes and identifies common practices across sectors.

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

One of the greatest challenges for cybersecurity improvement is information sharing between the Federal government and the private sector. The Electricity Sub-sector is very timely and efficient with information sharing with and between owners and operators of the BPS, but as the NERC Grid Security Exercise (GridEx 2011) showed,[1] improvements should be made with the sharing of threat information from the Federal government to private industry. The information sharing process can be better defined and significantly improved by providing better access to information through the clearance program and classified briefs. NERC's Electricity Sector Information Sharing and Analysis Center (ES-ISAC) hosts annual sector-specific classified briefs, where the Federal government has provided timely security briefs and NERC recommends additional classified briefs be given to the Electricity Sub-sector. Because of the large number of private asset owners and operators in the Electricity Sub-sector, the effort must also focus on increasing the flow of non-classified threat information from the Federal government to those entities.

Another challenge in improving cybersecurity practices across the critical infrastructures is workforce development and training. Many program owners across multiple sectors recognize that adversaries are highly skilled and increasingly capable. Several United States Federal departments and agencies have confirmed that their systems have been compromised due, in part, to human responses to spear phishing attempts. NERC provides industry exercises and training opportunities through webinars and on-site assessments as one way to address this challenge.

[1] http://www.nerc.com/files/NERC_GridEx_AAR_16Mar2012_Final.pdf.

Technology vendors are bringing significantly more advanced technologies to address the threats and vulnerabilities companies face; advances in firewalls, data diodes, virtualization, clouds, and encrypted operating systems have hardened our systems. In addition, the presence of cybersecurity standards for the Electricity Sub-sector is significant, because those standards provide a base on which to build an effective cybersecurity program.

Even with these advances, the proliferation of attack surfaces requires ongoing training and identification of best practices to ensure the workforce understands how to identify and address threats that affect critical infrastructure.

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

A cross-sector standards-based framework must take into account the varying aspects of each of the critical infrastructure and key resources (CIKR) sectors. While a framework of cybersecurity standards that is applicable to all sectors is possible, the framework may need flexibility to have certain common elements to be valuable or effective. Some sectors, such as the Electricity Sub-sector, are far more advanced in their cybersecurity efforts; other sectors may need time to meet minimum (voluntary) standards. The framework must build on existing standards and programs to develop a comprehensive approach to cybersecurity.

In addition, standards and laws developed to address cybersecurity have been addressed by various Federal departments and agencies. This sector-by-sector approach has led to a variable set of guidelines, standards, and regulations. Executive Order (EO) 13636 changes this “siloed” approach by looking across all CIKRs, while recognizing further legislation may be needed.

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?**

NERC’s mission is to ensure the reliability of the North American BPS and promote reliability excellence with accountability for standards and compliance, risks to reliability, and continued coordination and collaboration with public and private sector partners.

NERC has established standards, as well as policies and procedures to address risk, including cybersecurity risk. These include:

- Mandatory and enforceable CIP Standards, applicable to certain BPS users, owners, and operators
- Activities conducted through the ES-ISAC, including issuing alerts related to cybersecurity concerns
- A risk management process guideline to help utilities better understand their cybersecurity risks, assess severity, and allocate resources more efficiently to manage those risks

- Completing the first phase of the High-Impact Low-Frequency Task Force reports identifying recommendations for owners and operators with respect to addressing severe impact resilience, cyber attacks, spare equipment, and geomagnetic disruptions
- Facilitating the first-ever distributed-play, GridEx 2011, for the Electricity Sub-sector in North America (GridEx II is scheduled for 2013)
- Participating in government partnership initiatives, including the Department of Homeland Security's (DHS) National Level Exercise series and various cybersecurity forums and briefings with Canadian government agencies, as well as the White House–initiated, Department of Energy (DOE)-led Electricity Sub-sector Cybersecurity Capability Maturity Model (ES-C2M2)
- Electricity Sub-sector Cybersecurity Risk Management Process (RMP) Guideline, developed with DOE, NIST, NERC, and the sub-sector, which supports ongoing development and measurement of cybersecurity capabilities and entity risk within the sub-sector

Additionally, in 2012, NERC established the Reliability Issues Steering Committee (RISC) to consider various threats to reliability, including those threats associated with cybersecurity, and to allocate appropriate levels of resources to respond to those threats. In February 2013, the RISC recommended to NERC's Board of Trustees that it should consider threats associated with cyber attacks one of four top priorities for NERC to address. NERC's Board accepted this recommendation, and the RISC is now working with NERC's Critical Infrastructure Department staff to develop actionable strategic plans for dealing with cyber attacks in a meaningful, efficient, and measurable way.

4. Where do organizations locate their cybersecurity risk management programs/offices?

Based on NERC's interactions with sector entities, the locations, structures, roles, and responsibilities for cybersecurity risk management programs and offices vary significantly across the electricity industry. This is understandable in view of the wide range in size, business model, and nature of sector participants. Larger organizations may have multiple locations where cybersecurity risk management activities occur. For instance, an entity with electric generation, electric transmission, and natural gas operations may conduct cybersecurity risk management activities within each business unit. Risk management activities conducted at the business unit level often inform, or are informed by, a broader "enterprise" risk activity that looks across the entire organization.

Drivers for risk management implementation may include integration or division of the information technology (IT) activity relative to the operations technology (OT) within the organization. In addition, implementation of certain technologies or systems may drive organizations to segregate or integrate cybersecurity risk management activities. Some small-to-medium organizations with a single business unit such as transmission or distribution may integrate IT completely with OT within the organization because the same personnel are responsible for both systems. Additionally, the senior manager responsible for IT and OT may directly report to the chief executive officer or governing board, integrating cybersecurity risk

management activities across the organization and within the various levels of the organization (system administrators, managers, leadership).

5. **How do organizations define and assess risk generally and cybersecurity risk specifically?**

Generally, most organizations view risk as anything that has the potential to disrupt delivery of service or result in a failure to meet organizational objectives. For the electric power industry, risk generally means something that has the potential to disrupt delivery of electric power to customers. Cybersecurity risk is defined in numerous documents applicable to the sub-sector. The RMP guideline developed by DOE, in partnership with NIST, NERC, and the sub-sector, defines cybersecurity risk as "the risk to organizational operations (including mission, functions, image, and reputation), resources, and other organizations due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or IT and ICS."[2] This definition is derived from the NIST Special Publication 800-39, "Managing Information Security Risk Organization, Mission, and Information System View" definition for Information Security Risk.

Cybersecurity risk assessments can use a variety of methodologies that often are more broadly applicable to organizational risk management. For example, Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is a suite of tools, techniques, and methods for risk-based information security strategic assessment and planning designed specifically for cybersecurity risk management. Attack trees are another method sub-sector organizations use to understand and assess risk. This methodology develops chains of events required to execute an attack from an adversary, or more generally, a chain of events leading up to any event that may have an adverse impact on a system of asset. Organizations can use this methodology to determine the likelihood of an incident and in developing capabilities for mitigating or protecting against attacks. One of the challenges facing all industries is that data on cyber events is often limited, so determining likelihood of occurrence—and thus, assessing risk—can be challenging for organizations. Overcoming information sharing hurdles among organizations, government, and sectors will improve the Nation's ability to assess cybersecurity risk. Organizations such as the ISACs are in place to reduce hurdles, enable sharing of information, and provide aggregated information to assist in risk assessment and management activities.

6. **To what extent is cybersecurity risk incorporated into organizations' overarching enterprise risk management?**

Incorporating cybersecurity risk into the overarching enterprise risk within sub-sector organizations varies across the industry. Some mature organizations have largely integrated cybersecurity risk into enterprise risk management activities. NERC is applying a risk management approach to the mandatory standard

[2] Industrial Control Systems (ICS).

process as well as mandatory compliance. Due to the highly technical nature of cybersecurity activities, some organizations treat cybersecurity risk independently from enterprise risk, but may develop organizational reporting mechanisms for risk management assessments to senior leadership within the organization. Organizational challenges, such as whether cybersecurity risk is the responsibility of the security organization or the network operations group, can shape whether the organization treats cybersecurity as an enterprise risk from a reporting and monitoring perspective.

To the extent organizations have incorporated cybersecurity risk into the overarching enterprise risk, the organization has greater awareness of the impact of cyber threats to its operations. As a result, senior management is more involved and resources are more appropriately allocated to address the threats.

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

Depending on an entity's business and operations, an organization may use many standards, guidelines, and best practices. NERC has developed a set of mandatory standards for the Electricity Sub-sector that address cybersecurity.

CIP Standards

NERC Reliability Standards define the reliability requirements for planning and operating the North American BPS, and are developed using a results-based approach that focuses on performance, risk management, and entity capabilities. NERC develops Reliability Standards using an industry-driven American National Standards Institute (ANSI)-accredited process. CIP standards are Reliability Standards for critical infrastructure protection focused on cybersecurity and physical security of cyber assets. NERC's current CIP standards include the following:

CIP-001-2 – Sabotage Reporting
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 CIP standards goes into effect on April 1, 2014. NERC filed Version 5 of the CIP standards with FERC on January 31, 2013, providing a more comprehensive approach to CIP.

Some examples of industry-wide guidelines include:

Electricity Sub-sector Cybersecurity RMP guideline

Published: May 2012

The Electricity Sub-sector cybersecurity RMP guideline was developed by DOE, in collaboration with NIST and NERC, as well as members of industry and utility-specific trade groups. The primary goal of this guideline is to describe an RMP that is tailored to the specific needs of Electricity Sub-sector organizations. The NIST Special Publication (SP) 800-39, Managing Information Security Risk, provides the foundational methodology for this document.

ES-C2M2

Published: May 2012

The ES-C2M2 was developed by DOE, in collaboration with NIST, NERC, DHS, and industry. The goal of this model is to support ongoing development and measurement of cybersecurity capabilities within the Electricity Sub-sector through the following four objectives:

- Strengthen cybersecurity capabilities in the Electricity Sub-sector
- Enable utilities to effectively and consistently evaluate and benchmark cybersecurity capabilities
- Share knowledge, best practices, and relevant references within the sub-sector as a means to improve cybersecurity capabilities
- Enable utilities to prioritize actions and investments to improve cybersecurity

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?**

The United States Energy Policy Act of 2005 added section 215 to the Federal Power Act and authorized the creation of an ERO with FERC oversight (in the United States). Section 215 contemplated that the ERO would achieve equivalent recognition in Canada and Mexico. In 2006, FERC certified NERC as the ERO for the United States. As a result, Section 215 made compliance with Reliability Standards mandatory and enforceable for users, owners, and operators of the BPS within the United States. NERC has the legal authority to monitor and enforce compliance with NERC Reliability Standards and, subject to FERC oversight, to impose penalties or sanctions for non-compliance. NERC has delegated certain activities to eight Regional Entities. FERC also has independent authority to enforce compliance with the Reliability Standards.

At the state level, each state has a state public utility commission (PUC) or equivalent office that is responsible for regulating the electric power utilities in that state. Some states, such as Pennsylvania, have required cybersecurity response plans.

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

For the Electricity Sub-sector, other critical sectors such as communications and transportation may affect industrial control systems, energy market systems, energy management systems, and various energy generation, transmission, and distribution systems. Sector analytic and communication/coordination tools may also be affected by interdependent critical sectors. Interdependency impacts from other sectors could affect the Electricity Sub-sector (and the larger Energy Sector), including each of the sectors listed in Question 9, either with direct impacts, or by providing early advanced indications and warning of potential risks to the sector. These indications could be actionable, with timely mitigation guidance that could help reduce or eliminate threat exposure.

Generally, the Energy Sector as a whole stands at or near the top of interdependent critical infrastructure cascading interdependency priorities. The coordinating councils serve an important role in providing cross-sector information, but additional sector coordination could significantly reduce impact exposure in other critical sectors, assets, and missions.

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

The ES-ISAC provides essential communication and situational awareness. As part of an organization's continuity of operations plans, many organizations will identify those critical functions necessary to deliver electric power and restore systems. Organizations with mature cybersecurity programs will develop recovery time objectives for incident response and recovery operations, and incorporate these objectives into their plans and procedures. During exercises, organizations can test these recovery time objectives to see if restoration and recovery plans are effective. Maintaining the integrity of the BPS is a core goal for those organizations responsible for maintaining the system. Additionally, the ability to quickly restore and recover from an event is typically another high-level performance goal.

In addition to the CIP cybersecurity standards, NERC has also developed operational standards for the sub-sector, including the Emergency Operations Planning (EOP) standards that address operational resilience through mandated backup and recovery goals. The EOP standards complement the CIP standards and can be effectively integrated into an organization's goals of ensuring the availability of essential services.

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?

NERC reports to FERC, DOE, and other legislative and regulatory bodies with authorized oversight responsibility for NERC activity. Reporting and sharing occurs and is consistent with all applicable security classification and proprietary or commercial handling requirements pertinent under NERC's North American area of jurisdiction. Information that may be subject to sharing includes compliance oversight reports, non-compliance security dialogue, and information regarding how NERC operates and how entities interact with NERC in response to NERC activity. The ES-ISAC also routinely exchanges information with leading industry technology and services vendors.

NERC's overall reporting experience has been positive and in effect for several years. Currently, NERC is focused on aligning with established government reporting formats, encouraging greater entity-level participation in security dialogue, developing automated information exchanges, and increasing the application of data to actionable activity.

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

NERC has long developed and applied NERC standards in a transparent and effective manner; however, NERC acknowledges that new and advanced persistent threats and challenges exist. NERC—and the Electricity Sub-sector—is unique among critical infrastructure sectors by playing a leadership role in developing mandatory security standards as a part of its full body of comprehensive Reliability Standards. NERC views standards and standards-making bodies a necessary component of conformity. Standards create a baseline for stakeholders to adopt security best practices and resources into their organizations.

While technology and emerging threats are dynamic in nature, standards development and the ES-ISAC provide key tools to address new threats and vulnerabilities for the Electricity Sub-sector. All ES-ISAC activities support standards development and application. NERC and ES-ISAC subject matter experts have long participated in many of the collaborative industry, professional, and standards setting venues that inform current and emerging policies and best practices. NERC benefits from this involvement by facilitating its own sector standards development and separate compliance activity.

NERC's existing approach to standards development, technical and business feasibility management, implementation guidance, and assessment or audit guidance is comprehensive. This approach includes participation from external organizations through NERC staff and entity staff involvement. Certain threats and vulnerabilities may require that NERC develop and distribute mitigation guidance to industry in an abbreviated period of time. NERC and the ES-ISAC manage these challenges and include a response loop for industry participant conformance. The ES-ISAC has collaborated in key governmental initiatives related

to capability maturation and best practice adoption. In addition, the ES-ISAC conducts Cyber Risk Preparedness Assessments (CRPA) of NERC Registered Entities, assessing entity capability and response to cybersecurity challenges.

NERC, in conjunction with the private sector, stands ready to assist NIST in the development of the Framework, bringing technical expertise and knowledge from the Electricity Sub-sector in assessing critical infrastructure cybersecurity.

Section 2: Use of Frameworks, Standards, Guidelines, and Best Practices

As set forth in the Executive Order, the Framework will consist of standards, guidelines, and/or best practices that promote the protection of information and information systems supporting organizational missions and business functions. NIST seeks comments on the applicability of existing publications to address cybersecurity needs, including, but not limited to the documents developed by: international standards organizations; United States. Government Agencies and organizations; State regulators or PUCs; Industry and industry associations; other Governments, and non-profits and other non-government organizations.

NIST is seeking information on the current usage of these existing approaches throughout industry, the robustness and applicability of these frameworks and standards, and what would encourage their increased usage.

1. **What additional approaches already exist?**

NERC, under its authority as the FERC-designated ERO, has developed as part of its Reliability Standards, a set of CIP Standards, which are mandatory and enforceable for all "users, owners and operators" of the BPS, and hold monetary penalties for non-compliance. NERC recently finalized the CIP Standards' fifth revision (known as "Version 5"), and submitted it to FERC for approval on February 1, 2013. Once approved, and following an implementation period of approximately two years, the Version 5 standards will be mandatory and enforceable. Until that time, the prior approved version of the standards are already mandatory and enforceable, as described in the response to question #7 in the first section of these responses. In addition, as previously noted, the ES-ISAC issues alerts that provide actionable intelligence to the industry regarding cybersecurity threats and vulnerabilities.

NERC, through its Critical Infrastructure Protection Committee (CIPC), also develops voluntary guidance documents, which aid in compliance with the approved Reliability Standards, as well as address generic security concerns. NERC's CIPC has been developing and modifying guidance documents for more than 10 years, and has recently focused its efforts on providing guidance that is specific to the Electricity Sub-sector, and providing references to more generic security guidance on its website. CIPC guidance documents include:

- Threat and Incident Reporting
- Threat Alert System
- Physical Security
- Continuity of Business Processes and Operations Operational Functions

2. **Which of these approaches apply across sectors?**

While NERC's Reliability Standards are specific to the Electricity Sub-sector, many of the concepts are generic, and may be applicable to real-time process control networks and systems in other sectors.

3. **Which organizations use these approaches?**

NERC Reliability Standards apply to all "users, owners and operators" of the BPS, which is the subset of the Electricity Sub-sector that deals with reliability of the transmission network, generally including the parts of the electric grid responsible for higher voltage and larger quantities of electricity activity. As provided in Federal Power Act Section 215, the NERC Standards do not cover "facilities used in the local distribution of electric energy."

4. **What, if any, are the limitations of using such approaches?**

NERC has jurisdiction over the BPS. Its Reliability Standards apply to users, owners, and operators of the BPS; they do not apply to facilities used in the local distribution of electricity. Because the cyber threats are quickly evolving, standards cannot be the whole answer.

5. **What, if any, modifications could make these approaches more useful?**

NERC recognizes that the current threat landscape is dynamic in nature. NERC standards provide a base foundation of security, while the ES-ISAC through its alerts provides actionable intelligence on vulnerabilities to the Electricity Sub-sector. NERC is working to streamline the standards creation process to be more responsive to industry needs. The current mandatory standards are developed by industry through a consensus process applicable to a specific subset of the Electricity Sub-sector (users, owners, and operators of the BPS). The process is deliberative, utilizes industry expertise, and has mandatory compliance with possible enforcement action for non-compliance. Ensuring this structure is incorporated into the framework process in important in building on a more comprehensive approach to industry.

As a necessary complement to the standards, the ES-ISAC provides actionable intelligence to the Electricity Sub-sector through alerts. Timely sharing by the Federal government of actionable information about the threats the electricity industry and other critical infrastructure sectors are facing is critical to that effort. Additionally, organizations must develop and maintain effective cybersecurity risk management programs to address the dynamic nature of the threat. Through the RMP and the ES-C2M2,

as well as conducting CRPA exercises, NERC and industry have worked to improve risk management programs in the Electricity Sub-sector.

Recognizing these important tools, threats that rise to a national security level require a comprehensive approach by the Federal government. EO 13636 and PPD-21 take important steps, while recognizing that further topics may need to be addressed through legislation.

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

The NERC Standards were developed by, and for the use of, the Electricity Sub-sector. NERC follows an ANSI-accredited standards development process, which provides for initial development by industry stakeholders, utilizing their technical expertise, followed by commenting and balloting by interested stakeholders, primarily from the Electricity Sub-sector. Through this consensus-based process, the standards language is inherently developed to meet the needs and specificity of the members of the Electricity Sub-sector.

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

Both methods (sector-specific standards development and voluntary programs) are appropriate, but care must be taken to ensure they work together. NERC Reliability Standards are mandatory and universally applied across all relevant stakeholders within NERC's (and FERC's) jurisdiction. They provide the baseline framework on which all other standards and guidance statements are layered. Because NERC Reliability Standards are mandatory and enforceable, users, owners, and operators of the BPS must be in compliance. A second set of potentially conflicting or redundant standards will create undue hardship on the sub-sector.

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 (SSA) should align departmental priorities and resourcing towards leveraging existing vetted frameworks after gaps are identified. The SSA should work closely with the Government Coordinating Council (GCC) and Sector Coordinating Council (SCC) to facilitate support for the ISACs. The GCC/SCC, along with SSA support, should fully address executive alignment of priorities towards the following:

- Improving timely and actionable threat information sharing
- Defining sector partner organizations' roles and responsibilities
- Clarifying departmental and corporate resourcing and organizational structure and policy for enhanced security dialogue and reporting

- Providing programmatic and resource support for improved cross-sector information sharing using the sector ISACs
- Supporting sector analysis and understanding, as well as capability maturation encouragement
- Achieving leadership consensus across public-private partnerships, which drives emerging policy, implementation guidance, resource adequacy, and role definition

9. **What other outreach efforts would be helpful?**

The SSA and GCC/SCC should be involved in developing and providing executive sponsorship for a collaborative and comprehensive outreach effort. This effort would inform sector participants on key structures, policies, priorities, and approaches the sector employs. Such a campaign should be multimodal and allow participants to identify challenges, opportunities, and solutions. The SSA should then align resourcing to refined sector priorities, and publicize this information as part of the outreach content.

Section 3: Specific Industry Practices

In addition to the approaches above, NIST is interested in identifying core practices that are broadly applicable across sectors and throughout industry. NIST is interested in information on the adoption of the following practices as they pertain to critical infrastructure components:

- 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; and
- Privacy and civil liberties protection.

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

The nine practices listed in the RFI are widely used throughout the Electricity Sub-sector and addressed within the current CIP Standards. NERC Standards CIP-002 through CIP-009 provide specific actions for owners and operators to perform to protect Critical Cyber Assets that support reliable operation of the BPS. These standards recognize the differing roles of each entity in the operation of the BPS, the criticality and vulnerability of the assets needed to manage BPS reliability, and the risks to which they are exposed. Many of the concepts in the CIP Standards are generic in nature and agnostic towards specific technology regarding security solutions.

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

The new CIP Standards (Version 5) generally cover the same subject areas as both the NIST Federal Information Security Management Act framework and the ISA-99 Standards, along with the standards that they also reference. CIP Version 5 includes NIST Framework concepts such as:

1. Ensuring that all BPS cyber systems associated with the BPS, based on their function, receive some level of protection;

2. Using a tiered approach to security controls, which specifies the level of protection appropriate for systems based on their importance to the reliable operation of the BPS;

3. Tailoring protection to the mission and operating environment of the cyber systems subject to protection;

4. Defining the concept of the BPS cyber system; and

5. Including "Assess" and "Monitor" steps by adding requirement language for "identifying, assessing, and correcting" deficiencies in controls as part of the requirements' expected performance.

The NERC CIP Standards have been mapped against the existing NIST framework, as expressed in SP800-53; the technical requirements of both sets of standards address the same areas. The DHS Control Systems Security Program performed one example of a mapping document in 2009. The area where the SP800-53 control statements do not overlap is in the reporting and administrative areas (e.g., certification and accreditation), which are not required in the civilian private sector. NERC Reliability Standards generally address these areas via its compliance and audit program.

NERC Reliability Standards are mandatory and enforceable within the United States. If a requirement does not otherwise contain any qualification or exemption language, the requirement must be implemented as written in all cases, on all applicable systems, and is subject to a compliance and audit process. Guidance documents and voluntary standards, such as existing NIST and international standards, do not have these restrictions, and are therefore free to provide suggested implementation language within them.

NERC Reliability Standards are generally written as performance standards; that is, they prescribe an end-state or goal that can be measured, and attempt to not specify a technology or method for attaining that goal. The CIP standards have evolved in this practice during their development, and the Version 5 standards represent the latest step in that evolution.

An example of this process and evolution can be found in the anti-malware requirements. CIP Versions 1 through 4 require anti-malware software to run on all computer systems within a protected boundary, or else have a documented and approved exception to the requirement. Under the compliance process, even network switches qualify as computer systems that must run the anti-malware software, even though commercial anti-malware software is not available for network switches. Under Version 5, the anti-malware issues were recast as a higher-level preventative goal-oriented requirement (i.e., "deploy methods to deter, detect or prevent malicious code" and "mitigate the threat of detected malicious code") rather than requiring anti-malware software to run on every computer system within the boundary.

3. **Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?**

Practices that foster strong security, but not at the expense of grid reliability, are necessary. If the security framework that is imposed diminishes operability or reduces real-time data situational awareness, operations of the grid can be negatively impacted. Any practice that impedes the ability to successfully and safely operate the critical infrastructure will likely not be followed.

4. **Are some of these practices not applicable for business or mission needs within particular sectors?**

No. The nine listed practices are broadly applicable across both business and mission needs within the Electricity Sub-sector.

5. **Which of these practices pose the most significant implementation challenge?**

The most significant implementation challenge within the BPS is ensuring that entities adequately protect their operational systems, such as control systems, supervisory control and data acquisition (SCADA), from untrusted sources. The use of interoperable operating systems and networks has introduced a variety of threats and vulnerabilities to control systems environments. While the NERC standards require protections to be in place to secure SCADA systems, these networks are becoming more reliant on connections to third parties, such as other electric power entities or system vendors. Thus, simply segregating SCADA systems from a company's corporate networks is not sufficient. This is why NERC performs many other activities outside of standards and enforcement to provide the industry awareness and education on the dynamic risks inherent to the sector.

The most significant implementation challenge, within the listed practices above, involve the "monitoring and incident detection tools and capabilities" practice. Recent events in multiple sectors have demonstrated that Advanced Persistent Threats (APT) have significant, technically-capable personnel and sufficient resources to attack and overcome some of the most dedicated security programs in the world.

However, defenders against APT attacks are often at the other end of the scale in terms of personnel and resources, both in-house and through third parties. Threat information sharing between government and industry is extremely important, but—even with robust tools and capabilities to monitor and detect incidents within critical infrastructure controls and systems—the security threat from APTs is continually evolving with new methods of attack.

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

All Electricity Sub-sector participants that are users, owners and operators of the BPS are required to follow all NERC Reliability Standards, including the CIP standards. Entities also voluntarily follow guidance developed and issued by NERC and other organizations such as NIST, the International Society of Automation, the International Electrotechnical Commission, and the International Organization for Standards.

7. **Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards?**

Methodology practices vary in rigor and scope with the most vital Electricity Sub-sector environments having stringent change and configuration management controls based on proven IT standards as part of ensuring commitments to reliability and safety, including enforced NERC CIP standards and United States commercial nuclear 10 CFR 73.54 requirements. Factors such as associated scope, criticality and information sensitivity, compliance requirements, and unique organizational characteristics drive associated methodology practices.

8. **Do organizations have a formal escalation process to address cybersecurity risks that suddenly increase in severity?**

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 BPS 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 to which the alert was distributed
- Reporting requirements and details (if applicable)
- A set of "primary interest groups" within the receiving organization that 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

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

Risks may include sharing sensitive information regarding authorization of users accessing systems. Individuals' names are tied to the authorizations, which may raise privacy and civil liberties concerns, particularly if an incident occurs.

10. What are the international implications of this framework on your global business or in policymaking in other countries?

The interconnected BPS in North America spans the international border between the United States and Canada and that portion of the international border between the United States and Mexico for California and Baja California Norte. Because the BPS is in effect a single, very large machine, it must operate to a common set of rules. NERC has worked to establish a consistent set of standards that can function across the international boundaries. Versions of NERC's standards are now in effect in British Columbia, Alberta, Saskatchewan, Manitoba, Ontario, New Brunswick, and Nova Scotia. Those standards also apply to international power lines under the jurisdiction of the Canadian National Energy Board.

A key aspect of NERC's being recognized in Canadian jurisdictions is the ability of Canadian interests to participate in the development of NERC Reliability Standards. Continued use of the NERC standards process for standards that have impacts in Canada will be a key consideration in NERC's continuing ability to serve as the international electric reliability organization.

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

CIP-011 (information protection), within the proposed Version 5 of the CIP Standards, discusses handling sensitive information, which can extend to privacy and civil liberties. The purpose of CIP-011 is "to prevent unauthorized access to [Bulk Electric System (BES)] Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES."

Once Version 5 is approved, CIP-011 will specifically call for entities to establish Information Protection Programs to "document the circumstances under which BES Cyber System Information can be shared with or used by third parties." The standard outlines that entities should take care to distribute or share information on a need-to-know basis, establishing confidentiality agreements, non-disclosure arrangements, contracts, or written agreements. These types of arrangements may help to address risks to privacy and civil liberties.

12. In addition to the practices noted above, are there other core practices that should be considered for inclusion in the framework?

Training staff on protecting sensitive information and ensuring privacy will help to mitigate any risks to privacy and civil liberty issues. In addition, continued national level exercises such as Cyber Storm and the NERC GridEx will further assist training and information management issues with respect to cybersecurity and data protection.

Respectfully submitted,

/s/ Rebecca J. Michael

Gerald W. Cauley
President and Chief Executive Officer
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326-1001

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
charlie.berardesco@nerc.net

David N. Cook
Senior Counsel
Rebecca J. Michael
Associate General Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099– facsimile
david.cook@nerc.net
rebecca.michael@nerc.net

Counsel for North American Electric Reliability Corporation