U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Developing a Framework	**)**	
to Improve	**)**	**Docket No. 130208119-3119-01**
Critical Infrastructure Cybersecurity	**)**	
	)	

RESPONSE OF THE ISO/RTO COUNCIL TO NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY'S FEBRUARY 26, 2013 REQUEST FOR INFORMATION

OVERVIEW

The ISO/RTO Council ("IRC") respectfully submits these comments in response to the National Institute of Standards and Technology's ("NIST") February 26, 2013, Request for Information regarding the development of a framework to improve critical infrastructure cybersecurity. The IRC is composed of nine Independent System Operators ("ISOs") and Regional Transmission Organizations ("RTOs") in North America.[1] The following U.S. ISOs and RTOs are providing these comments: the California Independent System Operator ("CAISO"), Electric Reliability Council of Texas ("ERCOT"), ISO New England, Inc. ("ISO-NE"), Midwest Independent Transmission Operator System Operator, Inc. ("MISO"), New York Independent System Operator, Inc. ("NYISO"), PJM Interconnection L.L.C. ("PJM"), and Southwest Power Pool ("SPP") (collectively, the "ISOs/RTOs").

The ISOs/RTOs have been approved by the Federal Energy Regulatory Commission ("FERC"), or, in the case of ERCOT, the Texas Public Utilities Commission, to operate the electric bulk power grid within their respective state or region in accordance with tariffs, agreements, and protocols accepted by and on file with FERC or the Texas PUC respectively. The ISOs/RTOs provide open-access transmission service, administer open and competitive wholesale markets for electricity and related products, and perform system operation and planning functions for the bulk power system within their designated state or region.

The IRC appreciates this opportunity to participate in NIST's process for developing a voluntary framework to improve critical infrastructure cybersecurity. The electricity subsector oversees significant critical infrastructure and, for that reason, has been at the forefront of addressing cybersecurity for years. The ISOs/RTOs maintain

[1] The ISOs/RTOs include: Alberta Electric System Operator ("AESO"), the California Independent System Operator ("CAISO"), Electric Reliability Council of Texas ("ERCOT"), the Independent Electric System Operator of Ontrario, Inc. ("IESO"), ISO New England, Inc. ("ISO-NE"), Midwest Independent Transmission Operator System Operator, Inc. ("MISO"), New York Independent System Operator, Inc. ("NYISO"), PJM Interconnection L.L.C. ("PJM"), and Southwest Power Pool ("SPP"). AESO and IESO are not participating in these comments.

extensive risk management processes to address all risks to the reliable operation of the bulk power system within their designated state or region. Each ISO/RTO's process includes a comprehensive program to address cybersecurity risks organization-wide that draws on both mandatory and enforceable reliability standards and additional cybersecurity standards, guidelines, and best practices. Each ISO/RTO's cybersecurity program has been developed based on its specific structure, operating characteristics, responsibilities, and risk assessments.

The IRC believes that with the right formulation the NIST framework can complement and enhance existing ISO/RTOs' cybersecurity frameworks. The IRC encourages NIST to establish an overarching framework that recognizes, accommodates and complements the extensive cybersecurity standards in use within the electricity subsector. The NIST framework should facilitate the dissemination of useful information and guidance to companies, such as the ISOs/RTOs, with important cybersecurity responsibilities and promote communication concerning cyber protection across industries and between the public and private sectors. The NIST framework should not, however, create additional obligations, duplicate, or create conflicting requirements relative to the extensive standards already applicable to the electricity subsector.

Current Cybersecurity Framework for the Bulk Power System

A primary responsibility of ISOs/RTOs is to ensure the reliability of the bulk power system within their designated states or regions. ISOs/RTOs operate wholesale electric markets and use market tools, along with their operational control over the transmission system, to ensure both the security and adequacy of the bulk power system within their footprint.[2] Given their responsibility for the reliability of critical infrastructure, ISOs/RTOs have a long history of developing and complying with reliability standards, including cybersecurity requirements. The ISOs/RTOs have also collaborated with other organizations to improve sector-wide cybersecurity protection. This includes their mutually beneficial collaboration with their Sector Specific Agency ("SSA") – the U.S. Department of Energy ("DOE"). This collaboration has resulted in, among other things: the development of best practices for securing smart grid technologies, participation in federally-funded research projects to develop advanced cybersecurity technologies for the energy sector, and training exercises for advanced techniques in computer network defense.

With the Energy Policy Act of 2005, Congress directed FERC to exercise regulatory authority over the reliability of the bulk power system and specifically identified cybersecurity as one such area within FERC's charge. FERC's authority encompasses all users of the bulk power system but is circumscribed to approving and enforcing reliability standards developed by the designated Electric Reliability Organization ("ERO"). The North American Electric Reliability Corporation (NERC)

[2] Congress has defined "bulk power system" as, "(A) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and (B) electric energy from generation facilities needed to maintain transmission system reliability."

serves as the ERO for the western, eastern and Texas interconnections in the United States, Canada, and parts of Mexico.

NERC first adopted voluntary cybersecurity standards in 2003. These were replaced by NERC's Critical Infrastructure Protection ("CIP") reliability standards in 2006. The CIP reliability standards include requirements that address all major aspects of cyber protection. They were accepted by FERC as mandatory and enforceable reliability standards in 2008.

The CIP reliability standards were developed by industry stakeholders using their technical expertise and taking into account the unique needs and attributes of the electricity subsector. These standards were developed to enhance the already robust cybersecurity protection for a data-rich industry without compromising system operators' ability to reliably dispatch thousands of generating units and manage the flow of power over hundreds of thousands of miles of transmission lines in real time, during every hour of every day. Since the initial CIP reliability standards were adopted, they have been further refined several times through NERC's iterative stakeholder process to enhance their protections and clarify their requirements. Version 3 of the CIP standards is currently in place. Version 4 will go into effect on April 1, 2014, and version 5 was filed for FERC approval on January 31, 2013.

Each ISO/RTO maintains its own comprehensive cybersecurity program that draws from both the mandatory NERC CIP reliability standards and other industry standards and guidelines to ensure the reliable provision of electric service. The IRC is providing in its responses to NIST's questions below a description of ISOs/RTOs' current cybersecurity framework, noting that these responses are constrained, in some cases, by the ISOs/RTOs' obligation to protect confidential and critical infrastructure information from public disclosure.

A Model for a Complementary NIST Framework

NIST should establish an advisory umbrella framework that recognizes the existing cybersecurity frameworks already in place within the electricity subsector and other sectors. The NIST framework should make available tools and processes that will enhance the effectiveness of existing programs in all sectors. NIST should, for example, establish processes that will promote communication, collaboration, and innovation across industry sectors and between the public and private sector to address evolving cybersecurity threats. In this way, NIST can inform and promote the flexibility required for companies to respond rapidly to constantly evolving cybersecurity threats.

Specifically, NIST should address cross-sector issues such as:

- Information sharing between the government and various sectors, including the provision of actionable information regarding real-time threats and mitigation, tactics, and solutions regarding such threats;
- Similar information sharing between and among industry sectors;

- Development of and access to cybersecurity tools and information to address common cross-sector needs, including hardware and applications;
- Development of and support regarding cybersecurity processes and best practices that are potentially transferable across sectors;
- Identifying and encouraging the development of human and technology resources to meet anticipated future cybersecurity needs; and
- Focusing research and development to meet short and long term cyber protection goals.

NIST should not, however, create additional obligations or requirements that duplicate or conflict with the extensive sector-specific requirements already in place. Such additional or conflicting requirements would, at best, create an unnecessary and cumbersome administrative burden and, at worst, could impede the effective threat management it is intended to promote.

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?

The electricity subsector is at the forefront of cybersecurity protection. As described above, ISOs/RTOs already maintain extensive cybersecurity programs that draw from both mandatory and enforceable NERC CIP reliability standards and other industry standards and guidelines. These standards and guidelines were developed and are continually refined by technical experts, establish robust cybersecurity requirements that protect the transmission backbone of the United States, and ensure that the industry can reliably provide necessary electric service in real time for every hour of every day. Each ISO/RTO has developed its cybersecurity program based on its structure, operating characteristics, responsibilities, and risk assessments.

The IRC believes a substantial challenge to improving cybersecurity practices across its critical infrastructure will be the careful development of a flexible framework that recognizes and complements existing robust industry-specific cybersecurity frameworks, while providing for the coordination, communication, and leveraging of important cybersecurity information, technical expertise, and training resources among industry stakeholders, across different industry groups, and between the public and private sectors.

In addition, the IRC believes that there are additional challenges to the enhancement of critical infrastructure cyber protection that exist across all industry sectors. These challenges include:

- Companies with critical infrastructure responsibilities may lack timely access to actionable intelligence necessary to disrupt ongoing threats. Some cybersecurity threats operate outside the capabilities of most commercially-available security technology. Until actionable intelligence can be communicated at machine speed to entities with cybersecurity responsibilities, in a manner that allows machine-speed response, it will be difficult to mitigate such threats.

- Even with access to relevant information and intelligence, many entities lack access to information on effective operational and defensive tradecraft beyond what can be gleaned from generic best practice guidance or regulatory requirements. Without real operational training, access to trusted communities interested in sharing tradecraft, or access to information required to protect the relevant critical infrastructure, entities may have difficulty effectively applying those resources.

- In addition, there is a forward-looking need to recruit and train additional computer network defense professionals, whose limited numbers could undermine the effective management of cybersecurity programs. There are limited resources capable of performing the site-specific detailed security analysis necessary to uncover the activity of unknown threats. There are also limited resources available for advanced research on threats and the associated tools, techniques, practices, and ongoing activities necessary to counter them.

NIST could address these challenges through improved processes for communication and collaboration across industry sectors and between the public and private sector. In addition, it would be very helpful if NIST could identify the most important research and development priorities and highlight the policy initiatives that can promote greater consideration of best practices and development of human resources. NIST's ability to develop a cross-sector process can lead to the development of the research and development and policy/software initiatives that can best meet future cross-sector needs. By contrast, a strict industry-by-industry approach on these cross-sector issues would likely lead to sub-optimal results and a more balkanized agenda for future research and development and human resource initiatives. The IRC stands ready to help drive this cross-sector analysis through a robust NIST process.

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

The electricity subsector is subject to an extensive cybersecurity framework that draws from both mandatory and enforceable reliability requirements and other industry standards and guidelines that cover all aspects of cyber protection and are tailored to address the unique attributes of the industry. The NIST process should not add to these obligations, but rather should create an overarching framework that recognizes, accommodates, and complements the existing cybersecurity standards for the electricity subsector, while providing for improved coordination and collaboration among stakeholders within the electricity subsector, among different industry groups, and between the public and private sectors.

The NIST framework should not create static requirements that would duplicate or conflict with the existing cybersecurity framework already in use by the electricity subsector. An overly prescriptive approach to creating standards or best practice solutions that has a one-size-fits-all focus would not align well with, nor effectively address the present and future cybersecurity risks facing the electricity subsector. Such

an approach risks becoming outdated as new risks and threats are identified. Given the extensive cybersecurity framework within the electricity subsector, such a prescriptive approach would likely result in more harm than good. In addition, adding duplicate requirements will impose an administrative burden on electricity subsector members without providing additional benefit and could distract limited resources from performing their risk management functions.

A flexible, umbrella NIST framework would allow electricity subsector members to evaluate and address risks within their industry-specific contexts. In addition, an overarching framework could leverage the extensive cybersecurity work already performed and carefully refined by the electricity subsector over the past several years for the benefit of other industries. Moreover, such framework could facilitate the communication of important cybersecurity information and resources among industries and between the public and private sector.

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?

All ISOs/RTOs consider reliable operation of their critical infrastructure assets as the most important component of their respective missions. Furthermore, ISOs/RTOs consider cybersecurity to be a critical component of their overall reliability mission. Each ISO/RTO's risk management program includes a comprehensive program for addressing cybersecurity risks that draws from both the mandatory and enforceable NERC CIP reliability standards and other industry standards and guidelines. Examples of such cybersecurity requirements include:

- NERC CIP-002 R1 requires covered entities, including ISOs/RTOs, to document a risk-based assessment methodology to identify critical assets. CIP-002 R1 is the foundation of many CIP programs within the electricity subsector and defines the universe of cyber assets that fall within its CIP protection program.

- NERC CIP-002 R4 and CIP-003 R2 address senior management roles with regard to the CIP standards. The provisions require policies, senior management responsibility, direction and sign-off on ISO/RTO cybersecurity practices.

A description of applicable NERC reliability standards and other industry standards and guidelines are provided in response to Section 1: Question 7.

Each ISO/RTO has developed a cybersecurity program based on its structure, operating characteristics, responsibilities, and risk assessments. The IRC is constrained from detailing these policies and procedures by the ISOs/RTOs' obligation to protect information regarding critical infrastructure from public disclosure.

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

Each ISO/RTO's risk management program includes a comprehensive program for addressing cybersecurity risks that draws from both the mandatory and enforceable NERC CIP reliability standards and other industry standards and guidelines. The NERC CIP standards include requirements regarding the physical security of critical cyber assets and senior management's roles and responsibilities with regard to cyber security practices. A description of applicable NERC reliability standards and other industry standards and guidelines are provided in response to Section 1: Question 7.

Each ISO/RTO possesses a risk management program, although each ISO/RTO organizes its program differently based on its specific structure, operating characteristics, responsibilities, and risk assessments. The IRC is constrained from detailing these policies and procedures by the ISOs/RTOs' obligation to protect information regarding critical infrastructure from disclosure.

In addition, the IRC also has an organizational security risk management function. IRC member entities have designated representatives to form a "Security Working Group" to monitor and assess security risks that may affect multiple ISO/RTO members, or the IRC as a whole.

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

For the electricity subsector, the reliable provision of electric service is the primary goal. The most important risk metric is whether a threat or risk has the potential to impact electric reliability. Cybersecurity risks are assessed as with other risks (e.g., weather events, contact between vegetation and transmission lines, and other potentially serious disturbances) based on their potential impact to reliable operation.

Each ISO/RTO maintains a risk management program to manage risks to the reliability of the bulk power system. This includes a program for addressing cybersecurity risks that draws from both the mandatory and enforceable NERC CIP reliability standards and other industry standards and guidelines. These risk management programs include processes to identify, assess, track, and mitigate risks that may pose a threat to reliable operations.

A description of additional NERC reliability standards and other industry standards and guidelines are provided in response to Section 1: Question 7. Each ISO/RTO has developed a cybersecurity program based on its structure, operating characteristics, responsibilities, and risk assessments. The IRC is constrained from detailing these policies and procedures by the ISOs/RTOs' obligation to protect information regarding critical infrastructure from public disclosure.

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

Each ISO/RTO's risk management program includes a comprehensive program for addressing cybersecurity risks that draws from both the mandatory and enforceable NERC CIP reliability standards and other industry standards and guidelines. A description of additional NERC reliability standards and other industry standards and guidelines are provided in response to Section 1: Question 7.

Each ISO/RTO has developed a cybersecurity program based on its own structure, operating characteristics, responsibilities, and risk assessments. The IRC is constrained from detailing these policies and procedures by the ISOs/RTOs' obligation to protect information regarding critical infrastructure from public disclosure.

In addition, the IRC, itself, has a cybersecurity risk management function that is implemented through its Security Working Group.

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

Each ISO/RTO maintains a risk management program to address risks to the reliability of the bulk power system, including cybersecurity risks. These programs draw from both the mandatory and enforceable NERC CIP reliability standards and other industry standards and guidelines.

The following NERC reliability standards, including CIP, Communications ("COM"), and Emergency Preparedness and Operations ("EOP") standards, establish mandatory and enforceable cybersecurity and related requirements for users of the bulk power system:

- CIP-002: Cyber Security – Critical Cyber Asset Identification
- CIP-003: Cyber Security – Security Management Controls
- CIP-004: Cyber Security – Personnel and Training
- CIP-005: Cyber Security – Electronic Security Perimeters
- CIP-006: Cyber Security – Physical Security
- CIP-007: Cyber Security – Systems Security Management
- CIP-008: Cyber Security – Incident Reporting and Response Planning
- CIP-009: Cyber Security – Recovery Plans for Critical Cyber Assets
- CIP-010: Cyber Security – Configuration Change Management and Vulnerability Assessments
- CIP-011: Cyber Security – Information Protection
- COM-001: Communications
- COM-002: Communications and Coordination
- EOP-004: Disturbance Reporting

These reliability standards can be viewed at:

http://www.nerc.com/page.php?cid=2%7C20

In addition to NERC reliability standards, ISOs/RTOs also draw from additional industry standards and guidelines to address cybersecurity risks.

For example, ISOs/RTOs use a variety of reference frameworks, such as the Computer Security Resource Center's ("CSRC") Special Publication 800 series ("NIST SP 800") and International Organization for Standardization/International Electrotechnical Commission ("ISO/IEC") 27000 series, to structure program organization and activities at a management level. ISOs/RTOs also use these frameworks to develop processes that support ongoing operations needed to both manage risk and satisfy regulatory reporting requirements where applicable.

ISOs/RTOs use a variety of technical control references to implement their organizational risk management policy and process directives. ISOs/RTOs generally prefer to use automated data collection to measure technical risk and employ a variety of tools to baseline against those reference standards where possible. Each organization's specific risk management process dictates how that data is assessed in context.

ISOs/RTOs use varying tools to baseline and measure infrastructure-level technical security controls. These include the following:

- Commercially-available proprietary software and content for configuration security management;

- Tools that evaluate XCCDF/OVAL from the National Checklist Program where NIST's Security Content Automation Protocol ("SCAT") content is available;

- Benchmark tools and guidelines from the Center for Internet Security ("CIS");

- Reference standards and tools directly from hardware, operating system, and software vendors; and

- Open source and commercially available vulnerability assessment tools to supplement configuration baseline measurement processes.

In addition to infrastructure-level risk, ISOs/RTOs have developed additional instrumentation tools to measure technical cybersecurity risk related to software development and lifecycle management. Some ISOs/RTOs have engaged software vendors to conduct application and source code assessments for key pieces of software. ISOs/RTOs periodically engage outside assessment services companies to supplement their internal assessment programs with specialized expertise in key infrastructure areas.

ISOs/RTOs rely heavily on each other and their public sector partners at the Electric Sector Information Sharing and Analysis Center ("ES-ISAC"), Industrial Control System Cyber Emergency Response Team ("ICS CERT"), and the DOE to share and receive information on evolving threat activity and its significance to ISOs/RTOs' operational risk profiles and technical security postures. This process of information sharing across organizations and with trusted public sector partners has been mutually beneficial and has contributed significantly to ISOs/RTOs' ability to protect their critical infrastructure networks. Such information sharing is useful and should be provided for within NIST's overarching framework.

Open technical standards, such as NIST's Security Content Automation Protocol ("SCAP") and Common Vulnerabilities and Exposures ("CVE")/ Common Vulnerability Scoring System ("CVSS") are particularly useful in measuring, monitoring, and managing risk at an operational and technical level. They are also useful for expressing information about specific vulnerabilities in an unambiguous manner that supports automated assessment. Other technical standards such as Intrusion Detection Message Exchange Format ("IDMEF"), Malware Attribute Enumeration and Characterization ("MAEC"), and Open Framework for Sharing Threat Intelligence ("OpenIOC") are extremely useful for exchanging unambiguous descriptions of cyber threat information. These open and automation-oriented protocols and standards enhance real-time situational awareness and make indicator sharing a much more productive activity.

These standards not only allow integration with the defensive infrastructures, but they directly support the objective of continuous monitoring and comprehensive situational awareness through automation. Even more, these technical interoperability standards present a means to create and share important content that can be directly consumed and immediately used if distributed through a trusted channel.

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?

A. Regulatory Requirements

The electric sector is among the few industries that are subject to a regulatory structure that includes mandatory and enforceable cybersecurity standards. These standards derive from a development process that has been in place for more than 40 years to ensure that electric reliability is maintained. This had been an industry-led voluntary process with substantial industry participation, but changed substantially and became essentially regulatory in nature with the enactment of the Energy Policy Act of 2005 ("Act"). That Act added a new Section 215 to the Federal Power Act, making the industry-developed standards mandatory and enforceable through both NERC and FERC.

A notable feature is that this is a consensus-based development process. NERC develops the standards with input from stakeholders and submits the standards that it adopts to the FERC for regulatory approval, which is required for the standards to become effective. In this manner, the standards that are developed rely on the collective expertise and experience of the owners, operators, and regulators of the bulk power system and become federally enforceable. FERC periodically has sent back to NERC for revision proposed reliability standards that it has deemed insufficient. The statute prohibits FERC from proposing its own standards, but it authorizes FERC to order NERC to submit a new or modified standard if it deems it appropriate to carry out the reliability purposes of the Act.

Recent changes have improved NERC's process for enforcing its standards. Much of the enforcement of the NERC standards – including cyber-related standards – is achieved through industry self-reporting and self-auditing. A review of NERC's reported CIP violations show that a majority were brought to light by the industry's own diligence. However, NERC's past violation enforcement process was quite cumbersome, with even minor violations resulting in lengthy investigations and protracted enforcement decisions. This diverted resources away from addressing threats. NERC is addressing the problem by instituting a "find, fix, track and report" system that has resulted in a more appropriate emphasis on reliability over administrative violations.

The electric sector does not need another regulatory layer imposed on top of the existing regulatory NERC-FERC structure and other industry standards and guidelines, which could create a potential diversion from addressing risks. The IRC is concerned that the framework, even if implemented through a voluntary program as set forth in the Executive Order 13636, may take on a mandatory character – if not from the outset, then over time – by imposing additional substantive, procedural, or reporting burdens without materially improving security or contributing to electric reliability. The NIST framework should accommodate existing ISOs/RTOs' cybersecurity programs by crafting its own framework in a manner that allows the existing programs to continue to function unencumbered. Where the framework addresses issues that are not regulatory in nature and are outside the scope of the existing structure, such as information sharing, the framework should play a complementary role.

B. Reporting Requirements

NERC's CIP and other reliability standards and guidelines establish requirements for covered companies, including ISOs/RTOs, to report cybersecurity information to the following organizations:

- Federal Bureau of Investigation ("FBI"): Under NERC CIP-001-2a R4, covered entities are required to establish communication links with local FBI offices to report sabotage events. Sabotage events could include cyber incidents. ISOs/RTOs maintain appropriate communication protocols pursuant this requirement, and subject those protocols to periodically updates and testing.

- Electricity Sector Information Sharing and Analysis Center ("ES-ISAC"): Under NERC CIP-008 R1.3, covered entities must ensure that all reportable cyber Incidents are reported to ES-ISAC. ISOs/RTOs have implemented this requirement through various policies and departmental procedures to ensure that all incidents regarding CIP cyber assets are reported to ES-ISAC. ES-ISAC also provides ISOs/RTOs with periodic cyber security updates and serves as a central location for information dissemination.

- North American Electric Reliability Corporation ("NERC"), Department of Energy ("DOE"): Under NERC EOP-004, ISOs/RTOs are required to report "disturbances," including cyber-related events, to assets within their operating regions to NERC within 24 hours. As well, depending on the event type, ISOs/RTOs may also be required to report to DOE.

Certain ISOs/RTOs must also comply with other reporting requirements, including:

- Statement on Standards for Attestation Engagements No. 16
- Health Insurance Portability and Accountability Act requirements
- Payment Card Industry Data Security Standards
- Breach notification laws
- State and local statutory obligations and reporting requirements

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

The interdependence of various public services, including those mentioned above, is well known. In the rare instances where public services have been disrupted (typically related to weather incidents), the electricity subsector has identified the impacts of these interdependencies and factored them into future operations and planning requirements to minimize future disruptions. The IRC cannot publicly disclose detailed information regarding this topic due to ISOs/RTOs' obligation to protect information regarding critical infrastructure from public disclosure.

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

The primary performance goal of the electricity subsector is maintaining electric reliability – i.e., "keeping the lights on." The industry has a number of strong performance metrics that track the reliability and resiliency of the bulk power system in North America. Companies in the electricity subsector, including ISOs/RTOs, must

ensure the reliability and resiliency of the bulk power system in their state or region taking into account all reliability risk factors, including cybersecurity related risks.

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?

As described in response to Section 1: Question 8, ISOs/RTOs' reporting requirements are as follows. NERC's CIP and other reliability standards and guidelines establish requirements for covered companies, including ISOs/RTOs, to report cybersecurity information to the following organizations:

- Federal Bureau of Investigation ("FBI"): Under NERC CIP-001-2a R4, covered entities are required to establish communication links with local FBI offices to report sabotage events. Sabotage events could include cyber incidents. ISOs/RTOs maintain appropriate communication protocols pursuant this requirement, and subject those protocols to periodically updates and testing.

- Electricity Sector Information Sharing and Analysis Center ("ES-ISAC"): Under NERC CIP-008 R1.3, covered entities must ensure that all reportable cyber Incidents are reported to ES-ISAC. ISOs/RTOs have implemented this requirement through various policies and departmental procedures to ensure that all incidents regarding CIP cyber assets are reported to ES-ISAC. ES-ISAC also provides ISOs/RTOs with periodic cyber security updates and serves as a central location for information dissemination.

- North American Electric Reliability Corporation ("NERC"), Department of Energy ("DOE"): Under NERC EOP-004, ISOs/RTOs are required to report "disturbances," including cyber-related events, to assets within their operating regions to NERC within 24 hours. As well, depending on the event type, ISOs/RTOs may also be required to report to DOE.

Certain ISOs/RTOs must also comply with other reporting requirements, including:

- Statement on Standards for Attestation Engagements No. 16

- Health Insurance Portability and Accountability Act requirements

- Payment Card Industry Data Security Standards

- Breach notification laws

- State and local statutory obligations and reporting requirements

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 electric sector is subject to NERC reliability and security standards, which apply within the US, Canada, and parts of Mexico.

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; U.S. 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?

Each ISO/RTO maintains a risk management program to manage risks to the reliability of the bulk power system. These programs includes a program for addressing cybersecurity risks that draws from both the mandatory and enforceable NERC CIP reliability standards and other industry standards and guidelines.

The electric utility sector also uses other industry standards and guidelines to address cybersecurity risks, including:

- Ad-hoc and undirected approaches based on available information. Periodic assessments from outside consultants
- Industry-driven compulsory assessments, such as Statement on Standards for Attestation Engagements ("SSAE") No. 16, which address reporting on controls for service organizations
- Numerous voluntary standards such as:
    - NIST 800-137: Information Security Continuous Monitoring ("ISCM") for Federal Information Systems and Organizations[3]
    - NIST 800-53: Information Security - Security and Privacy Controls for Federal Information Systems and Organizations[4]
    - NIST Special Publication 800-53 (Rev. 3) and 800-53A (Rev. 1) Security Controls and Assessment Procedures for Federal Information Systems and Organizations[5]

[3] http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf
[4] http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf
[5] http://web.nvd.nist.gov/view/800-53/home

- NIST 800-82: Industrial Control System – Guideline to Industrial Control Systems ("ICS") Security Supervisory Control and Data Acquisition ("SCADA") systems, Distributed Control Systems ("DCS"), and other control system configurations such as Programmable Logic Controllers ("PLC")[6]

- NIST 800-39: Information Security – Managing Information Security Risk Managing Information Security Risk[7]

- NIST 1108 R2: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0[8]

- NISTIR 7628: Guidelines for Smart Grid Cyber Security[9]

- SANS Top 20 Security Controls: SANS - CSIS: 20 Critical Security Controls - Version 4.1[10]

- ISO 27000 Series Standards[11]

- DOE Guidelines C2M2

- DOE: Cybersecurity Risk Management Process ("RMP")[12]

- DOE: Cybersecurity Risk Management Process ("RMP") Guideline - Final (May 2012)[13]

- DOE: Roadmap to Achieve Energy Delivery Systems Cybersecurity[14]

Outside of these approaches, some organizations have adopted Agile software development processes to support their cybersecurity programs. Agile software development focuses heavily on rigorously defined functional specifications and automated testing to reduce operational risk caused by ongoing change. Automated unit and functional testing allows more frequent change to occur by ensuring that potential

---

[6] http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf?bcsi_scan_13fcdd49727957d3=0&bcsi_scan_filename=SP800-82-final.pdf

[7] http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

[8] http://www.nist.gov/smartgrid/upload/NIST_Framework_Release_2-0_corr.pdf?bcsi_scan_13fcdd49727957d3=0&bcsi_scan_filename=NIST_Framework_Release_2-0_corr.pdf

[9] http://www.egov.vic.gov.au/focus-on-countries/north-and-south-america-and-the-caribbean/united-states/trends-and-issues-united-states/information-and-communications-technology-united-states/cyber-security-united-states/nistir-7628-guidelines-for-smart-grid-cyber-security.html

[10] http://www.sans.org/critical-security-controls/guidelines.php

[11] http://www.27000.org/

[12] http://energy.gov/oe/services/cybersecurity/cybersecurity-risk-management-process-rmp

[13] http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf

[14] https://www.controlsystemsroadmap.net/Pages/default.aspx

functional failures are identified quickly. A management process that encourages and enables rapid low-risk change also enables security patches, configuration changes, and infrastructure changes to occur at a rapid pace.

Some organizations have also adopted an Infrastructure as a Service, Platform as a Service, Software as a Service ("IaaS/PaaS/SaaS") cloud approach to infrastructure management in support of their security programs. These approaches use high levels of virtualization and automation to rapidly assemble and build entire application clusters. The automation capabilities inherent in private cloud infrastructures also afford high levels of security automation. Furthermore, this approach to enable rapid infrastructure building, measured in minutes and seconds, also increases operational resilience by allowing infrastructure managers to tear down and rebuild failed infrastructure, or redeploy known good versions of corrupted infrastructure into a known clean location. If resources are available, there is no reason this approach could not be considered as a security tool as well.

2. Which of these approaches apply across sectors?

Several of the voluntary standards listed above can and do apply across sectors. The NERC CIP reliability standards are specific to the electricity subsector. However, most of the concepts contained in the NERC CIP reliability standards are considered prevailing, accepted security practices and, therefore, may be applicable in other sectors.

3. Which organizations use these approaches?

Each ISO/RTO's program for addressing cybersecurity risks draws from both the mandatory and enforceable NERC CIP reliability standards and other industry standards and guidelines. All "users, owners and operators" of the bulk power system, which is the subset of the electricity subsector, are subject to mandatory compliance with the NERC CIP reliability standards. Compliance with those standards is monitored and enforced by NERC through authority delegated by FERC. The ISOs/RTOs also reference NIST and ISO 27000 series and other industry standards and guidelines for guidance.

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

In developing their cybersecurity programs, ISOs/RTOs rely on a variety of standards and guidelines. An overemphasis on any particular approach as a one-size-fits-all solution would create difficulties in adapting to specific risk scenarios. Any approach that fails to account for rapidly changing adversarial action and changes in tactics, techniques, and procedures will fail to mitigate any risk over time and will consume resources better allocated elsewhere.

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

Any approach adopted by NIST must focus more on enabling data-driven risk decision making than on delivering reports. Useable site-specific detail can better inform risk-based decisions on protective strategies, tactics, and operational processes.

NIST's adoption of a voluntary consultative approach that guaranteed, by law, the privacy of and non-attribution to the participating entity could encourage engagement. Having a neutral, trusted, disinterested, and technically-adept 3rd party could provide context and expertise necessary for an entity to develop action plans and help mitigate risks. Voluntary approaches should also include education, training, and access to tools and other resources as incentives.

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

For purposes of the electricity subsector, the NERC standards development process is sector-specific and is driven by input from sector stakeholders. NERC's American National Standard Institute ("ANSI") accredited stakeholder process allows for multinational and organizational development of the standards. This process could service as a template for the development of the NIST framework.

NERC reliability standards are developed according to the NERC Standard Processes Manual. According to NERC, the standards development processes "provide reasonable notice and opportunity for public comment, due process, openness, and balance of interests in developing a proposed Reliability Standard consistent with the attributes necessary for ANSI accreditation." Consistent with this description, NERC lists the following essential attributes of NERC standards development processes:

- Open Participation
- Balance
- Coordination and harmonization with other American National Standards activities
- Notification of standards development
- Transparency
- Consideration of views and objections
- Timeliness
- Consensus Building
- Consensus vote

This consensus-centric approach leads to standards designed to meet sector-specific needs of those operating the bulk power system. As NIST develops the cybersecurity framework, the IRC encourages NIST to incorporate many of the principles set forth in the NERC Standard Processes Manual.

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

Each sector (or sub-sector, as the case may be) should have the opportunity to shape any potentially applicable cybersecurity framework based on the realities of operating in that sector and the business needs of the firms in that industry. Given the existing cybersecurity framework in the electricity subsector, voluntary programs are preferred.

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

Sector-specific agencies ("SSAs") are and should retain their leading position regarding the security of their respective sectors. SSAs can serve as a valuable resource in facilitating the following:

- Information Sharing - The rapid dissemination of the information into organizations for analysis and implementation would be a key improvement to address cybersecurity threats.

- Technology Expertise and Research Capabilities – SSAs can provide expertise and capabilities to develop a better understanding of sector-specific technological vulnerabilities and their appropriate countermeasures. For example, the DOE National SCADA Test Bed program has applied such capability to improve cybersecurity at the vendor and product level. The DOE also makes available technology experts through its Work For Others program to provide consultative engagements that help Critical Infrastructure and Key Resource Asset Owners and Operators mitigate specific vulnerabilities within their networks.

- Security Clearances - Providing additional critical sector security clearances and expediting the process to allow more levels of access to address operational events.

- Background Checks - National background check processes including the FBI and international databases are elements that could aid in securing access to critical infrastructure.

9. What other outreach efforts would be helpful?

As part of the NERC CIP standards, covered entities within the electricity subsector, including ISOs/RTOs, are required to report cybersecurity and other reliability information to certain organizations, including the FBI, NERC, and the ES-ISAC. Transmitting information to the appropriate organizations where it can be further disseminated and action taken upon it is an important component of cybersecurity. However, a more robust system of information sharing is needed to confront the evolving nature of cyber-threats. For example, organizations responsible for critical

infrastructure require better real-time sharing of actionable information pushed to the organizations, and improved sharing of information among industries and between the private and public sectors.

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?

ISOs/RTOs incorporate most of these practices into their cybersecurity programs. However, privacy and civil liberties considerations for the most part are inapplicable to ISOs/RTOs. Other than information related to ISO/RTO personnel, ISOs/RTOs typically do not have consumer information. Thus, ISOs/RTOs' security practices largely do not raise privacy or civil liberties concerns.

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

The electricity subsector is subject to the NERC reliability standards, including the NERC CIP reliability standards, the scope of which extends into Canada and Mexico. The NERC CIP reliability standards touch on several of the practice areas described above, including:

- Separation of business from operational systems
- 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

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

The cybersecurity practices described above are all important. Each ISO/RTO might prioritize the practices somewhat differently based on its risk assessment experiences and configuration of security programs. Electric reliability is the key focus

of the ISO/RTOs' risk management programs. ISOs/RTOs view these cybersecurity practices through that lens, as well as through the lens of other responsibilities, such as operation of wholesale electricity markets.

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

Privacy and civil liberties considerations for the most part are inapplicable to ISOs/RTOs. Other than information related to ISO/RTO personnel, ISOs/RTOs typically do not have consumer information. Thus, ISOs/RTOs' security practices largely do not raise privacy or civil liberties concerns.

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

Each ISO/RTO faces different implementation challenges based on its particular risks and required actions.

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

For the electricity subsector, the reliable provision of electric service is the primary goal. Each ISO/RTO maintains a risk management program to manage risks to the reliability of the bulk power system, including a program for addressing cybersecurity risks that draws from both the mandatory and enforceable NERC CIP reliability standards and other industry standards and guidelines. The risk management programs cover the cybersecurity practices described above.

As described above, the electricity subsector is required to comply with the NERC CIP reliability standards and also assess and implement other standards, guidelines, and best practices based on business requirements and risks assessments. Control guidelines and reference frameworks, such as ISO 2700X and NIST SP 800-53/A, are used as management-level models for governance and process controls. ISOs/RTOs adapt these practices to their needs by implementing specific processes and procedures. ISOs/RTOs further refine these processes to ensure compliance with mandatory standards. The use of these reference frameworks provides additional support.

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

Each ISO/RTO has a methodology in place to allocate resources for IT standards, though that methodology varies by ISO/RTO based on their specific business requirements and risk assessment. In general, ISOs/RTOs include regular planning as part of their cybersecurity programs to identify resource needs, including needs for IT standards. At a minimum, ISOs/RTOs annually review and approve procedures necessary to support mandatory compliance controls.

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

Each ISO/RTO addresses this concern differently according to its local business needs. Each ISO/RTO has a cybersecurity program that includes local incident management, proactive threat management, and vulnerability management. Escalation activities follow organization-specific procedures according to the nature and severity of the risk.

NERC CIP reliability standards (CIP-008-3, R1.1-1.3) require regulated entities to establish incident classification and reporting criteria, formalize incident response actions, roles and responsibilities, and report these incidents to the Energy Sector Information Sharing and Analysis Center ("ES-ISAC"). Furthermore, these standards (CIP-001-2a, R3) require regulated entities to report suspected cybersecurity sabotage events to federal (FBI) or national (Royal Canadian Mounted Police – "RCMP") law enforcement and other appropriate parties within their interconnects or control areas. Finally, the standards (EOP-004-1) require regulated entities to report disturbance events, which could include cybersecurity events, to NERC, the relevant NERC regional entity, and the Department of Energy.

In addition, the electricity subsector supplements public information sources and standard vendor support with sector-specific resources, including ES-ISAC, US-CERT, ICS-CERT, industry associations, and sector-specific vendors to ensure timely access to new threat and vulnerability information. Certain companies within the utility industry also engage outside private sector firms for threat and vulnerability information.

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

Privacy and civil liberties considerations for the most part are inapplicable to ISOs/RTOs. Other than information related to ISO/RTO personnel, ISOs/RTOs typically do not have consumer information. Thus, ISO/RTO security practices largely do not raise privacy or civil liberties concerns.

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

Business activities of some ISOs are coordinated with Canadian and Mexican organizations. The NERC reliability standards extend to entities in Canada and parts of Mexico.

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

Privacy and civil liberties considerations for the most part are inapplicable to ISOs/RTOs. Other than information related to ISO/RTO personnel, ISOs/RTOs typically do not have consumer information. Thus, ISO/RTO security practices largely do not raise privacy or civil liberties concerns.

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

NIST should address the following practices in developing its umbrella framework:

- organizational awareness and education;
- workforce development through academic education or training programs;
- cooperative research and development regarding cybersecurity technologies and their application;
- vulnerability/application assessment and secure software development techniques;
- robust IT monitoring and rapid change management to reduce operational risk from vulnerability mitigation and to allow faster deployment of patches and other fixes;
- information sharing for threat indicators, analytical techniques, and operational tradecraft; and
- network and host forensics to gather threat indicator data from recovered artifacts.

Respectfully submitted,

/s/ Nancy Saracino
Nancy Saracino
General Counsel
Anthony Ivancovich
Deputy General Counsel, Regulatory
Anna McKenna
Assistant General Counsel, Regulatory
California Independent System Operator Corporation
151 Blue Ravine Road
Folsom, California 95630
amckenna@caiso.com

/s/ Carl F. Patka
Carl F. Patka
Assistant General Counsel
Raymond Stalter
Director of Regulatory Affairs
New York Independent System Operator, Inc.
10 Krey Blvd.
Rensselaer, New York 12144
cpatka@nyiso.com

/s/ Matthew Morais
Matthew Morais
Assistant General Counsel
Electric Reliability Council of Texas, Inc.
7620 Metro Center Drive
Austin, Texas 78744
mmorais@ercot.com

/s/ Paul Suskie
Paul Suskie
Senior Vice President, Regulatory Policy and General Counsel
Southwest Power Pool
201 Worthen Drive
Little Rock, Arkansas 72223-4936
(501) 688-2535
psuskie@spp.org

/s/ Theodore J. Paradise
Theodore J. Paradise
Assistant General Counsel, Operations
And Planning
John Galloway
Manager, Cybersecurity
ISO New England Inc.
One Sullivan Road
Holyoke, Massachusetts 01040
tparadise@ise-ne.com

/s/ Craig Glazer
Craig Glazer
Vice President-Federal Government Policy
PJM Interconnection, L.L.C.
Suite 600
1200 G Street, N.W.
Washington, D.C. 20005
202-423-4743
glazec@pjm.com

/s/ Stephen G. Kozey
Stephen G. Kozey
Vice President, General Counsel, and
Secretary
Midwest Independent Transmission
System Operator, Inc.
P.O. Box 4202
Carmel, Indiana 46082-4202
skozey@midwestiso.org