



Randy D. Crissman
Vice President
Technical Compliance
Operations

914.681.6471
914.469.2965 (Cell)
914.681.6534 (Fax)
randy.crissman@nypa.gov

April 8, 2013

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

**RE: NIST Docket No. 130208119-3119-01
Comments of the New York Power Authority in Response to NIST Request for
Information on Developing a Framework to Improve Critical Infrastructure
Cybersecurity**

Dear Ms. Honeycutt:

The New York Power Authority (NYPA) hereby respectfully submits these comments in response to the notice and request for information (RFI) on “Developing a Framework to Improve Critical Infrastructure Cybersecurity” issued on February 26, 2013 by the National Institute of Standards and Technology (NIST).¹

Introduction

On February 26, 2013, the NIST issued an RFI to facilitate a voluntary set of standards and best practices to guide industry in reducing cyber risks to the networks and computers that support critical infrastructure vital to the nation’s economy, security and daily life. NYPA fully supports NIST’s effort to gather data in furtherance of establishing a robust national framework to assess the effectiveness of critical infrastructure protection and to establish best industry practices. The electric sub-sector is already subject to Section 215 of the Energy Policy Act of 2005 which dictates comprehensive rules and requirements for cybersecurity and critical infrastructure protection mandates. The answers submitted herein are not exhaustive and rather are intended to provide an overview of how critical assets are currently being managed and regulated. NYPA also supports the joint comments submitted in response to the RFI by the Electric Trade Associations in response to the RFI.

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

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

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 greatest challenges to improving cybersecurity practices across critical infrastructure are timely and complete communication of cybersecurity threats, management of economic costs, and improvement of supply chain issues and monitoring of vulnerabilities. With regard to communication, Industrial Control System (ICS) Engineers must work more closely with Corporate Information Technology (IT) groups to improve the security posture of the industry. At NYPA, IT and ICS groups meet regularly to formulate improvements to our cybersecurity programs. With regard to economic costs, the development of cost effective solutions should be optimized and the costs of unfunded mandates should be considered, as they may have a great financial impact on ratepayers, consumers and smaller businesses. With regard to supply chain issues, ICS vendors should be required to adhere to the same security standards as customers and vendors must be required to deliver secure solutions and ultimately should be certified pursuant to established standards to meet minimum requirements. The goal should be a unified and fully integrated corporate approach to proactively managing cybersecurity challenges which minimizes system unavailability and improves workforce development and training to mitigate social engineering, phishing and other threats.

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

The greatest challenges in developing a cross-sector standards-based framework for critical infrastructure are costs, effective communication and ensuring standards remain relevant across the different sectors. In order for a common standards-based framework to be applicable and adaptable across multiple sectors, it needs to be flexible so that each industry can develop and implement appropriate security controls for its industry. The cyber security standards that the electric sub-sector has been using for more than a decade provides an adaptable standards-based approach built on best practices and national and international guidelines. The challenge for each sector is to develop a properly tailored and carefully designed risk methodology for determining and identifying critical systems based on risk or impact to the sector that are flexible enough to accommodate breakthroughs and new information and formalized enough to have sufficient strength but not be too prescriptive.

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?

NYPA has developed a rigorous governance program for cyber security with internal controls, including policies and procedures, which are communicated from the highest levels of the organization to all employees and contract personnel. All of the applicable policies and procedures are easily accessible through NYPA's intranet, which regularly advertises changes to the policies and procedures. In general, best practices of organizations with

robust programs utilize internal and external subject matter expertise on a continual basis for evaluating and improving policies and procedures to identify and address new risks and vulnerabilities as they are discovered. NYPA regularly reviews and updates its Enterprise Risk policies and procedures to ensure risk management activities are appropriate to the organization and aligned to best practices. NYPA's Executive Risk Management Committee is comprised of senior managers responsible for reviewing and approving Enterprise Risk policies and procedures and is the controlling authority responsible for risk management activities.

4. Where do organizations locate their cybersecurity risk management program/office?

NYPA's Information Technology and Real Time Operations Groups practice and facilitate management of cybersecurity risks and have responsibility for compliance with cybersecurity standards and policies. The NYPA Internal Audit group performs periodic audits on Information Technology systems and the industrial control systems. The NYPA Reliability Standards & Compliance Group performs internal compliance assessments against the standards-based cyber security practices of the Industrial Control Systems. Both Internal Audits and Reliability Standards and Compliance provide recommendations to Senior Management.

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

Operational cybersecurity risks are defined as operational risks to information and technology assets that have consequences typically affecting the Confidentiality, Integrity or Availability (i.e. the CIA triangle) of subject matter information or systems. On an enterprise level, NYPA defines risk as any uncertainty that could materially impair or enhance its ability to carry out its mission objectives. NYPA uses a risk-based methodology to define, assess and mitigate risk. This methodology was designed by NYPA staff working in conjunction with third party subject matter experts.

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

Cybersecurity risk mitigation is an integral part of overall enterprise risk management within NYPA. Organizations with robust programs typically examine risk through a holistic approach, ensuring that resources are adequately deployed to the areas deemed the highest risk (evaluated at least annually). The greatest challenges in developing a cross-sector standards-based framework for critical infrastructure are costs, effective communication and ensuring standards remain relevant across the different sectors. Smaller organizations or those with limited geographical reach generally team with similarly situated organizations in creating programs with an extended breath that would otherwise be difficult to create unilaterally due to limited resources.

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

- NERC Critical Infrastructure Protection (CIP) standards
- NYS DHS cyber security standards
- NIST SP 800 guidelines
- SANS security practices
- ES-ISAC best practices
- MS-ISAC best practices
- Enterprise – COSO Enterprise Risk Management framework

Some of the tools and practices in use include:

- Firewalls
- Network segmentation
- Intrusion Detection System
- Two-factor authentication
- Anti-virus protection
- Security vulnerability and patch monitoring service
- Security event monitoring service and call-out

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?

- NERC CIP standards
- NYS Executive Law 715 regarding the Office of Cyber Security
- NYS Security Breach and Notification Act
- FPA Section 215 / Audits
- Section 215 of the Federal Power Act made compliance with reliability standards mandatory and enforceable on users of the Bulk Power System. NERC, as the Electric Reliability Organization designated by FERC pursuant to Section 215(c) of the Federal Power Act has the legal authority to monitor and enforce compliance with NERC Reliability Standards and to impose, subject to FERC oversight, penalties or sanctions for non-compliance.

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

The Supervisory Control and Data Acquisition (SCADA) systems, peripherals and other support equipment are highly specialized electromechanical and telemetric systems and key to the monitoring and controlling the critical infrastructure associated with the energy, water and transportation sectors. Critical assets in the electric sub-sector that are potentially interdependent on the communications and transportation sectors include industrial control systems, energy marketing and management systems, as well as generation, transmission and distribution systems. Such critical assets remain dependent on non-specialized computing systems to handle organizational management and communications (i.e. feeds to business systems), which vastly complicates the implementation of the physical and electronic controls required for their operational protection without excessive impact.

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

Organizations have adopted Key Performance Indicators, Service Level Agreements, and Disaster Recovery and Business Continuity programs that include recovery time objectives. In addition, regular testing is conducted to ensure that the plans are accurate, effective, and the processes are working and relevant to the business goals of the organization as well as measured response goals for validating the existence of robust controls through internal and external testing of critical infrastructure on a continual basis, with an added level of randomness to simulate risks. NERC has also developed operational reliability standards for the electric sub-sector including the Emergency Operations Planning (EOP) standards that address operations resilience through mandated backup and recovery goals. The EOP standards compliment the CIP standards.

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?

NYPA is subject to the NERC reliability standards and FERC oversight. This regulatory framework includes both internal and external routine audits of critical infrastructure and cyber assets identified pursuant to the relevant NERC and FERC policies, standards and regulations. In addition, NYPA is subject to the Department of Homeland Security Office of Cybersecurity requirements and standards.

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

A robust national regulatory framework currently exists established by FERC pursuant to section 215 of the Federal Power Act. In this framework, NERC plays an important role as facilitator of industry-wide reliability standards concerning cybersecurity and critical infrastructure protection. Maintaining and complying with such standards is integrated into the daily work routines of the real-time, ICS operations groups. The practices, which are addressed by the NERC CIP standards for the electric sub-sector, can be found within the International Standards Organization 27000 (ISO 27000) series cybersecurity practices from the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC).

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 Public Utility

Commissions; 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. Please provide information related to the following:

1. What additional approaches already exist?

NERC, in its capacity as the Electric Reliability Organization (ERO), has developed as part of its reliability standards, a set of Critical Infrastructure Protection (CIP) standards, which are mandatory and enforceable for all “users, owners and operators” of the Bulk Electric System (BES) and hold monetary penalties for non-compliance.

The ES-ISAC issues alerts to provide actionable intelligence to the industry on cybersecurity threats and vulnerabilities (NERC Alerts).

NERC, through its Critical Infrastructure Protection Committee (CIPC), also develops voluntary guidance documents which are used to aid in compliance with the approved reliability standards as well as to 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 electric 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
- ISO 27000
- Department of Homeland Security

In addition to established NERC CIP standards for the electric sub-sector guidance, regulations and standards are applicable as per International Standards Organization 27000 series cybersecurity practices from the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC) as well as pursuant to the Department of Homeland Security.

2. Which of these approaches apply across sectors?

While NERC’s Reliability Standards are specific to the electric sub-sector, many of the concepts are generic and may be applicable to real-time process control networks and information systems in other sectors. The primary specificity to the electric sub-sector is in the consideration of a methodology for identification of critical systems. These were derived from the International Standards Organization 27000 series.

3. Which organizations use these approaches?

With respect to the electric sub-sector, the NERC Reliability Standards apply to all “users, owners and operators” of the Bulk Electric System, which 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.

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

The CIP standards, pursuant to Section 215 of the Federal Power Act apply to users, owners and operators of the Bulk Electric System. They do not apply to “facilities used in the local distribution of electric energy.” The DOE ES-C2M2 and Risk Management Process (RMP) guidelines apply to the entire electric sub-sector, which includes entities involved in the generation, transmission, distribution and marketing of electricity.

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

Owners, operators and users of the Bulk Electric System participate and are subject to the requirements of NERC’s ES-ISAC alert system. This program may be substantially enhanced when federal agencies coordinate the release of timely information possessed by the government regarding existing and emerging threats. In addition, Version 5 of the CIP standards, soon to be approved by FERC, is more comprehensive than Version 4 and should be adopted. It appears to address many of the issues and concerns voiced by the electric sub-sector. The cost of such programs should be balanced between the Utility/Private Industry and the Government.

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

The ISO 27000 Standards were the basis for the NERC CIP standards, which were written by electric sub-sector experts, for the electric sub-sector. The working groups supported by NERC allow the industry to craft standards that will help secure and maintain critical infrastructure. The NERC standards take into account the sector-specific needs by setting guidance and a framework for the identification of critical systems and the application of security controls based on risk and impact to the Bulk Electric System.

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

The NERC reliability standards are mandatory. While there is a role for supplementary practices needed in order to respond to emerging threats, creation of an additional superfluous set of potentially conflicting standards would only serve to obfuscate the established model.

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

They can offer the needed technical support and guidance when requested.

9. What other outreach efforts would be helpful?

Ensure that vendors are accountable to provide secure appliances and systems for Industrial Control Systems. Such vendors must be held accountable for secure solutions and minimal standards consistent with best industry practices.

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;
- Privacy and civil liberties protection.

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

- Separation of business from operational systems:
 - The most common management structure at present is that of separation of business and operational networks. Some utilities are moving towards a single Security Department, reporting to the Chief Operating Officer or Risk Officer.
- Use of encryption and key management:
 - Where technically feasible, this is implemented on the critical cyber assets, per the NERC CIP standards
- Identification and authorization of users accessing systems:
 - Yes, per the NERC CIP standards
- Asset identification and management:
 - Yes, per the NERC CIP standards
- Monitoring and incident detection tools and capabilities:
 - Yes, per the NERC CIP standards
- Incident handling policies and procedures:
 - Yes, per the NERC CIP standards
- Mission/system resiliency practices:
 - Yes, per the NERC CIP standards
- Security engineering practices:

- Yes, per the NERC CIP standards and good business practice
- Privacy and civil liberties protection:
 - NYPA adheres to best industry practices.

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

The practices, which are addressed by the NERC CIP standards for the electric sub-sector, can be found within the International Standards Organization 27000 series cybersecurity practices from the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC). The CIP standards apply to the same subject areas as both the NIST FISMA framework and the ISA-99 Standards, together with the standards they reference.

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

Critical practices are those that strengthen security without impeding system reliability. If the security framework that is imposed diminishes operability or reduces real-time data situational awareness, operations of the grid can be negatively impacted. Similarly, critical to the secure operation of critical infrastructure, is the “separation of business from operational systems” for the secure operation of critical infrastructure. The implementation of this practice can greatly reduce the overall attack surface.

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

All of these practices are applicable.

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

The most significant challenge is asset identification and management. The electric sub-sector encompasses many categories of systems that are now ‘Internet Protocol (IP) Ready’. Accordingly, the added connectivity and control options that result in being ‘IP Ready’ may ultimately pose a significant cyber security control risk for such equipment. This is further complicated by the fact that identifying which of the assets present the most significant risk, is often purely dependent on how that equipment is configured for specific applications.

The use of encryption and key management should be approached with caution. Due to the latency and legacy system limitations, the introduction of robust encryption practices can hinder the required availability of systems. Many components of an industrial control system have traditionally limited processing speed and memory with sub-millisecond response requirements; the introduction of traditional encryption methods can result in adverse effects to power operations.

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

Existing energy sector standards are the result of significant effort by numerous Federal agencies, industry consortiums and private/public entities working together in evaluating

definitive risk versus the cost needed to improve and secure daily operational practices. The regulatory compliance framework has evolved and has continually improved. The most recent version of the NERC CIP Standards, pending final FERC approval, represent a further step in refining controls that will have measurable benefit to the electric sub-sector.

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

NYPA has such a methodology in place.

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

Pursuant to its compliance with the NERC CIP-008 standard, NYPA has in place a formal escalation process. In addition, NYPA has a layered security system that is monitored twenty-four hours a day seven days a week and maintains a well-tested escalation process.

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

Privacy and civil liberties are important and rules and regulations applicable thereto must be followed. The electric sub-sector is driven by reliability and security balanced with privacy and civil liberties concerns.

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

NYPA does not maintain a global footprint.

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

The CIP-011 standard in Version 5 of the CIP standards, which will soon be approved by FERC, addresses information sharing and the handling of sensitive information which extends to privacy and civil liberties. The sharing of sensitive information may raise privacy issues and the appropriate protective mechanisms should be established to protect individual liberties when practicable or required.

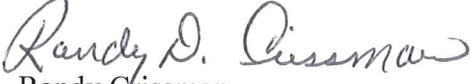
12. In addition to the practices noted above, are there other core practices that should be considered for inclusion in the framework?

Supply chain vendors should be made to adhere to minimal industry standards and best practices and such security standards should apply to all entities and businesses providing hardware, software or any other infrastructure to US markets, particularly hardware from China.

Conclusion

NYPA appreciates the effort of the Administration and NIST to improve cybersecurity protections and looks forward to working with the administration to improve the energy sector.

Respectfully submitted,


Randy Crissman
New York Power Authority