Salt River Project
P.O. Box 52025
Mail Stop: CUN204
Phoenix, AZ 85072-2025
Phone: (602) 236-6011
Fax: (602) 629-7988
James.Costello@srpnet.com

James J. Costello
Director, Enterprise IT Security

April 8, 2013

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

RE: NIST Docket No. 130208119-3119-01
Comments of the Salt River Project
Request for Information on "Developing a Framework to Improve Critical Infrastructure Cybersecurity."

Dear Ms. Honeycutt:

The Salt River Project Agriculture Improvement and Power District ("SRP") appreciates the opportunity to respond to the National Institute of Standards and Technology ("NIST") February 26, 2013 Request for Information (RFI). The NIST RFI seeks to gather information to facilitate development of a voluntary set of standards and best practices to guide industry in reducing cyber risks.

SRP is an electric utility serving nearly one million customers in the Phoenix metropolitan area. In FY 2010-11, our customers used more than 26 million MWh of electricity and hit a retail peak demand of 6,350 MW. SRP's diverse resource portfolio includes nuclear, coal, gas, large hydro, small hydro, wind, solar, geothermal, biomass, landfill gas, demand response programs and energy efficiency initiatives.

SRP supports NIST's effort to develop an appropriate framework to better understand and improve cybersecurity practices across critical sectors of our nation's economy. SRP provides the following comments 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 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?

There are a number of challenges to improving cybersecurity practices across critical infrastructure including: the sharing of actionable information by governmental entities with industry; the introduction of traditional Information Technologies ("IT") technologies into the operational environment and the potential for duplicative and conflicting regulatory oversight. First, we recognize and appreciate recent efforts of the Department of Homeland Security ("DHS") and the Department of Energy ("DHS") to provide better access to threat and vulnerability information. We believe, however, that more must be done. North American Electric Reliability Corporation's ("NERC") Electricity Sector - Information Sharing and Analysis Center ("ES-ISAC") provides a framework that can be built upon to accomplish this goal. The ES-ISAC is a valuable source of reliable information but efforts should be made to improve the content of the information provided to enable entities to appropriately secure their systems.

Second, while providing significant benefits (e.g., remote communication, opportunities for improved security, and structured procedures), the introduction of traditional IT technologies into the operational environment also carries risk. The complexity and pace of technological changes creates risk for the operational areas such as missing security patches, identified system vulnerabilities and potential unauthorized remote access. Additionally, industrial control systems devices tend to have a lifespan of 10-20 years before being replaced creating an environment that is difficult to implement and maintain robust cybersecurity controls similar to traditional IT environments.

Lastly, the potential for conflicting regulatory regimes as to the electric sector is a significant concern. SRP is subject to applicable mandatory reliability standards that address cybersecurity developed by NERC and approved by the Federal Energy Regulatory Commission ("FERC"). The framework being developed through this process should encompass the existing standards and not create conflicting regimes. Improper coordination of the existing NERC Critical Infrastructure Protection ("CIP") regulation with another layer of NIST-based cybersecurity standards could duplicate efforts, cause possible conflicts and complicate cybersecurity work.

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

The greatest challenge for implementing a cross-sector standards-based framework for critical infrastructure is acceptance from the industries in-scope. Although there are clear commonalities in the types of devices each industry uses and the risks associated with the technology in use, each sector may point to their individual nuances to create distance between them and any cross-sector standards-based framework. The argument being any "one-size-fits-all" approach to cybersecurity will miss the individual requirements that only apply to their specific sector. To overcome this concern the NIST framework should be sufficiently flexible to address needed concerns but apply in multiple scenarios by addressing cybersecurity configurations and control points, not the specific technology or equipment used to implement it.

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?

SRP is structured with a formal Risk Management Department responsible for evaluating safety, physical security and operational risk. Risk Management procedures are developed to manage and guide corporate standards related to these specific business processes and areas.

Cybersecurity risk is captured within a set of enterprise cybersecurity policies and standards. These standards contain standard-content from industry frameworks [i.e., NIST, International Organization for Standardization ("ISO"), Information Technology Infrastructure Library ("ITIL")] and applicable regulations [i.e., NERC CIP]. The cybersecurity policies and standards establish parameters around Information Technology ("IT") and Operational Technology ("OT") system configurations, cybersecurity-related personnel procedures around operational responsibilities.

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

The Cybersecurity Risk Management Program at SRP resides within the Enterprise IT Security department. The function reports up to the Chief Financial Executive within the Financial and Corporate Services business unit.

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

The organization assesses cybersecurity risk by applying elements of the NIST 800 Special Publication guidance documents. These documents outline a risk management methodology that evaluates each organization's internal IT and OT systems based on criticality. Based on this categorization process, cybersecurity controls are applied to the environment and assessed to determine their effectiveness. These assessment results are collected and responsible stakeholders accredit the assessment results to establish a security baseline that then will be used to validate improvement over a period of time. The risk management methodology is captured below:

- CATEGORIZE Information System
- SELECT Security Controls
- IMPLEMENT Security Controls
- ASSESS Security Controls
- AUTHORIZE Information System

- MONITOR Security Controls

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

At SRP, cybersecurity risk management is performed by the Enterprise IT Security department with close partnership with the key business units. Cybersecurity assessment efforts are prioritized and coordinated based on system criticality.

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

The industry standards and guidance documents used to understand, measure, and manage risk at the management, operational, and technical levels include:

- NERC CIP Standards
- NIST 800-37: Guide for Applying the Risk Management Framework.
- NIST 800-39: Managing Information Security Risk
- DOE ES-RM: Electricity Subsector Cybersecurity Risk Management Process
- DOE ES-C2M2: Electricity Subsector Cybersecurity Capability Maturity Model

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 primary regulatory requirements that apply to the electric sector are the NERC CIP standards. These standards require a set of cybersecurity standards to be implemented to critical infrastructure as defined under NERC CIP. The standards are outlined below:

- 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

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

SRP is dependent in some part on the telecommunications, the financial services and the transportation sectors.

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

SRP follows the following standards and performance indicators to ensure a consistent and comprehensive approach to managing cyber risk:

- Capability Maturity Model Integration (CMMI)
- Internal Controls for technology systems
- Business Continuity Planning and Disaster Recovery processes in coordination with applicable standards and regulations (NIST 800-53, NERC CIP, etc.)
- Metrics reporting for Management and visibility of enterprise risk posture

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?

SRP reports to NERC under the mandate of NERC CIP standards. NERC completes CIP audits on a tri-annual cycle to evaluate responsible entities compliance. NERC reports up to FERC on compliance efforts within its jurisdiction.

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

Use of national cybersecurity industry frameworks (e.g., NIST, ISO) – in addition to NERC CIP – would promote a comprehensive framework-based assessment approach. Existing regulatory standards that apply to critical infrastructure such as NERC CIP play a critical role to ensure that appropriate controls are in place for that sector. A broader common framework would ensure greater coverage and could be beneficial, as long as, it does not create a duplicative or conflicting regulatory regime.

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?

As discussed above, the NERC CIP Standards focus on cybersecurity and physical security for the electric sector. These are mandatory cybersecurity standards that carry significant penalties and sanctions for non-compliance. The standards are developed in consultation with industry and approved by FERC.

Additionally, NIST and ISO have developed cybersecurity and information security frameworks that capture cybersecurity controls and configurations that can be applied to across sectors in critical infrastructure. The key guidance documents that could be used to evaluate cybersecurity configurations are noted below:

- NIST 800-53: Recommended Security Controls for Federal Information Systems and Organizations
- NIST 800-53A: Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans
- ISO27002: Information Technology – Security Techniques – Code of Practice for Information Security Management
- NIST 800-82: Guide to Industrial Control System ("ICS") Security
- DOE ES-RM: Electricity Subsector Cybersecurity Risk Management Process
- DOE ES-C2M2: Electricity Subsector Cybersecurity Capability Maturity Model

Note these cybersecurity/information security frameworks must be overlaid and then be applied to the critical infrastructure under review *contextually* based on the capabilities of these systems. Because some of the systems in the power and utility industries are legacy systems that operate for 10-20 years, many of the standard security configurations and controls found in traditional IT environments cannot be directly applied. Consequently, a flexible approach to the cybersecurity/information security framework is necessary to apply mitigating controls that address the risk comparably to traditional approaches.

2. Which of these approaches apply across sectors?

NIST and ISO have developed cybersecurity and information security frameworks that list security controls and configurations that can be applied to specifically to power and utility industries as well as across sectors. The key guidance documents that could be used to evaluate cybersecurity configurations are noted below:

- NIST 800-53: Recommended Security Controls for Federal Information Systems and Organizations
- NIST 800-53A: Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans
- ISO27002: Information Technology – Security Techniques – Code of Practice for Information Security Management

- NIST 800-82: Guide to ICS Security

3. Which organizations use these approaches?

The organizations that used NIST and ISO-based cybersecurity/information security frameworks to guide cyber/IT risk management activities include government, private and public organizations. The frameworks can be applied in various environments across sectors; however they do require some level of interpretation to contextually rationalize the content based on system limitations within the power and utility IT or OT environment.

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

The limitations of using a cybersecurity/information security framework-based approach (i.e., NIST 800-53, NIST 800-53A, ISO27002, NIST 800-82) to establish cybersecurity controls are that some level of interpretation and flexibility is necessary to *contextually* overlay these standards on legacy OT devices used to manage and operate the bulk electric system. Using a framework-based approach to cybersecurity requires interpretation and contextual application based on the guidance documents used. A further prescriptive-based approach to cybersecurity/information security may provide clarity on what cybersecurity controls should be implemented, however the more prescriptive the approach becomes, the less the approach can be extended across sectors.

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

Like other electric sector entities, SRP participates in the NERC ES-ISAC alert system. This program may be enhanced when federal agencies provide timely and actionable information regarding existing and emerging threats.

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

The NERC CIP standards and the DOE ES-C2M2 Model for the electric sector were developed with the participation of industry. The development of a model that draws upon the technical expertise and experience of industry should be part of the framework.

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

Whether a new cybersecurity framework is created that accounts for new and emerging threats to critical infrastructure or an existing cybersecurity/information security framework/guidance document (i.e., NIST 800-53, NIST 800-53A, ISO27002, NIST 800-82) is used, sector-specific guidance should be issued to address any/all unique attributes associated with IT/OT systems used in the corresponding sector for example in the electric sector the NERC CIP standards should play this role. Industry-specific experts should review and develop a sector-specific model of how to apply the security standards to address risk within that 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?

The role of sector-specific agencies and related sector coordinating councils would be to further discuss, educate and promote the use of a cybersecurity/information security framework to review and assess critical infrastructure. These activities would apply whether a new cybersecurity framework or leveraging existing cybersecurity/information security frameworks.

9. What other outreach efforts would be helpful?

As discussed in the previous answer, the sector specific agencies and sector coordinating council can be used to share information and facilitate a better understanding threats and vulnerabilities.

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?

All of these practices are used at varying degrees within the electric sector. The cybersecurity controls and protections noted above are predominantly enforced to the power and utility industry through the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards. These standards require a set of cybersecurity standards to be implemented to critical infrastructure as defined under NERC CIP.

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

NERC CIP standards provide a baseline set of cybersecurity standards required to meet a regulatory mandate for protecting critical infrastructure.

NERC CIP is derived and is effectively a subset of cybersecurity/information security standards from NIST 800-53, NIST 800-53A, ISO27002, and NIST 800-82. NERC CIP is the *prescriptive* baseline security standard to which the electric sector critical infrastructure is assessed to ensure minimum protections are in place for our most critical systems supporting the bulk electric system. NIST 800-53, ISO27002, and NIST 800-82 are the broader, *framework-based* view of cybersecurity control points that should be evaluated for implementation based on system criticality.

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

They each play vital role toward a robust cybersecurity environment. Our objective is to implement tools that increase security without sacrificing system reliability.

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

No. All of these practices can be applicable to the electric sector.

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

The biggest challenge with implementing any of these practices will be coordinating between existing Cybersecurity/information security frameworks (e.g., NIST 800-53, NIST 800-53A, ISO27002, NIST 800-82, DOE ES-RM: Risk Management Process, DOE ES-C2M2: Cybersecurity Capability Maturity Model) and a new framework that extends across sectors due to the nuances and unique characteristics of each critical infrastructure area.

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

The combination of existing power and utility regulation under NERC CIP plus existing cybersecurity frameworks (e.g., NIST 800-53, NIST 800-53A, ISO27002, NIST 800-82, DOE ES-RM: Risk Management Process, DOE ES-C2M2: Cybersecurity Capability Maturity Model) provide a foundation for evaluating each of the organizations against industry-leading cybersecurity practices. For example, NERC CIP grouped into the following areas that then have underlying cybersecurity standards that in-scope entities must adhere to:

- 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

Similarly, the cybersecurity frameworks noted above – and their underlying cybersecurity configurations, controls, and tools – map to the cybersecurity control areas noted below and function to support these areas:

- 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

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

SRP has a methodology in place to ensure the proper allocation of resources to meet our cybersecurity goals.

Duplicative efforts and competing authoritative bodies may tax existing cybersecurity resources.

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

Because the threat landscape is consistently changing and evolving, NERC provides a mechanism to communicate and share threat and risk information to government and peer private institutions. ES-ISAC provides a channel to share actionable intelligence to the government and amongst industry peers within 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. Further shared communication by the government and amongst industry peers will improve cybersecurity defense capabilities to minimize new and emerging threats. Opportunities exist to improve these communication channels and ensure companies have timely information so they can respond and mitigate risk from evolving threats.

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

The application of the aforementioned security practices if properly applied should work to prevent unauthorized access to systems and limit the release of sensitive information.

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

SRP does not operate in other countries.

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

Privacy and civil liberties protections are addressed as a component of each organization's information sensitivity assessment and protection process and legal department.

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

None

Conclusion

SRP appreciates this opportunity to respond and looks forward to future engagement and collaboration with NIST as it seeks to develop the framework.

Sincerely,

James J. Costello

James Costello
Director, Enterprise IT Security