santee cooper

B. Shawan Gillians
Sr. Attorney
Office of General Counsel
(843) 761-7004
fax: (843) 761-4010
shawan.gillians@santeecooper.com

April 8, 2013

Ms. Diane Honeycutt
National Institute of Standards and Technology
United States Department of Commerce
100 Bureau Drive, Stop 8930
Gaithersburg, Maryland 20899

Re: Developing a Framework to Improve Critical Infrastructure Cybersecurity

Dear Ms. Honeycutt:

On behalf of the South Carolina Public Service Authority ("Santee Cooper"), I am respectfully submitting the following responses to the Request for Information ("RFI") issued by the National Institute of Standards and Technology ("NIST") and published at 78 Fed. Reg. 13,024 (February 26, 2013). Santee Cooper shares the Administration's desire to reduce cyber risks to critical infrastructure and appreciates the opportunity to help develop the Cybersecurity Framework.

As a threshold matter, Santee Cooper welcomes the initiative expressed in President Obama's Executive Order of February 12, 2013 ("Executive Order"), particularly Section 4 of that Order which contemplates providing private sector entities with actionable information on emerging threats. Santee Cooper also welcomes the opportunity to assist in the creation of a broad multiple-sector Voluntary Critical Infrastructure Program that would establish a set of core cybersecurity best practices.

From an Electricity Subsector perspective, the Cybersecurity Framework should be careful not to conflict with existing mandatory and consensus-based Critical Infrastructure Protection Standards ("CIP Standards") developed by North American Reliability Corporation ("NERC") and approved by the Federal Energy Regulatory Commission ("FERC") pursuant to Section 215 of the Federal Power Act. The CIP Standards prescribe a core set of mandatory baseline requirements for critical energy infrastructure.

The Framework should establish a baseline set of goals and processes, and should not attempt to prescribe or even suggest specific methodologies or technologies. For the Electricity Subsector, DOE's Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) offers a good starting point for the Framework.

Below, Santee Cooper will respond to the three groups of the questions in the order in which they appear in the RFI.

I. SANTEE COOPER RESPONSES TO NIST RFI

A. Current Risk Management Practices

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

The following would be included among the greatest challenges from an organizational perspective:

- Establish a single, unified and fully integrated corporate approach to proactively managing cybersecurity challenges.
- Improve cybersecurity threat information sharing cross-sector to enable a more proactive response to improve system reliability and mitigate systems unavailability.
- Improve DoS and DDoS attack response solutions.
- Improve 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?

A cross-sector critical infrastructure framework that is too flexible may fail to provide standards that effectively protect all critical infrastructure equally. On the other hand, a cross-sector framework that is too rigid may require some sectors to implement standards that may not be applicable, or may be detrimental, to their mission.

Meeting the needs of all critical infrastructure sectors with a single, balanced, real-world framework could become a costly, resource intensive endeavor. The "single bullet" approach, while attractive, seems impractical and unrealistic given the sensitive, critical nature of the infrastructure being protected. In contrast, sector-specific frameworks could be developed relatively quickly using mature cybersecurity programs that exist today within the Energy Sector.

Finally, it should be noted that the organizations in the Energy Sector have been implementing highly secure, robust cybersecurity architectures, policies, procedures, and standards for over a decade.

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?**

   As a bulk power provider, Santee Cooper operates in accordance with the Reliability Standards established by NERC, including those standards related to Critical Infrastructure Protection. Additionally, Santee Cooper has implemented its own internal cybersecurity policies, procedures, and standards relating to information and systems security. In particular Santee Cooper has promulgated standards on the company's IT security in general, and specific standards on information classification and protection, system and network administration, secure access controls, virus protection, password administration, secure remote access administration, and security exceptions procedures. The company also administers a corporate security awareness program. These policies, procedures, and standards are all communicated through educational programming, required training, and through the company's internal webpage, to which all employees have access.

   Santee Cooper's senior management oversees the above through its creation and oversight of the Corporate Information Resource Council which directs the work of the Corporate Cybersecurity Committee. Both the Council and the Committee meet on a monthly basis.

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

   Santee Cooper's IT Security Unit is responsible for the day-to-day implementation, operation, and management of the company's cybersecurity management program/policy. This unit is housed at the company's headquarters. The corporate committees responsible for the creation of the company's cybersecurity management program are comprised of representatives from all areas of the company. These committees meet on a monthly basis.

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

   Santee Cooper views risk as acts that would threaten to negatively impact the confidentiality, integrity, or availability of Santee Cooper information or systems. To assess these risks, in 2004 Santee Cooper established a Business Impact Analysis (BIA) process that is used to determine the corporate impact (risk) associated with each networked system. The BIA is used to assess the impact that a system being compromised would have via disclosure, modification, or unavailability. The BIA measures the cost of a system compromise through determination of any Loss of

Competitive Advantage, Operational Disruption, Denial of Service, Financial Loss, or Legal Transgression resulting from a disclosure, modification or system failure.

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

   Cybersecurity risk is fully incorporated into Santee Cooper's enterprise risk management process. Every system must undergo a risk assessment before it is implemented and thereafter again at each upgrade cycle. Santee Cooper's Corporate Cybersecurity Committee is the cybersecurity governing body that oversees all cybersecurity initiatives.

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

   Santee Cooper is a part of the Electricity Subsector and therefore must adhere to NERC's CIP Standards, which are part of a body of NERC Reliability Standards. These Standards necessarily address the risks to which the Electricity Subsector is exposed. The Standards were developed pursuant to authority granted to NERC under Section 215 of the Federal Power Act (16 U.S.C. §§ 791-828c) and as such are mandatory and enforceable, carrying potential penalties of up to $1 million per day, per violation.

   In addition to adhering to mandatory industry standards Santee Cooper also employs best practices such as Defense in Depth Protection, Firewalls and Application Firewalls, Malware and Antivirus protection, Server Installation and Hardening Best Practice, Desktop Installation Best Practice, Internet Categorization Filtering, Disaster Recovery and High Availability Strategy, and Backup / Retention Strategy.

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?**

   Electric utilities such as Santee Cooper are regulated by NERC, which was designated as the Electric Reliability Organization (ERO) by FERC pursuant to Section 215(c) of the Federal Power Act. NERC has used its authority to formulate, monitor, and enforce CIP Standards. Civil penalties can be imposed on entities not in auditable compliance with the CIP Standards.

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

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

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

    In order to enhance its situational awareness, Santee Cooper monitors information provided through the ES-ISAC. As part of Santee Cooper's continuity of operations planning, it has identified those critical functions necessary to deliver electric power and maintains plans to restore those systems should the need arise. Santee Cooper has a mature cybersecurity program and has established recovery time objectives (RTOs) and recovery point objectives (RPOs) for incident response and recovery operations, and incorporate those objectives into disaster recovery and business continuity plans and procedures. Santee Cooper tests all RTO and RPO objectives on an annual basis to ensure that the restoration and recovery plans are effective. Maintaining the reliability of the Bulk Power System (BPS) is a core goal for Santee Cooper.

    NERC has also established operational reliability standards including the Emergency Operations Planning (EOP) standards that address operational resilience through mandated backup and recovery goals. The EOP standards complement NERC's CIP Standards and are integrated into Santee Cooper's goals.

    Additionally, Santee Cooper has established Corporate Security Goals to effectively support all IT Security objectives (e.g., testing & deploying security patches and virus protection) so that no major IT security incidents occur at any facilities.

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?**

    Not Applicable.

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 Electricity Subsector is unique among critical infrastructure sectors in that it is regulated by national organizations, namely FERC and its certified Electric Reliability Organization, NERC, which play an active leadership role in developing mandatory cybersecurity standards as a part of its full body of comprehensive Reliability Standards. Santee Cooper believes that it has been beneficial to have national standards from a national organization, and believes that it has been best served by the fact that these national standards come from a national organization that is attuned to and has the necessary knowledge base to adopt standards that address the very unique risks and demands of the Electricity Subsector as opposed to a more generalized set of standards which would be applicable across sectors and subsectors and perhaps conflict with legally required standards which are already in place.

From a more general perspective, national and international standards and organizations could facilitate the development of sector specific frameworks to facilitate organizations and/or sectors that have not already adopted strong cybersecurity programs.

B. Use of Frameworks, Standards, Guidelines, and Best Practices

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

NERC, in its capacity as ERO, has developed as part of its Reliability Standards, a set of CIP Standards, which are mandatory and enforceable for all "users, owners and operators" of the BPS. The CIP Standards have recently completed their fifth revision, with that revision (known as "Version 5") submitted to FERC for approval on February 1, 2013. Once approved, and following an implementation period of approximately two years, the Version 5 standards will be mandatory and enforceable. Until that time, the prior approved version of the standards will remain mandatory and enforceable. Additionally, the ES-ISAC issues alerts to provide actionable intelligence to the industry on cybersecurity threats and vulnerabilities.

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 Electricity Subsector, and providing references to more generic security guidance on its website. CIPC guidance documents include:

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

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

   Many of the concepts of NERC's Reliability Standards are and may be applicable to similar systems in other sectors.

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

   NERC Reliability Standards apply to all "users, owners and operators" of the BPS, which is the subset of the Electricity Subsector whose activities may impact reliability of the transmission network. As provided in Federal Power Act Section 215, the NERC Standards do not cover "facilities used in the local distribution of electric energy."

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

   Though NERC Reliability Standards apply to users, owners and operators of the BPS they do not apply to facilities used in the local distribution of electricity. However because the NERC Reliability Standards apply to a portion of Santee Cooper's system, the company applies those same cybersecurity protection across the organization, even those areas in which the Standards might not otherwise apply such as the company's Distribution SCADA system and Regional Water SCADA System.

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

   The federal government's sharing of actionable information about the threats the electricity industry and other critical infrastructure sectors are facing in a timely fashion is critical to security efforts.

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

   NERC's CIP Standards, which were developed for the use of the Electricity Subsector, were developed by the Electricity Subsector, using the technical expertise of industry stakeholders and taking into consideration the comments of interested stakeholders for use by the Electricity Subsector.

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

   With regard to the Electricity Subsector, NERC Reliability Standards are already in place and are mandatory and universally applied across all relevant stakeholders within NERC's (and FERC's) jurisdiction. Because NERC Reliability Standards are

mandatory and enforceable, care must be taken to avoid creation of additional standards that would conflict with the pre-existing NERC Standards.

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 sector-specific agencies (SSA) can provide greater focus on distribution and restoration functions, and also work closely with Government Coordinating Council and Sector Coordinating Council to facilitate support for the ISACs.

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

   It would be helpful for the SSA and GCC/SCC to assist in developing and providing executive sponsorship for a collaborative and comprehensive outreach effort that informs sector participants on key structures, policies, priorities and approaches employed by the sector.

C. Specific Industry Practices

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

   The nine practices listed in the RFI (see above) are widely used by Santee Cooper and are also addressed within the current set of CIP Standards. Santee Cooper employs all of the aforementioned practices in securing critical infrastructure and other corporate assets.

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

   The proposed Version 5 of NERC's CIP Standards generally cover the same subject areas as both the NIST FISMA framework and the ISA-99 Standards, along with the standards that they also reference.

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

   The most critical practices are those that strengthen security without impeding system reliability. If a security framework requiring compliance is put into place and that framework diminishes operability or reduces real-time data situational awareness, operations of the grid can be negatively impacted.

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

   No. All of these practices are applicable to the Electricity Subsector.

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

   The most significant implementation challenge at Santee Cooper is ensuring that the application of any practice does not impact the reliability of operational systems (control systems, SCADA, etc.) or compromise their protection from untrusted sources.

   Another significant implementation challenge within the listed practices above is monitoring and incident detection tools and capabilities. Threat information sharing between government and industry is extremely important, but the continually evolving security threat from Advanced Persistent Threats is significant.

   The use of encryption and key management on data at rest poses an implementation challenge because of the challenges that presents with regard to usability of the data, the productivity of the users, and the performance degradation to the systems.

   Mission/system resiliency practices are a challenge because the cost inherent in fully resilient systems is as much as eight times the cost of a non-resilient system.

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

   Santee Cooper is required to follow all NERC Reliability Standards, including the Critical Infrastructure Protection standards. Santee Cooper also follows voluntary guidance developed and issued by NERC and others such as NIST, International Society of Automation (ISA), International Electrotechnical Commission (IEC), and the International Organization for Standards (ISO). Additionally, Santee Cooper has created standards and guidelines to address many of these practices.

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

   Santee Cooper does have a methodology that takes into consideration strategic planning and regulatory compliance needs in place for the proper allocation of business resources with regard to IT standards.

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

   Speaking specifically to Santee Cooper, we have created a "Computer Incident Response Standard/Procedure" for addressing escalations in cybersecurity risks within the organization.

   Additionally, Santee Cooper complies with NERC's CIP Standards, which requires reporting for significant compliance matters to the ES-ISAC along with voluntary

non-compliance reporting. A NERC Alert System addressing such matters has been implemented and formalized across the industry for registered entities.

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

   Santee Cooper is mindful of the legal and regulatory issues surrounding privacy and civil liberties, which may include risks associated with sharing sensitive information regarding authorization of users accessing systems due to the fact that individuals' names are tied to the authorizations, which may raise privacy and civil liberties concerns.

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

    While Santee Cooper does not engage in global business, it is a part of the BPS in North America which spans the international border between the U.S. and Canada and that portion of the international border between the U.S. and Mexico at California and Baja California Norte. Because of the interconnected and international nature of the BPS is must operate under a common set of rules. NERC has established a consistent set of standards that can function across international boundaries, and versions of NERC's standards are now in effect in several Canadian jurisdictions.

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

    It may be appropriate to consider NERC's CIP Standard CIP-011 (information protection) within the proposed Version 5 of the CIP Standards, and its extension to the classification and security of all sensitive information that may exist for organizations in the Electricity Subsector.

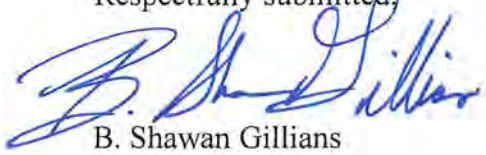
12. **In addition to the practices noted above, are there other core practices that should be considered for inclusion in the Framework?**

    The proper and regular training of personnel is a core practice that should be considered for inclusion in the Framework.

II. CONCLUSION

Santee Cooper supports NIST's efforts to develop a Cybersecurity Framework that is consistent with the Executive Order, and asks that NIST take these comments into consideration as it develops the Framework.

Respectfully submitted,



B. Shawan Gillians