Responses to NIST Request for Information: Developing a Framework to Improve Critical Infrastructure Cybersecurity
April 8, 2013
Southern California Edison

INTRODUCTION

SCE recognizes the risks cyber threats pose to its customers and shareholders, as well to our national security. A Cybersecurity Framework can provide a basic cyber protection baseline for participating companies. Unfortunately, published paper-based standards and governance are not enough to protect against cyber threats. Cyber threats do not remain static; they morph very quickly as do the corresponding prevention methods.

Due to the rapid changes in cyber threats, sharing information about newly discovered threats becomes essential. Alerting companies to the threats alone is insufficient. Understanding techniques for prevention near real-time is also required and equally essential.. This is especially true for smaller companies with fewer resources so they also apply adequate protection. In a configuration like the electric grid, which becomes more vulnerable in a more complex and modernized state, companies are so inter-connected, a weak link can be detrimental.

The Department of Defense and the Defense Industrial Base (DoD/DIB) program provides opportunities essential to addressing this issue. The Department of Defense (DoD) and Department of Homeland Security (DHS), through a partnership, have established the Defense Industrial Based (DIB) Cybersecurity /Information Assurance Program that includes a defense network designed to provide classified threat and technical prevention information near real-time over a secured network. The Presidential Executive Order – Improving Critical Infrastructure Cybersecurity (EO) Section 4 also sets a potentially helpful direction. Although the details are unclear, the Enhanced Cybersecurity Program appears to leverage the DoD/DIB digital defense network with the Department of Homeland Security (DHS) performing a role similar to the DoD.

Regardless of the possible lack of efficiencies by having the DHS perform a function the DoD is already performing, the models are positive. We believe the most critical companies within each critical infrastructure sector should be part of the DIB and leverage the DoD digital defense network. The Enhanced Cybersecurity Services could be very useful for the remaining critical infrastructure entities.

NIST has the opportunity, as part of its Cybersecurity Framework, to direct critical infrastructure companies to participate in the DoD/DIB and the Enhanced Cybersecurity Services programs. We encourage NIST to seriously consider this possibility as a way to address the gap between lagging published standards and emerging, unanticipated threats.

SECTION 1

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?
    - Ensuring alignment amongst the federal entity jurisdictions, and then ensuring alignment between federal and state regulatory environments. Being subject to multiple regulatory regimes (federal, state, local) can create investment conflicts and operational. Satisfying multiple governing bodies can become so complex that cyber defenses are actually degraded.
    - Managing cybersecurity in a complex and interdependent environment. The electric grid is complex with many entry points requiring cybersecurity safeguards; the complexity is increased exponentially when sector interdependencies are considered. One sector's vulnerability can impact another sector due to the operational interdependencies.
    - Establishing metrics for evaluating cybersecurity effectiveness.
    - Standardizing vendor products with security features and assurance mechanisms that are interoperable.
    - Near real-time information sharing of threats and prevention techniques between government and private sectors.

2. What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?
    - Ensuring the framework is not overly prescriptive. A common cybersecurity framework that supports multiple sectors is possible if goals are targeted and the framework is not too prescriptive. Critical assets vary greatly across sectors, as do the protection solutions; in addition, flexibility is required for quick adaptation to new threats.
    - Acknowledging the framework can only be a baseline. A cross-sector framework will result in the lowest-common-denominator being applied. This becomes a baseline, and should not be confused with what is actually required in the various sectors for sufficient protection.
    - Standards conflicts. Resolution of conflicts amongst standards bodies at federal, state, and local levels is required for an effective approach.

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?
    - SCE maintains a formal set of risk management and cybersecurity policies and standards that apply to the enterprise.

  - The policies and standards are reviewed regularly and ratified at the executive level.
  - Policy communication follows a standard approach, whether cyber related or not.
  - Policies are posted on our intranet, awareness messages are created and shared, and policies are shared in various forums for better dissemination.
  - Formal governance processes and teams address policy compliance and exception management.
- Procedures are developed at an operational level. Communication and deployment varies depending on the procedure.

4. Where do organizations locate their cybersecurity risk management program/office?
   - A dedicated cybersecurity organization is led by the Director of Cybersecurity, an executive manager reporting to the CIO. Additional cybersecurity responsibilities are distributed across a multitude of departments and roles. EIX's Audit Committee and Board of Directors are regularly briefed on the cybersecurity risk environment and mitigating strategies, any significant developments, and how the cybersecurity program is responding. Finally, SCE's Director of NERC Compliance and personnel in the NERC Compliance Program office also collaborate with the cybersecurity organization on related cybersecurity issues as they apply to NERC CIP standards.
   - Recently a Cybersecurity Oversight Committee was formed to report to the Board of Directors. The Director of Cybersecurity reports to the Cybersecurity Oversight Committee, which is chaired by the Chairman of the Board.

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

   Please see Section 1, #6 below.

6. To what extent is cybersecurity risk incorporated into organizations' overarching enterprise risk management?
   - SCE's overall risk assessment approach identifies cybersecurity as one significant risk area. SCE's Cybersecurity program works with SCE's Enterprise Risk Management program.
   - Within the Cybersecurity program, SCE maintains a standard cybersecurity risk assessment methodology, and has a trained team that conducts risk assessments in a consistent manner.

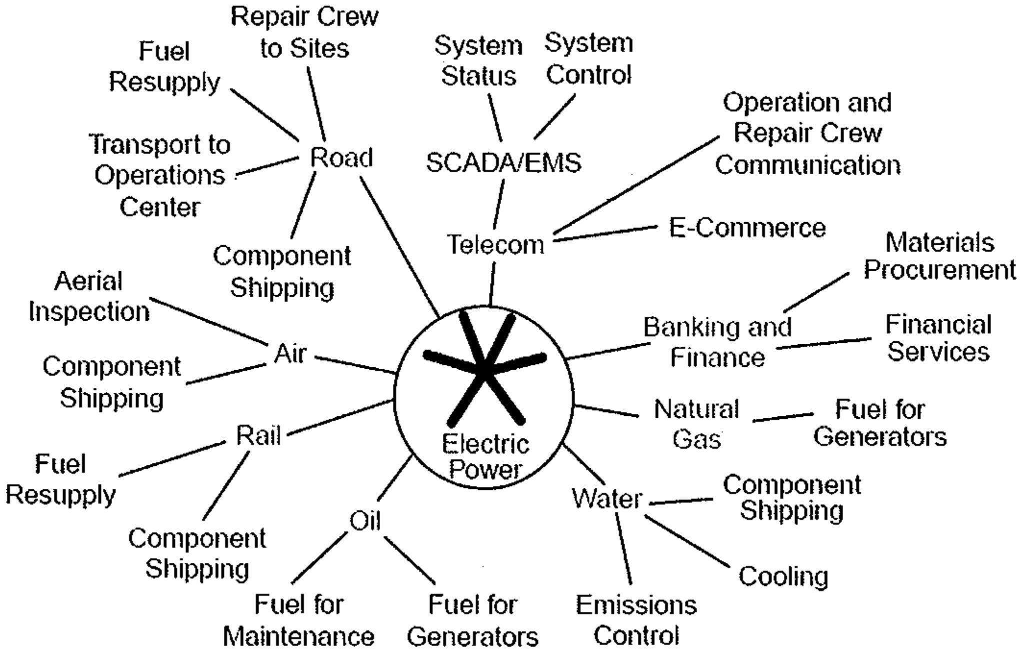
7. What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?
    - SCE has developed a Risk Assessment Methodology (RAM) that adopts NIST 800-39 - Managing Information Security Risk. RAM currently includes SCE internal cybersecurity policies, standards and data classification. Audits and third party reviews also help assess and manage risks. The Cybersecurity program manages identified risks and the solutions required to mitigate the risks.

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?

    SCE is subject to the following regulatory reporting requirements;

    - Federal Energy Regulatory Commission (FERC)/North America Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standards
        - CIP-002-3 Critical Cyber Asset Identification
        - CIP-003-3 Security Management Controls
        - CIP-004-3 Personnel and Training
        - CIP-005-3a Electronic Security Perimeter(s)
        - CIP-006-3c 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
    - NERC Communications (COM) standards
        - COM-001-1 Telecommunication: R2. ~ alarm, test and/or actively monitor vital telecommunications facilities
        - COM-002-2 Communications and Coordination: R1. ~ communications (voice and data links) shall be staffed and available for addressing a real-time emergency condition
    - Nuclear Regulatory Commission (NRC) 10 CFR 73.54
    - California Public Utilities Commission (CPUC) - Smart Grid Data Privacy, 15/15 Rule
    - Federal Trade Commission (FTC)
    - Other regulatory requirements that SCE is subject to, but are not "critical" to the safe operation and reliability of the bulk power system, include:
        - Sarbanes-Oxley
        - Payment Card Industry
        - Health Insurance Portability Accounting Act
        - California Civil Code § 1798.29(a)

9. What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?
    - The SCADA and Energy Management System (EMS) environments and their supporting network infrastructures are critical assets in the energy sector.
    - The distribution of electricity to users is dependent on power generation (e.g., hydro, nuclear, natural gas) and transmission, all of which must remain in balance across the grid network.
    - Hydro generation is dependent on water and dams
    - Telecommunications is essential for electric power operational activities, from voice communications to information transmission about the grid stability
    - Crew mobilization depends on transportation to reach many of the assets spread across the territory.
    - The below diagram nicely illustrates interdependencies. The complete accuracy could be debated, but this is a helpful start to understanding the electric power interdependencies and complexities.



Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Indentifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine*, p. 14. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=969131&tag=1

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

- For quite a few years, SCE has defined specific goals related to enhancing cybersecurity. The cybersecurity goals have been balanced with other operational goals through a robust process. SCE continues to address cybersecurity goals through the Enterprise Risk Management program and processes.

11. If your organization is required to report to more than one regulatory body, what information does your organization report and what has been your organization's reporting experience?

- NERC CIP Reliability Standards
  - Annual Self-certification report for NERC standards
  - Annual Technical Feasibility Exceptions status report for NERC CIP standards
  - As needed, self-report for potential noncompliance with NERC standards
  - As needed, Technical Feasibility Exceptions for assets that do not comply with technical/specific technical requirements in NERC standards
- NRC
  - 10 CFR 73.54 - For reporting cyber events involving plant systems
  - NERC EOP-004-1 - For reporting cyber events involving non-plant systems
- Privacy
  - SCE's privacy maintenance requirements are governed by three primary regulatory agencies which enforce reporting requirements: Federal Trade Commission (FTC), California Attorney General's Office (CA AG), and the CPUC.
    - The FTC requires an annual "Red Flags" assessment be conducted of the company's controls for the Fair Credit Reporting Act
    - The CA AG requires reporting privacy breaches affecting 500 or more customers
    - The CPUC requires reporting privacy breaches affecting 1000 or more customers, and requires an annual privacy report, as well as triennial security and privacy audits/reports

12. What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?
    - Establish standards that vendors must adhere to for critical infrastructure protection. Vendors are naturally driven to develop proprietary software, which thwarts opportunities for interoperability on a wide scale.

- Work towards eliminating standards conflicts at federal, state, and local levels. The conflicts can (1) inherently introduce more risk due to the complexity that arises, and (2) require additional funding to address redundant requirements.
- Avoid putting unnecessary requirements on a specific sector if sufficient standards already exist, or allow one set of standards to suffice as framework participation. For example, NERC standards currently exist for the electric sector.
- As part of the Cybersecurity Framework, require companies with critical infrastructure to participate in the DoD/DIB digital defense network and Enhanced Cybersecurity Services program to enhance visibility to real time threat indicators and provide better near real time defenses against cyber threats. What may work best is identifying the more critical companies in each sector to participate directly in the DoD/DIB network and for the remaining companies, require participation in Enhanced Cybersecurity Services. The cost to participate should be nominal to nothing. The broader the participation, the more our national security improves.
- Establish a software-based standard that is military grade and interoperable across the utility sectors. Electric grid modernization includes increased grid automation and connectivity, which inherently increases its complexity and vulnerability. This complexity, coupled with the increasing threat of cyber-attacks, requires the deployment of military-grade cybersecurity solutions to ensure continued grid reliability. Over the past several years, SCE has been developing Common Cybersecurity Services (CCS), based on common services architecture that enables any device in the newly deployed networks to access common services (e.g., cybersecurity, device management, network monitoring, etc.) in utility control centers. Multi-vendor interoperability can be supported through standards enforcement across the architecture, while simultaneously driving down cybersecurity costs.

  CCS is designed to implement security mechanisms for enforcing confidentiality, integrity, and availability as security services and policies that protect electronic information, communication and control systems necessary for the management, operation, and protection of the SCE Smart Grid System of Systems. CCS is specifically designed to satisfy the Smart Grid requirements and standards developed by NERC, NIST, DHS, and DOE as part of the national effort on critical infrastructure and information protection standards as well as Smart Grid standards development.

  Industry adoption of a common services architecture that uses software based standards, and meets regulatory requirements as part of a unified approach, would enhance the overall security of the electric grid. CCS can also be extended into other similar industries that use industrial control systems such as oil and gas.

SECTION 2

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?
   Please refer to EEI's response.

2. Which of these approaches apply across sectors?
   Please refer to EEI's response.

3. Which organizations use these approaches?

SCE has adopted, used, and contributed to the development of various industry standards and guidelines which include: NERC CIP, NISTIR 7628, NIST 800-53, NRC CFR 10 73.54, NEI 08-09, and the DOE Risk Management Maturity Model.

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

Using frameworks, standards, and guidelines alone, without a risk management-based approach, does not necessarily achieve security. A combined approach is favorable because federal mandates and corporate business goals can be better aligned.

Some approaches focus on "how," rather than "what" needs to be secure. When standards focus on "how," the implementations can be very costly and inefficient because environments, even within a sector, can be different.

Paper-based standards, as opposed to software-based standards, don't produce certain desired benefits because of the lack of uniformity. Uniformity can offer better interoperability between systems and networks.

5. What, if any, modifications could make these approaches more useful?
   - If a company is already adhering to similar standards or is mandated to adopt similar standards (e.g., NERC CIP), allow the adoption of those standards (e.g.,., NERC Reliability Standards) to suffice for purposes of Cybersecurity Framework participation.
   - Alignment of state and federal cybersecurity policies, standards, and guidelines may help avoid redundant and overlapping mandates.

- Where it is important to have standardization across systems and networks, provide software-based standards to improve interoperability, flexibility, and communications. The expense of vendor lock-in can be avoided when standards are set in this manner. SCE has developed a Common Cyber Security solution that provides Department of Defense grade security, which could serve as a software-based standard for the government to provide.

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

   NERC CIP Reliability Standards are enforceable on the electric energy sector and address the unique concerns and features applicable 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 electric industry sector is already governed by FERC/NERC mandated and enforceable standards. Sector specific standards should be consistent with the cross sector framework.
   - Paper-based standards take a long time to develop and implement. Cyber threats will always outpace these standards. Refer to Section 1, #12 regarding standards that should be adopted and encouraged.
   - Sector specific standards would have to be sufficiently flexible and not overly prescriptive to allow for innovation of new technologies and rapid adoption of cyber protection.

8. What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?
   Please refer to EEI's response.

9. What other outreach efforts would be helpful?
   Please refer to EEI's response.

SECTION 3

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?

   SCE has an extensive cybersecurity program that covers critical energy management systems and applies a defense-in-depth strategy using the measures and practices in the areas listed above. Similarly, other SCE cybersecurity practices include:

   - Threat & vulnerability analysis
   - Cybersecurity Out posting
   - Data Protection
   - Perimeter Defense
   - Interior Defense
   - Industrial Control Systems Security (known at SCE as "PSC")
   - Nuclear Computer Systems & Network Protection
   - Common Cyber Security (CCS) service solution for Smart Grid requirements
   - Training and Awareness

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

   SCE's practices are derived from NIST guidelines. The NIST guidelines are in-line with international best practices such as ISO/IEC 27002/17799 which covers a broader industry

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

   SCE views cybersecurity as a comprehensive strategy with no single practice being more important than the others. The combined practices work together as a comprehensive defense-in-depth approach. SCE utilizes various solutions and strategies in its cybersecurity program and must ensure that all areas are strong operationally.

   Also, practices can be 'designed' into systems, thereby reducing issues and problems that trigger reactive security controls. Separation of business versus operational systems, encryption, identity management, asset id and management, and engineering can all be embedded to some degree into the systems, thereby improving the effectiveness of their respective adoption.

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

The stated practices are relevant to any organization interested in providing cybersecurity to its organization. How they are implemented may vary given critical infrastructure sectors are unique. Because inter-dependencies exist amongst sectors for the security and reliability of the grid, some practices may be more or less important.

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

   Cybersecurity implementations differ from business-to-business and from sector-to-sector. Each poses a unique set of challenges, including implementation, administrative, operational, complexity, and cost.

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

   SCE developed its internal cybersecurity policies, standards, and procedures based on a number of industry standards and guidelines (i.e., NERC CIP, NIST 800-53, NIST 800-82, NRC CFR 73.54, NEI 08-09, etc.) for the protection of IT information assets, as well as for the safety and reliability of the bulk electric system.

   Using industry guidelines in conjunction with a cyber risk-based management approach will ultimately lead to compliance at the local and federal levels and will provide a baseline of security for the company. Compliance, however, is not always enough for a company's cyber protection. Rapid changes in threats require constant adaptation efforts that go beyond the baseline standards.

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

   - SCE has an established Cybersecurity group staffed by certified cybersecurity professionals exclusively dedicated to SCE's cybersecurity program. Responsibilities include the development and on-going maintenance of cybersecurity policies, standards, and practices. Reviews and updates of these policies occur annually. Standards are modified based on threats and regulations.
   - In addition, technology standards related to cyber protection are established and governed through an Architecture Review Board process. This helps ensure a standardized method for implementing risk mitigating measures.

8. Do organizations have a formal escalation process to address cybersecurity risks that suddenly increase in severity?
   - SCE management escalation: SCE has a formal escalation process for real time threats. The Director of Cybersecurity escalates to the CIO, then to the Cybersecurity Oversight Committee if appropriate. The Cybersecurity Oversight Committee reports to the Board of Directors. Escalation can be rapid.
   - Threat escalation to external entities: SCE monitors increases in severity of cyber risks and reports threats to ES-ISAC if Bulk Electric power related.

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

   - Data Privacy risks include:
     - Fraud
     - Personal behavior patterns/appliances used
     - Real time remote surveillance
     - Non-grid commercial uses of data
     - Unauthorized third party access
     - Reselling of consumer data
     - Financial and reputational costs

   - When applying the practices, risks and issues arise related to:
     - Conflicting sector and state specific rules regarding what is defined as Personally Identifiable Information (PII) and who is allowed to obtain the information
     - Non-aggregated PII being made available to the government for data mining purposes, without customer choice/notification
     - Law enforcement circumvention of the legal request process by obtaining customer information through a national database or other government agency in an effort to obtain PII.
     - Sharing information regarding detected cyber threats, vulnerabilities discovered, and vendors' cyber protection capabilities, which can leave the sharer open to legal ramifications

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

    - SCE is an investor owned utility, serving more than 14 million customers in the Southern California region. SCE engages with state and federal governments on cybersecurity related legislative and regulatory matters.

SCE does not engage in global business or in international policy-making decisions.

- If the framework becomes prescriptive, then vendor products and standards at an international level could be impacted.
- Outsourcing at an international level could be impacted depending on the standards set.

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

SCE views sensitive information such as Personal Identifiable Information (PII), Consumer Energy Usage Data (CEUD), financial, health and other sensitive related information as an asset that should be protected by security practices and business processes. A privacy risk management framework that embeds privacy into a day-to-day operation, also known as Privacy by Design, coupled with a strong government partnership, would also enhance protection of sensitive information. Other governing considerations include:

- Having a single agency, as opposed to multiple agencies, set regulations for defining and managing PII in an effort to be more efficient and avoid confusion.
- Protecting an individual's rights and preventing government use of PII or Consumer Energy Usage Data (CEUD) for any purpose other than its initially intended use
- Protections and preemptions from the Freedom of Information Act (FOIA) for those protecting critical cyber assets; information shared with the government should be exempt from disclosure under the FOIA at both the federal and state levels.
- Obtaining PII through the current legal process (e.g. subpoena/warrant) should it be required. Companies complying with an agency's request should be protected from harm/lawsuits.

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

Please refer the Introduction section.