April 8, 2013

VIA EMAIL

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 Electric Trade Associations in Response to NIST's Request for Information on "Developing a Framework to Improve Critical Infrastructure Cybersecurity."

Dear Ms. Honeycutt:

The Sacramento Municipal Utility District (SMUD) hereby responds 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]

A. General Comments

SMUD is the sixth largest customer-owned utility in the U.S., providing electricity to the California capital region since 1946. We serve 1.4 million customers within a 900-square mile service territory. SMUD operates the Balancing Authority of Northern California (BANC), a 5,000 MW balancing authority (BA) that spans most of Northern California. SMUD is a not-for-profit entity that is directly accountable to its customers – the citizens in our community. Our commitment is to provide highly reliable, low cost and environmentally responsible electric service to our citizen-customers.

The electric industry has a long history of reliability excellence and a proven commitment to maintain these high standards as technology evolves. Cybersecurity is central to the day-to-day operations of SMUD and other utilities throughout the nation. Because of the differences in design, configuration and operations among utilities, industry expertise is an essential component of national

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

cybersecurity protection planning and implementation. Collectively, we have the deepest understanding of how our systems operate.

SMUD wholeheartedly supports the provisions in the Executive Order that would facilitate information sharing by government agencies with critical infrastructure owners and operators. Public-private information sharing has enabled SMUD and other utilities to improve the overall resilience and reliability of the bulk power system. However, the federal government has access to significant threat and vulnerability information at a classified level that has not been filtered down to the owners and operators of critical infrastructure. Because we operate in a 24/7 environment, industry stands ready to respond immediately to timely and actionable information on imminent cyber threats. Accordingly, we are hopeful that with the implementation of the provisions of the Executive Order that call for increased information sharing and expedited security clearances, the electric industry will receive the information that it needs to implement protective measures to address existing and emerging cyber threats.

SMUD is a member of the American Public Power Council (APPA) and the Large Public Power Council (LPPC) and supports the comments submitted to you by the Electric Trade Associations.

Notices and communications regarding these comments may be addressed to:

Laura Lewis
Assistant General Counsel
Sacramento Municipal Utility District
6201 S Street
Sacramento, CA 95817
(916) 732-6123
Email: Laura.Lewis@smud.org

B. Specific Comments

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?*

One of the greatest challenges in improving cybersecurity practices across critical infrastructure is with information sharing and access to actionable threat and vulnerability information. While there has been a concerted effort from the Energy Sector – Information Sharing and Analysis Center, Department of Homeland Security and the Department of Energy to share information, very few industry representatives possess the appropriate level of clearance to receive non-public information. There needs to be sufficient disclosure and attribution provisions created to ensure that sensitive security information is handled appropriately. Additionally, for sectors that are under mandatory regulatory cybersecurity standards like the electricity sub-sector there needs to be sufficient provision for ensuring there is no regulatory punitive actions as a result of participating in an information sharing forum.

Another challenge associated with improving cybersecurity practices within critical infrastructure is the amount of legacy systems that were not developed with the capabilities of modern systems. Within the electricity sub-sector, many of the supervisory control and data acquisition (SCADA) systems were developed with availability as the major component. These devices have small processors and little memory to perform common practices such as encryption, access control, logging, monitoring and alerting. Wholesale replacement of these devices requires extensive planning and capital investment and is typically achieved over several years. This requires applying compensating measures to achieve commensurate cybersecurity posture.

A final challenge in improving cybersecurity practices across critical infrastructure is the engagement with the manufacturers of hardware and software developing new systems and retrofitting existing systems to support appropriate cybersecurity controls. It is imperative that we have fully engaged vendors who identify cybersecurity as a core requirement of their business practices and deliver systems in a secure manner.

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

Each of the 16 Critical Infrastructures have unique attributes with differing degrees of requirements for confidentiality, integrity and availability. Aligning a harmonized framework across each of the sectors may require one sector to lower their threshold to accommodate these unique cross-sector attributes. Additionally, developing a common threat profile across sectors may be a challenge.

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?

SMUD's elected Board of Directors has adopted a resolution requiring the implementation of Enterprise Risk Management, which includes cybersecurity risk. The CEO/GM established an Enterprise Risk Management Office under the Chief Financial Officer. The Office is responsible for working with each of the business units to identify risks to the utility operations including cyber threats and vulnerabilities. Risks are regularly reviewed by the executives and communicated to the business units.

SMUD has also established an Information Security Office that has enterprise responsibility promulgated from the Board of Directors and Chief Executive Officer by signed policies and procedures and mandatory annual training. These policies and procedures are regularly reinforced through meetings and presentations for the implementation of cybersecurity practices, including cyber risk management. Additionally, as part of SMUD's procurement risk practices, significant Information Technology projects are evaluated to determine whether additional cybersecurity insurance is required. SMUD works with its insurance providers and contract awardees to maintain appropriate certificates.

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

The cybersecurity risk management program is located within the Information Technology Department. There is a designated Information Security Officer (ISO) with responsibility for carrying out cybersecurity practices including identifying and communicating cybersecurity risk to the enterprise. The ISO reports to the Director of Information Technology. The Information Security Office works very closely with all lines of business, enterprise risk management and Internal Audits to raise and evaluate risk and determine the appropriate risk response.

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

Cyber risk is identified as those means to disrupt the operations of the utility or the ability to steal/breach systems to attain unauthorized access to systems and data. Risk is assessed based on the threats and vulnerabilities to operations/systems/data and the controls in place to detect, deter and defend against the threat actors. Value is placed on the resources, business processes, systems and data to determine the level of protection necessary. Executive leadership ultimately makes the determination on what risk responses should be implemented (i.e. Acceptance, Transference, Mitigation, Avoidance, Insurance or a combination of these responses).

SMUD has developed policies and practices related to the acquisition of Information Technology, which requires the development of a System Security Plan (SSP) as part of the solicitation process. The SSP covers the following areas of every proposer: Information Security Program, Security Development Lifecycle, System Architecture, Application Architecture, Authentication, Authorization and Accounting services, Data Exchanges, Data Storage, Session Handling (for web applications), System Logging, Vulnerability Management Program, System and Data Recovery Program (including recovery time and recovery point objectives), Change Control Process, Physical Security Program, Audits and Assessments (independent assessments and certifications). SMUD evaluates the responses to the SSP against expected cybersecurity and information technology practices using existing guidelines and standards such as, the National Institute of Standards and Technology (NIST) Special Publications, International Standards Organization (ISO) 27000 series, and the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards. Once approved, the SSP is incorporated into the contract and becomes a living document of the project. Plans must be updated as part of change control and configuration management and be reapproved by the Information Security Office.

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

Cyber risk is an integral component of the enterprise risk management practice at SMUD. From a project perspective, cyber risk is assessed through the entire lifecycle with collaboration between the Information Security Office subject matter experts and the business unit project staff. The cyber risks are then included within the enterprise risk management system.

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

SMUD has begun adoption of the Department of Energy (DOE) Risk Management Process (RMP) guideline along with the DOE Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2). The DOE RMP was tailored to the electricity subsector from the NIST Special Publication 800-39, *Managing Information Security Risk*. The guideline establishes a repeatable process that allows entities to assess cyber risk in a linear manner over three tiers: (1) Organizational (executive leadership), the (2) Mission and Business Processes (the supporting processes to the organization operations identified in the top tier), and (3) Information Technology and Industrial Control System (the actual systems). Within each of these tiers there is a systematic risk cycle with four circular steps: Risk Framing, Risk Assessment, Risk Response and Risk Monitoring. The systematic and circular nature of the Risk Management Process allows entities to perform discrete assessment against a specific operational aspect and repeat the process throughout the entire organization.

The DOE ES-C2M2 provides entities the ability to measure the maturity of the organizations cybersecurity program over 10 domains; (1) Risk Management, (2) Asset, Change and Configuration Management, (3) Identity and Access Management, (4) Threat and Vulnerability Management, (5) Situational Awareness, (6) Information Sharing and Communication, (7) Event and Incident Response, Continuity of Operations, (8) Supply Chain and External Dependencies, (9) Workforce Management, and (10) Cybersecurity Program Management. Within each of these domains there are specific objectives and practices that can be measured for institutionalization within the entity. A result of applying the ES-C2M2 is a scorecard that can be used to show the maturity of an organization and provide a roadmap for improving the maturity level.

Combining the DOE RMP and ES-C2M2 provides SMUD with a comprehensive cybersecurity risk methodology to understand, measure, and manage risk at the management, operational, and technical levels. From a technical perspective, SMUD uses several vulnerability assessment technical controls to understand, measure, and manage risk to specific systems. SMUD owns and operates the nCircle IP360 vulnerability assessment system and the nCircle Change and Configuration Management system. SMUD performs continuous vulnerability assessments throughout the enterprise to ensure that systems are being maintained according to established policies and procedures. Systems are interrogated to determine patch levels, authorized applications, authorized configurations, authorized services, etc. Reports are generated from the assessments and delivered to system owners for remediation.

Using the nCircle reporting capabilities, SMUD is able to quantify system level risk. Additionally, SMUD owns and operates Imperva's SecureSphere Discovery and Assessment Server (DAS). This application allows SMUD to assess vulnerabilities and misconfigurations related to the various databases within SMUD's enterprise. Both of these tools can be further set to align with specific industry standards and best practices using pre-defined or custom policies. Since both of these tools show potential vulnerabilities and potential misconfigurations, SMUD also owns and operates enterprise Metasploit for performing proof of concept penetration testing based on what nCicle and Imperva identify. Together these vulnerability assessment tools allow SMUD to measure the cyber risks to the individual systems and applications.

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?

As an electric utility we are regulated under the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards. These standards were promulgated from the Section 215 of the Energy Policy Act of 2005, and give the Federal Energy Regulatory Commission (FERC) authority to establish an Electric Reliability Organization (ERO) with responsibilities for the development and enforcement of cybersecurity standards. The North American Electric Reliability Corporation (NERC) was designated as the ERO. The NERC, in collaboration with industry, established the CIPs. Electricity subsector entities are audited at least every three years for their adherence to the CIPs. Failure to comply with the CIPs can subject entities to penalties and sanctions amounting to $1 million per day per violation.

If entities determine they are not in compliance with the standards, they may self report to their regional auditors and develop mitigation plans to come into compliance. Additionally, under the Incident Response requirements of CIP-009, entities are required to report to the Electricity Subsector – Information Sharing and Analysis Center suspected cyber events.

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

For optimal operations of the bulk electric system, SMUD is dependent on the telecommunication sector for providing and maintaining digital and analog circuits. SMUD also depends upon the financial services sector to provide access to banking activities for supporting energy market practices related to buying and selling of power across the grid. Further we are dependent on the transportation sector to provide access to the delivery of equipment such as power poles, transformers, etc.
Lastly, SMUD recognizes the unique importance electricity plays to the entire list of critical infrastructures. To some degree, electricity is needed by every other sector to facilitate optimal operations.

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

The NERC CIPs provide several "Key Performance Indicators" to measure the efficacy of cybersecurity practices. Audits of the NERC CIPs require direct performance evidence to demonstrate compliance. Additionally, as part of the CIP-009 Recovery Plans for Critical Cyber Assets standard, entities are required to establish plans to address "required actions in response to events or conditions of varying duration and severity that would activate the recovery plan."

At SMUD, request for exceptions to the NERC CIPs or corporate policy requires documented business cases along with the identification of compensating measures that meet the intent of the control that is the subject of the exception. Approvals of these exceptions require several approvals by SMUD's Information Security Office, CIP Senior Manager and other SMUD leadership.

Additionally, using Business Impact Assessments and Business Continuity practices, SMUD has assessed critical operations and aligned recovery time and recovery point objectives. The business processes are at least annually reassessed to measure whether their services can be maintained during an event. By SMUD policy, vulnerabilities must be assessed within a specific timeframe. SMUD uses the vulnerability assessment tools previously discussed (nCircle, Imperva and Metasploit) to evaluate patch and configuration performance throughout the enterprise. These tools generate scorecards that can be used to manage cyber risk.

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

As part of the NERC CIP-008, Incident Reporting and Response Plans, SMUD is required to report to its local regional auditor suspected non-compliance with the NERC CIP standards. Additionally, entities are required to report to the Electricity Sector – Information Sharing and Analysis Center (ES-ISAC) suspected cyber events. SMUD's experience reporting to the ES-ISAC has been very positive. The ES-ISAC has been able to use their resources to review events and provide early warning to other ISAC members.

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 under the NERC CIP mandatory cybersecurity standards is already required to have independent assessments performed at least every three years. The assessments are performance based and determine the organization's adherence to the NERC CIP standards. Additionally, for those organizations that process and store credit card payments card information, mandatory annual independent assessments and certifications from a Payment Card Industry Data Security Standards (PCI DSS) qualified assessor is also required. The assessment measures the organization's implementation and adherence to the PCI DSS requirements. The degree of assessment is contingent upon the type of data the merchant processes. This approach provides the ability to manage the scope of the assessment to ensure that the assessment covers the requirements that are germane to the merchant. Including this type of conformity assessment methodology for the Executive Order framework recognizes the differences between smaller and larger organizations.

Conformity assessments are a foundational practice for ensuring that cybersecurity practices and controls are operating effectively. Establishing conformity assessments needs to be evaluated to ensure that the reviews follow established repeatable processes that remove subjectivity as much as possible. Any conformity assessment needs to balance a "check-list" approach versus a technical performance based approach to assessments. NIST has a unique opportunity as part of the Presidential Executive Order to develop a consensus based conformity assessment practice associated with the consensus based framework. Building upon the ES-C2M2 framework as a very strong foundation for the "check-list" conformity assessment approach and the mandatory NERC CIP performance based audits, NIST can facilitate establishing the repeatable technical performance based conformity assessment practices (i.e. vulnerability testing, patch management verification, malware detection practices, etc.)

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?

Within the electricity subsector several approaches already exist:

1.) The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards. These are mandatory and enforceable cybersecurity standards that carry significant penalties and sanctions for non-compliance. The standards are industry developed through a public-private partnership. The NERC Board of Trustees approve the standards when an industry quorum ballot is reached. Ultimately, as required by Section 215 of the Energy Policy Act of 2005, the Federal Energy Regulatory Commission (FERC) has to formally adopt the standards. Once FERC adopts the standards they become mandatory and enforceable.

CIP version 3 is the currently enforced version of the standards. These standards cover the following domains: 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. The fourth version of the CIP standards have been adopted and become enforceable in April 2014. A subsequent fifth version of the standards has been approved by industry, approved by the NERC Board of Trustees and is currently under review by FERC for adoption. It is important to highlight the industry ballot approval percentages exceeded 90%. This is the highest acceptance vote relative to all previous versions of the standards.

2) Department of Energy Risk Management Process. This is a public-private guideline tailored for the electric sub-sector from the National Institute of Standards and Technology (NIST) Special Publication 800-39, *Managing Information Security Risk*. While the RMP was tailored for the electricity sector, this could also be tailored and used by any of the critical infrastructures; using the same foundational NIST Special Publication. As described above, this guideline establishes a repeatable process that allows entities to assess cyber risk in a linear manner over three tiers: (1) Organizational tier (executive leadership), (2) Mission and Business Processes (the supporting processes to the organization operations identified in the top tier), and (3) the Information Technology and Industrial Control System (the actual systems). Within each of these tiers there is a systematic risk cycle with four circular steps: Risk Framing, Risk Assessment, Risk Response and Risk Monitoring. The systematic and circular nature of the Risk Management Process allows entities to perform discrete assessment against a specific operational aspect and repeat the process throughout the entire organization.

3) Department of Energy Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2). This framework was developed for the electricity subsector as a measure of cybersecurity program maturity. The model identifies objectives and practices over 10 domains: (1) Risk Management, (2) Asset, Change and Configuration Management, (3) Identity and Access Management, (4) Threat and Vulnerability Management, (5) Situational Awareness, (6) Information Sharing and Communication, (7) Event and Incident Response, Continuity of Operations, (8) Supply Chain and External Dependencies, (9) Workforce Management, and (10) Cybersecurity Program Management. While it was developed for the electricity sector, it can easily be adopted

for other critical infrastructures. Marrying this framework with the RMP can create a holistic risk management framework from risk assessment and treatment to maturity.

4) National Institute of Standards and Technology (NIST) Special Publications and Interagency Reports. These guidelines may used as a source of best practices for implementing cybersecurity practices. Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations,* specifically contains a risk based selection of controls. The approach of SP800-53 risk selection of "high, moderate, low" has also been integrated into the latest revision to the NERC CIP mandatory cybersecurity standards. Using the NERC CIPs as a baseline, along with the analysis from the RMP, a proper risk based selection of controls can be selected. Finally, using the ES-C2M2 framework, a capability maturity benchmark of the cybersecurity program can be measured.

Additionally, NIST Special Publication 800-82, *Guide to Industrial Control Systems (ICS) Security* provides actionable program and control guidance for addressing threats and vulnerabilities to supervisory control and data acquisition (SCADA) systems. NIST's Interagency Report 7628, *Guidelines for Smart Grid Cyber Security* provides the electricity subsector with guidelines and controls related to the implementation of emerging Smart Grid systems.

5) Payment Card Industry Data Security Standards (PCI DSS). For companies that process credit cards payment card information, the PCI DSS standards are required to ensure that credit card information is properly safeguarded. These standards were drafted by the credit card companies and promulgated to merchants. The standards require annual assessments and certification of conformance to the requirements. The standards covers six domains and twelve requirements: Build and maintain a secure network, Protect Cardholder Data, Maintain a Vulnerability Management Program, Implement Strong Access Control Measures, Regularly Monitor and Test Networks, and Maintain an Information Security Policy. Depending on the type of merchant and type of data that is processed, there are different levels of assessment and certification required.

6) International Standards Organization (ISO) 27000 series. These are a collection of international guidelines developed by International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The standards contain best practices for the implementation of cybersecurity programs, controls and practices.

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

While the NERC CIPs were created directly for the electric sector, they are a robust framework of practices that can be easily tailored for other sectors.

Additionally, all of the guidelines and standards identified above could apply across multiple sectors with proper analysis of the unique attributes associated with risk and the requirements of confidentiality, integrity and availability.

3. *Which organizations use these approaches?*

Many organizations use these approaches in the development of the cyber programs. In the case of this respondent, a community owned municipal utility district providing retail electric service to approximately 600,000 customers over 900 square miles in the capitol of California is using these approaches.

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

Practically, each of the approaches sets forth foundational practices for cybersecurity. Because there are so many different frameworks and guidelines written and developed for different needs, conflicts exist with the degree of controls. In some cases, there is no universal set of conformity assessment practices that provides repeatable objective review of efficacy. There are varying degrees of prescriptive and proscriptive requirements that create conflicts with wholesale adoption of guidelines. Typically, for those sectors such as the electric subsector with mandatory and enforceable cybersecurity standards, the use of other guidance must be tempered to ensure any conflicts are mitigated.

Additionally, because cybersecurity threats and vulnerabilities are constantly evolving, usually faster than guidance and standards, it is imperative the appropriate level of actionable threat and vulnerability information is available to the owners and operators of critical infrastructure to ensure that the selected practices and controls are meeting the objective to reduce risk. Additionally, with actionable threat and vulnerability information organizations can be more agile in their ability to respond to emerging threats and modify their control selections accordingly ahead of the formal guidance.

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

First and foremost is recognizing the existing mandatory enforceable cybersecurity standards have to be a primary input and cannot be in conflict with the development of a cross-sector framework. Secondly, harmonizing the different approaches to create one baseline framework allowing for organizational size and complexity constraints to factor into "how much" and "how far" these approaches go within an organization. Implementing practices for the sake of a "check-list" will not itself necessarily improve the organization's cybersecurity posture. We must remain mindful that risk management must be at the foundation of any framework. For instance, the DOE RMP and NIST 800-39 guidelines include the identification of the threats and vulnerabilities measured against the value of the targets and capabilities of the threat actors.

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

The NERC CIP standards identify the critical assets and associated cyber assets that relate to the reliable operation of the bulk electric system (BES). This methodology took into account the unique attributes of the electric subsector and the BES and developed controls that do not inhibit the availability requirements of the systems. The DOE RMP and ES-C2M2 guidelines that were developed specifically for the electric sector provide the electric sub-sector with the ability to assess cybersecurity risk and measure the maturity of the cybersecurity program in a utility setting.

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

There is applicability for both approaches. The electricity subsector already has mandatory and enforceable cybersecurity standards development process that follows ANSI certified practices. Additionally, the subsector has developed other cyber risk management and cyber capability maturity measurement guidelines. It is important to caution that existing sector-specific development processes (e.g. NERC CIP) needs to be retained and should be an input to other development processes. Because each sector has different threat and vulnerability profiles, the creation of sector-specific voluntary frameworks may be necessary to ensure that the selection of controls and attempts at risk reduction do not impede upon another 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 sector-specific agencies (SSA) and coordinating councils (CC) can play an important role in communicating with industry on the threats and vulnerabilities. Since the SSA's and CC's have a closer alignment with the operations of their sector, they have a unique opportunity to bring together industry to develop case studies related to the implementation and adoption of the framework. These case studies can be used to develop uniformity across the sector. The SSA's and CC's have specific understandings of the unique attributes of their sector and can assist with the development of risk based measures so the adoption of the framework is commensurate with risk and operations of the sector organization.

9. What other outreach efforts would be helpful?

The SSA's and CC's can be the coordinators in the establishment of the public-private partnerships with industry as well as establishing collaboration across sectors. Where there are interdependencies between critical infrastructures, there is an opportunity for the SSA's and CC's to create information sharing and analysis that can be used to facilitate cross-sector understanding of threats and vulnerabilities. The SSA's and CC's can leverage economies of scale across sectors to improve the overall national cybersecurity posture. Using the Information Sharing and Analysis Centers (ISAC) for each sector, organizations can share with the ISAC specific log information that the ISAC can then use to correlate events across their sector and create reports and analysis as needed. Additionally, the SSA's and CC's can be an aggregator among the different critical infrastructures of log information to create a view across sectors and across interdependent sectors. From a public-private perspective, developing this scale of bi-directional security information has the potential to dramatically increase the security posture of each sector and the nation.

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 widely used to some degree within the electric subsector. These practices are foundational elements to the mandatory and enforceable NERC CIP cybersecurity standards.

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

The practices can be found within the International Standards Organization 27000 series cybersecurity practices from the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

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

All of these practices are important for the secure operations of critical infrastructure. It is the degree of implementation that needs to be managed to ensure that implementation of these controls do not impede the reliable operations of the systems and business processes. The degree of implementation needs to be balanced with the overall risk (i.e. threats, vulnerabilities, and likelihood/consequence of harm) to the systems.

Referencing the specific practices listed in this section, the "separation of business from operational systems" is one of the most critical controls for the secure operation of critical infrastructure. The implementation of this practice can greatly reduce the overall attack surface. It is important for organizations to use this practice to create a clear demarcation in their network and system architectures. The sensitivity related to operational systems is much different than the sensitivity related to corporate systems.

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

All of these practices are applicable to the electric sub-sector to some degree. Care must be taken to review the risk justification for the use of these practices.

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

There have been some challenges with the degree of implementation in the areas of encryption and log management. Due to the latency and legacy system limitations the introduction of robust encryption practices can hinder the required availability of systems. The supervisory control and data acquisition (SCADA) systems have traditionally limited processing speed and memory with sub-milisecond response requirements; the introduction of traditional encryption methods can result in adverse affects to power operations. Moreover, many of these devices were developed without sufficient processing for log management and access controls. Utilities must use other compensating methods to achieve some of these controls. Specifically, the NERC CIP standards recognize the technical feasibility constraints with some of these practices allowing utilities to submit documented exceptions to the strict adherence to the standards. NERC CIP Standard 005, R2.4 provides capability for a technical feasibility where "strong procedural or technical controls" cannot be implemented to "ensure authenticity of the accessing party." In some cases, manufacturers are still not fully adopting cybersecurity practices and are not delivering solutions that deliver these capabilities adding complexity to utility implementations.

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

For the electric sub-sector, the NERC CIP standards are mandatory enforced cybersecurity standards. The practices highlighted are included within the NERC CIP standards. The implementation of the practices identified in the standards are institutionalized and practiced continually. Regular review of compliance with the NERC CIP standards is measured continuously to identify gaps. Every three years NERC registered entities are subjected to performance audits to substantiate their compliance to the NERC CIP standards. For organizations that are classified as merchants under the PCI DSS cybersecurity standards for credit card payment card information, they are also continuously assessing their environments to ensure conformance. Annually the merchant organizations are subjected to audits to substantiate their compliance to the requirements.

The selection and use of other guidance documents are used as supplementary input to SMUD's cybersecurity program. Where mandatory enforceable standards do not exist, the guidance documents provide a basis of mapping best practices to assist in the development of justifications for business adoption and funding by executive leadership.

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

SMUD uses its existing resource allocation practices to determine the proper allocation of business resources. SMUD has established and reviews annually the staffing summaries across the organization to ensure a commensurate investment in the standards development lifecycle. External to SMUD, resources have been assigned to participate in the development of industry standard and guidelines. The IT Director has been a core drafter on the NERC CIP Drafting Team for version four and five of the standards. Additionally, the Information Security Officer has been a drafter of several DOE and NIST guidance documents, has acted as the vice chair of the Smart Grid Interoperability Panel.

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

Through either a regulatory compliance function or information security function, there is an escalation process based on new threat and vulnerability information. Specifically, for the electric subsector governed under the NERC CIP standards, entities are required to review vulnerability information within a specific timeframe and evaluate the risks to their operations and the bulk electric system. Entities are required to report suspected cyber events to the Electricity Sector –

Information Sharing and Analysis Centers. Disturbances to the reliability of the bulk electric system are required to be reported to DOE.

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

There seems to be a very limited affect to consumer privacy and civil liberties in the development of a framework and application of these practices. There is no expectation that access will be granted to confidential customer information beyond what is already legally mandated. Conversely, we expect that privacy and civil liberties protections will be improved through the adoption of risk reduction practices.
From an organizational perspective, there are concerns with privacy related to the information sharing of corporate security information. Where companies must share event logs to address a cybersecurity risk, there needs to be practices in place to enforce non-disclosure. There must also be measures implemented to ensure that there will be no risk to exposure to compliance violations or penalties for participation in information sharing, as well as liability protection.

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

Not Applicable.

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

Risks to privacy and civil liberties needs to follow the Fair Information Practice Principles (FIPPS): *Transparency* – provide notice to the individual regarding collection, use, dissemination, and maintenance of personally identifiable information (PII); *Individual Participation* – involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. Provide mechanisms for appropriate access, correction, and redress regarding use of PII; *Purpose Specifications* - specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used; *Data Minimization* - only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s); *Use Limitation* - use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected; *Data Quality and Integrity* - to the extent practicable, ensure that PII is accurate, relevant, timely, and complete; *Security* - protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure; *Accountability and Auditing* - accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

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

At a cross-sector perspective, the development of a framework that focuses on commonly accepted hygiene controls, such as the items found in SANS Top 20 Critical Security Controls (http://www.sans.org/critical-security-controls/) and the Open Web Application Security Project (OWASP) Top 10 Project for securing web applications would provide a significant cross-sector framework foundaton (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project). Both of these projects are constantly being updated based on new research and identification of new threats and vulnerabilities. The maintenance of these two bodies of controls is positive evidence of how cybersecurity risk and controls can be managed in a constantly evolving landscape.

The following list provides details of the current listing of the SANS Top 20 Security Controls:

Critical Control 1: Inventory of Authorized and Unauthorized Devices
Critical Control 2: Inventory of Authorized and Unauthorized Software
Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
Critical Control 4: Continuous Vulnerability Assessment and Remediation
Critical Control 5: Malware Defenses
Critical Control 6: Application Software Security
Critical Control 7: Wireless Device Control
Critical Control 8: Data Recovery Capability
Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps
Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services
Critical Control 12: Controlled Use of Administrative Privileges
Critical Control 13: Boundary Defense
Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs
Critical Control 15: Controlled Access Based on the Need to Know
Critical Control 16: Account Monitoring and Control
Critical Control 17: Data Loss Prevention
Critical Control 18: Incident Response and Management
Critical Control 19: Secure Network Engineering
Critical Control 20: Penetration Tests and Red Team Exercises

Listing of the OWASP Top Ten Project security controls:

A1 Injection
A2 Broken Authentication and Session Management (was formerly A3)
A3 Cross-Site Scripting (XSS) (was formerly A2)
A4 Insecure Direct Object References
A5 Security Misconfiguration (was formerly A6)
A6 Sensitive Data Exposure (merged from former A7 Insecure Cryptographic Storage and former A9 Insufficient Transport Layer Protection)
A7 Missing Function Level Access Control (renamed/broadened from former A8 Failure to Restrict URL Access)
A8 Cross-Site Request Forgery (CSRF) (was formerly A5)
A9 Using Known Vulnerable Components (new but was part of former A6 – Security Misconfiguration)
A10 Unvalidated Redirects and Forwards

Three additional practice areas that are important candidates are supply chain security, recruitment of a skilled workforce and cybersecurity awareness and training. Over the past two years there has been considerable breaches of suppliers of technology. In many cases these breaches have been a source of espionage and reconnaissance. Threat actors' capabilities have continued to increase at a rapid pace. Owners and operators need to have assurance that their suppliers are implementing commensurate cybersecurity practices.

Additionally the development of well trained workforce that is skilled in the identification of risks associated with threats and vulnerabilities is critical to improving the overall offensive and defensive cybersecurity posture. Encouraging organizations to establish a dedicated cybersecurity workforce, and providing sufficient ongoing education related to risk management practices and vulnerability assessment will also help to ensure organizations can recruit and retain the expertise needed for cyber defense.

The final area for consideration is cybersecurity awareness and training. It is imperative that there be not only a well skilled cybersecurity workforce, but also a well skilled corporate workforce who understand how they play a part in the defense of corporate networks. The establishment of robust corporate cybersecurity awareness and training programs is necessary to maintain a heightened awareness throughout every layer of an organization. Just as there are safety programs, there needs to be cybersecurity safety programs that provide the tools to the workforce to combat the tactics of the threat actors.

SMUD appreciates the opportunity to provide these comments, and looks forward to working with NIST to further develop the framework.

Respectfully submitted

Laura Lewis cdm

Laura Lewis
Assistant General Counsel
Sacramento Municipal Utility District