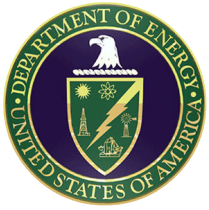
Response to National Institute of Standards and Technology's Request for Information "Developing a Framework to Improve Critical Infrastructure Cybersecurity"

April 8, 2013

DISCLAIMER

The views expressed herein are those of select United States Department of Energy employees and are provided solely to inform the NIST framework development process, and should not be interpreted as an official legal or policy position of the Department of Energy.

Department of Energy



Current Risk Management Practices

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

The 2011 "Roadmap to Achieve Energy Delivery Systems Cybersecurity" was developed with public-private collaboration and describes challenges to improving cybersecurity across the energy sector. Key barriers identified include:

- Cyber threats are unpredictable and evolve faster than the sector's ability to develop and deploy countermeasures
- Security upgrades to legacy systems are limited by inherent limitations of the equipment and architectures
- Performance/acceptance testing of new control and communication solutions is difficult without disrupting operations
- Threat, vulnerability, incident, and mitigation information sharing is insufficient among government and industry
- Historically weak business case for cybersecurity investment by industry
- Regulatory uncertainty in energy sector cybersecurity

The Roadmap provides a strategic framework to achieve the vision that resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber-incident while sustaining critical functions. It describes cybersecurity considerations for energy delivery systems along with trends and drivers affecting future energy delivery systems security.

The Roadmap is available at http://energy.gov/oe/downloads/roadmap-achieve-energy-delivery-systems-cybersecurity-2011.

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

With regard to the energy sector, the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure are that cyber infrastructures in different critical sectors have unique characteristics, are designed to meet different requirements, and may face different types and levels of risks. A one-size-fits-all approach for cross-sector standards may not deliver the optimal value at sector level. The need to arrive at a consensus on cross-sector standards may dilute any agreed standard to reduced effectiveness.

Cross-sector standards addressing operational systems may require numerous caveats to accommodate unique functions, processes and circumstances. These exceptions will have to be addressed without causing confusion or rendering the standards ineffective. Such limitations may be less applicable to cross-sector standards addressing business enterprise networks.

A cross-sector standards based framework will also need to account for the varying risk considerations and thresholds of different sectors. A risk-based approach will ensure that standards are scalable and effective.

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?

With regard to the energy sector, the Department of Energy (DOE) encourages and supports the sector's adoption of industry best-practices for cybersecurity risk management policies and procedures. Organizations may derive their cybersecurity risk management policies and procedures from a wide array of approaches e.g. North American Electric Reliability Corporation (NERC) Critical Cyber Asset determination guidance, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, NIST SP 800-39, DOE Order 205.1B, and DOE/OE-0003. Organizations may communicate and oversee these policies and procedures via senior management teams or leads aligned to specific business line or function.

In 2012, DOE published the Electricity Subsector Cybersecurity Risk Management Process (RMP) Guideline. The RMP Guideline was developed by public-private collaboration and may be used to implement a new cybersecurity risk management program within an organization or to build upon an organization's existing internal cybersecurity policies, standard guidelines, and procedures. The guideline is available at http://energy.gov/oe/services/cybersecurity/cybersecurity-risk-management-process-rmp.

With regard to the DOE complex, DOE policies and procedures governing risk generally and cybersecurity risk specifically are based on the Federal Information Security Management Act of 2002 (FISMA). These includeNIST SP 800-53 and Federal Information Processing Standards (FIPS) 199.

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

With regard to the energy sector, the size and operations of the organizations impact the position of organization's cybersecurity risk management program/office.

Generally, an Information Technology (IT) function manages business systems and networks, whereas an Operational Technology (OT) function manages industrial control systems. Either or both offices may conduct cybersecurity risk management activities. In larger organizations cybersecurity risk management program/office may be located within the office of the Chief Information Officer. In smaller organizations the senior leader responsible for cybersecurity may not be part of the executive leadership.

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

With regard to the energy sector, risk management practices vary from one organization to other and may be driven by business needs, goals or compliance mandates. Assessment of threats tends to depend on open source and unclassified materials. As an example, NERC standards are a minimal requirement for the Bulk Electric System (BES); whereas

NIST SP 800-37, NIST SP 800-39, DOE Order 205.1B and DOE/OE-0003, NIST Interagency Report (NISTIR) 7628, and NIST SP 800-53 may be used elsewhere. Depending upon the organization's leadership and resources, practices beyond the standards are as individual as the organizations themselves.

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

With regard to the energy sector, cybersecurity risk is generally used as a point of consideration for making business decisions. It is a subset of the enterprise risk management program. The extent of incorporation of cybersecurity risk into organizations' overarching enterprise risk management is dependent on the resources and maturity of the organization. For energy sector organizations, especially in the electricity subsector, cybersecurity risk management activities are driven by compliance requirements and audits. This sometimes results in energy organizations incorporating cybersecurity into their compliance functions instead of an overarching enterprise risk management function.

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

With regard to the energy sector, a wide variety of standards, guidelines, and practices are used. Examples include but are not limited to:

- DOE's "Electricity Subsector - Cybersecurity Capability Maturity Model (ES-C2M2)" and "RMP Guideline"
  http://energy.gov/oe/downloads/electricity-subsector-cybersecurity-capability-maturity-model-may-2012
  http://energy.gov/oe/downloads/cybersecurity-risk-management-process-rmp-guideline-final-may-2012

- The President's Critical Infrastructure Protection Board and the DOE's "21 Steps to Improve Cyber Security of SCADA Networks"
  http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf

- Department of Homeland Security's (DHS) "Cyber Security Procurement Language for Control Systems" and "Chemical Facilities Anti-Terrorism Standards" (CFATS)
  http://ics-cert.us-cert.gov/pdf/FINAL-Procurement_Language_Rev4_100809.pdf
  http://www.dhs.gov/chemical-facility-anti-terrorism-standards

- NIST's "NISTIR 7628 Guidelines for Smart Grid Cyber Security"
  http://csrc.nist.gov/publications/PubsNISTIRs.html

- NERC's "Critical Infrastructure Protection - Cybersecurity" reliability standards
  http://www.nerc.com/page.php?cid=2|20

- The American Petroleum Institute (API) standard "API 1164 Pipeline SCADA Security"
  http://www.techstreet.com/api/products/1629005

- The American Gas Association's "AGA-12 Cryptographic Protection of SCADA Communications General Recommendations" http://www.aga.org/Pages/default.aspx

- ISACA's "Control Objectives for Information and Related Technology (COBIT)" framework http://www.isaca.org/COBIT/Pages/default.aspx

- The Committee of Sponsoring Organizations of the Treadway Commission's (COSO) "Enterprise Risk Management - Integrated Framework" http://www.coso.org/erm-integratedframework.htm

- The Payment Card Industry (PCI) Security Standards Council's "Payment Card Industry Data Security Standard (PCI DSS) https://www.pcisecuritystandards.org/security_standards/

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?

With regard to the energy sector, Sarbanes Oxley (SOX), Federal Energy Regulatory Commission (FERC) rules, NERC reliability standards, and DOE FormOE-417 provide some of the current reporting requirements. The federal Power Marketing Administrations (PMAs) have FISMA reporting requirements as well.

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

With regard to the energy sector, organizations have a wide range of critical assets with interdependencies within the sector, e.g., natural gas or dams for generation assets. An organization's critical assets also have dependencies on its supply chain.

Other critical infrastructure sectors such as (but not limited to) Telecommunications, Transport, and Health are dependent on the energy sector.

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

With regard to the energy sector, in addition to business mission and goals regulatory requirements may also dictate performance goals. For the electricity subsector, FERC Orders and NERC Standards identify performance goals for reliability.

Energy sector organizations also adhere to regulations and recommendations at the state level. The National Association of Regulatory Utility Commissioners (NARUC) which represents the State Public Service Commissioners who regulate essential utility services, provides guidelines and programs such as the Cybersecurity for State Regulators: http://www.naruc.org/grants/Documents/NARUC%20Cybersecurity%20Primer%202.0.pdf.

The ES-C2M2 is a maturity model that can be used to measure performance on an enterprise-wide or functional basis (e.g., generation, transmission, distribution, markets, etc.). Organizations can evaluate the extent of their implementation of the cybersecurity practices listed in the model and determine their Maturity Indicator Level (MIL). The MILs indicate the level of sophistication of the organization's cybersecurity practices. The model does not prescribe an "ideal" maturity indicator level. The desired level is based on the organizations own risk tolerance. The model is described in further detail in response to Question 1 in the "Use of Frameworks, Standards, Guidelines, and Best Practices" section.

Further analysis is needed to determine whether existing performance goals are appropriate for cybersecurity risk faced by the sector.

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?

With regard to the energy sector, organizations have reporting requirements from their regulators – generally minimal information initially, and further information upon request.

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

Standards organizations may facilitate conformity assessment by providing guidance and interpretation of the standards. The US energy sector is interconnected with Mexico and Canada and therefore both national and international standards organizations may need to partner in standards development and in guiding organizations with respect to conformity assessment.

Use of Frameworks, Standards, Guidelines, and Best Practices

1. What additional approaches already exist?

Examples of frameworks, standards, guidelines, and best practices used in the energy sector include products from various organizations and associations e.g., NERC, NIST, API, AGA, National Association of State Energy Officials (NASEO), North American Energy Standards Board (NAESB), International Organization for Standardization, (ISO), International Electrotechnical Commission (IEC), American National Standards Institute (ANSI), Edison Electric Institute (EEI), Large Public Power Council (LPPC), National Rural Electric Cooperative Association, EnergySec, Electric Power Research Institute, Inc (EPRI), Interstate Natural Gas Association of America (INGAA), etc. For details about these products please refer to the organizations' websites.

A number of approaches also exist in the form of tools and methods. Some of the DOE products are explained below:

- LEMNOS: Utilities spend significant time investigating the functional features of new cybersecurity products to ensure they deliver the right solution, and at the same time are compatible with the products in their current system. Lemnos simplifies this process. The Lemnos profiles provide a standard configuration for vendors to use when building a variety of functions into their security products. The result is interoperable products from different vendors that can securely communicate and easily integrate. This simplifies a utility's buying process and increases product options for utilities**.** The Lemnos profiles also build in security features that improve productivity, such as central administration, which saves operators time by improving the efficiency of access management; remote access, which allows operators to observe and send commands to remote devices from a central location; and central log collection that eases compliance with NERC Critical Infrastructure Protection (CIP) logging rules. Details of the Lemnos security program are available at http://energy.gov/oe/downloads/lemnos-interoperable-security-program

- ASAP-SG: The Advanced Security Acceleration Project for the Smart Grid (ASAP-SG) is a public-private partnership to accelerate standards development for secure and resilient Smart Grid architectures. ASAP-SG has developed security profiles for key electric grid domains including advanced metering infrastructure, third-party data access, and distribution management, Wide-Area Monitoring, Protection, and Control (Synchrophasors), and a security profile for Substation Automation. The ASAP-SG has also published a Smart Grid Security Profile Blueprint and a white paper entitled "How a Utility Can Use ASAP-SG Security Profiles" that help clarify the frameworks, tools, and methods needed to create and customize smart grid domain-specific security profiles that should be applied to the procurement, implementation, and configuration of smart grid systems.

- ES-C2M2: The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) is a public-private collaboration effort to support the ongoing development of cybersecurity capabilities across the electricity subsector. The objectives of ES-C2M2 are to:

- Strengthen cybersecurity capabilities in the electricity subsector by identifying capability gaps of individual organizations as well as provide an aggregated picture of common capability gaps across the nation
- Enable sector owners and operators to effectively and consistently evaluate and benchmark cybersecurity capabilities based on risk, allowing for better informed investment decisions
- Share knowledge, best practices, and relevant references within the subsector as a means to improve cybersecurity capabilities
- Build effective cybersecurity programs (people, processes, and technology) within each organization across the industry, equipping them with the capacity to respond quickly and effectively to cybersecurity threats.

The ES-C2M2 is a scalable framework that can be used to develop capabilities and measure performance on an enterprise-wide or functional basis (e.g., generation, transmission, distribution, markets, etc.). It provides a common set of cybersecurity practices, logically grouped into ten domains, and designed to support specific objectives that help utilities build their cybersecurity capabilities and improve their overall resiliency. Utilities can measure their performance against each domain using the maturity indicator levels (MILs) as defined within the ES-C2M2. The MILs indicate the level of sophistication of utilities' cybersecurity practices within a specific domain.

Utilities may voluntarily request DOE to facilitate a Self Evaluation. A DOE Facilitated Self-Evaluation consists of an on-site visit by members of the ES-C2M2 team to provide guidance and assistance in evaluating the organization's cybersecurity capabilities through the use of the Cybersecurity Self-Evaluation Toolkit. The ES-C2M2 team is there to answer questions about the underlying concepts of the ES-C2M2 domains, objectives, and practices and facilitate discussion of the organization's cybersecurity program. Requests for the ES-C2M2 Toolkit, program information, or facilitated self-evaluations can be sent to ES-C2M2@HQ.DOE.GOV . The ES-C2M2 model document is available at http://energy.gov/oe/downloads/electricity-subsector-cybersecurity-capability-maturity-model-may-2012

The DOE is developing data collection capabilities in order to receive ES-C2M2 Self Evaluation results from individual organizations and develop a comprehensive national picture of the electricity subsector's cybersecurity capabilities. The collection of Self Evaluation data will enable the DOE to:

- Benchmark cybersecurity capabilities across various segments of the electricity subsector and share with individual organization's their performance compared to their peers
- Provide benchmark data that can inform organizations' planning and prioritization for cybersecurity investments
- Identify best practices and advanced cybersecurity capabilities that can be leveraged across the industry

- Inform other federal partners' strategies for cybersecurity investments, including programs and research
- Develop and prioritize the DOE's cybersecurity investments based on common challenges within the electricity subsector, including programs and research in new tools and solutions

- RMP: The Risk Management Process (RMP) Guideline was developed by the DOE, in collaboration with the NIST, the North American Electric Reliability Corporation (NERC), and representatives from both the public and private sectors.

  The RMP is designed to enable organizations—regardless of size, organizational or governance structure—to apply effective and efficient risk management processes tailored to meet the organization's unique mission and business needs. The process recognizes organizational constraints (resources, personnel, policy). It helps identify ownership of risk within the organization and facilitates resource allocation based on risk management principles.

  The RMP guideline may be used to implement a new cybersecurity risk management program within an organization or to build upon an organization's existing internal cybersecurity policies, standard guidelines, and procedures. It is based on the NIST *SP 800-39: Managing Information Security Risk* and is tailored for the electricity subsector. The RMP not only addresses risks from Information technology and industrial control systems but also from the increasing integration of Industrial Control Systems (ICS) with traditional business IT that provides corporate services (e.g., network, email). Other sectors such as Water, Dams, Oil and Natural Gas with similar technology trends may also benefit from this guideline.

  DOE is currently planning to facilitate pilot RMP implementations in the electricity subsector. Program information or requests to facilitate voluntary pilots can be sent to RMPGuideline@HQ.DOE.GOV

2. Which of these approaches apply across sectors?

Most of the NIST guidelines pertaining to cybersecurity risk management are applicable across sectors. Some of the standards or approaches developed by organizations like NERC, API and EPRI may be specific to the energy sector; others may be scalable across sectors. The DOE products such as Lemnos, ASAP-SG, ES-C2M2 and RMP are scalable across sectors. These were developed by energy sector subject matter experts for the subsector but can be tailored according to the unique characteristics and needs of other sectors. DOE has received inquiries from other sectors and agencies that are interested in adopting the ES-C2M2 and is currently planning to work with the Oil and Natural Gas subsector to develop an ONG version.

3. Which organizations use these approaches?

Different energy sector organizations may employ different standards and approaches. Examples of use of DOE products are as follows:

- 10+ power grid security device vendors are using Lemnos in developing energy delivery system solutions
- The ES-C2M2 model document is freely available for download. Since June 2012, 210 individuals representing 109 US electric utilities, 82 non-utilities and 19 international organizations have requested and received the ES-C2M2 Toolkit that is used along with the model document.
- Since June 2012, 15 electric subsector organizations have voluntarily requested DOE Facilitated Self-Evaluations, 8 have been completed successfully and 7 are scheduled to be completed in the upcoming months. Because the model and toolkit are freely available, the number of organizations that performed Self-Evaluation on their own is not currently tracked and is thus unknown.
- Because the RMP is freely available for download, the number of organizations that use the RMP on their own is not tracked and is thus unknown.

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

Standards and approaches tend to become audit guidelines and the application of and attainment of these approaches becomes a goal in itself. This discourages innovative risk management and commits resources to compliance-based processes.

Each standard, framework, guideline, tool or method may have its unique focus and thus may be inherently limited if used in a way for which it is not designed. The ES-C2M2 identifies where an entity's maturity level is, and provides results that can be used for planning; but does not prescribe controls or process steps for any gaps that are identified. So, the model may help organizations measure and strengthen incident management capabilities but will not provide instructions for containing an incident that the organization may be facing.

In addition, standards and guidelines take a long time to develop and obtain industry acceptance for implementation. Thus, they may not be able to keep up with the continually changing threat landscape and may become ineffective for incident management.

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

These approaches would be more useful if supplemented with implementation guidance and recommendations. In addition, some aspects of audits could be replaced with facilitated exercises, resulting in a focus on strengthening cybersecurity as opposed to ensuring compliance.

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

Most of the NIST guidelines pertaining to cybersecurity risk management are applicable across sectors. Some of the standards or approaches developed by organizations like NERC, API and EPRI may be specific to the energy sector; others may be scalable across sectors. The DOE products such as Lemnos, ASAP-SG, ES-C2M2 and RMP are scalable across sectors. These were developed by energy sector subject matter experts for the subsector but can be tailored according to the unique characteristics and needs of other

sectors. Key sector-specific needs that need to be accounted for the energy sector are as follows:

- Energy control systems are uniquely designed and operated to control real-time physical processes that deliver continuous and reliable power to support national and economic security. As such, they require security solutions that meet unique performance requirements, design, and operational needs.
- Cyber security technologies that are developed to protect business IT computer systems and networks can break an energy delivery control system. The computers and networks that control our Nation's power grid are very different from those on our desks in several important ways. These differences must be respected when securing these systems against cyber-attack.
- Energy delivery system communications must be fast. Data communications in substations require time-critical responses of less than 4 milliseconds for protective relaying, and technologies to provide wide-area situational awareness for transmission lines require data communications links with time delays of less than a second. A cascading power failure might be prevented by changing how power flows through the grid, but this change must often be brought about in a few milliseconds. Energy delivery system computers and networks must always be available. They cannot be patched or upgraded without extensive testing and validation, normally planned weeks or months in advance, to ensure that the change does not jeopardize power system operations, and the vendor's warranty for these systems can sometimes prevent the change from being implemented at all. Energy delivery systems include decades-old legacy components with limited resources for computation, and limited bandwidth for communications. These legacy devices perform their function well so there is no business case to replace them, but they were designed decades ago when the internet did not exist and cybersecurity was not a central concern.
- Energy delivery systems have predictable communication patterns, and predictable behavior. So it makes sense to allow only expected actions and deny any others. In contrast, desktop cybersecurity measures often allow any actions not explicitly denied. Energy delivery systems require complex access controls, including secure remote access for maintenance and operations support. Multiple energy-workers need different levels of access to the same device, and these access needs can change depending on operating mode. Most importantly, access controls must never jeopardize system availability as this could represent a safety hazard during an emergency response. Energy delivery systems have critical components that are widely distributed across extensive territories, and are, by necessity, located outside where they are vulnerable to physical tampering. Finally, control systems security involves ensuring the timely and proper operation of cyber-physical devices (e.g., opening a digital relay or changing settings on transformers). Thus, cyber attacks on control systems can cause physical damage to expensive electric grid components like generators that can take many months to replace.

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

Yes. There should be sector-specific standards development processes or voluntary programs. While sector regulators may have minimal standard requirements for the sector

in alignment with national reliability needs, there should also be approaches that facilitate identification and adoption of practices beyond minimal requirements. Entities choosing to adopt these practices approaches may do so on a voluntary basis, and may be compensated in some manner for doing so. The potential incentives should be reviewed as per the Executive Order. The ES-C2M2 is an example of such an approach.

NIST should identify, review, and facilitate de-confliction of overlapping standards e.g. NERC CIP and NIST Guidelines.

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 related sector coordinating councils (SCC) can play the following role to support these approaches:

- Conduct research & development
- Facilitate piloting and testing of tools and technologies
- Facilitate exercises to promote and test capabilities
- Identify sector specific best-practices through research, benchmarking, and review of sector incidents
- Identify standards and guidelines with overlapping requirements or recommendations
- Assist in adding specificity to cross-sector standards
- Provide implementation guidance to establish and enforce common sector-specific approaches

9. What other outreach efforts would be helpful?

SSA's could work with sector stakeholders to ensure critical asset owners and operators participate in the planned NIST Cybersecurity Framework Workshops.

The SSAs can provide an additional platform for (local, regional, or national) conferences to identify areas of weakness, areas of strengths, and address sector-specific needs for the Cybersecurity Framework development process.

Both SSAs and SCCs can promote the approaches through multiple means of communications, e.g., speaking engagements, social media, bulk email, leadership engagements.

Specific Industry Practices

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?

An organization's practices are a result of numerous factors, e.g., business needs; technical needs; regulations; vendor recommendations; guidelines; resources; and organizational maturity. Compliance requirements may drive some energy sector organizations to employ these practices at a minimum baseline security level. Others, depending on their resources and maturity, may implement these practices well beyond the compliance requirements.

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

These practices are generally addressed in existing international standards and practices as well, e.g., ISO/IEC 27002 and 15408.

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

Separation of business from operational systems, Identification and authorization of users accessing systems, and Monitoring and incident detection tools and capabilities are generally seen as being the most critical for the secure operation of energy critical infrastructure.

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

All practices listed above have applicability in the energy sector.

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

From a technical perspective, encryption and key management may pose the most significant implementation challenge. From an organizational perspective, asset identification and management may pose the most significant implementation challenge.

Some of the unique energy sector challenges to implementation of standard security practices are:

- patching of software for control systems
- testing of system upgrades in a timely and efficient manner
- monitoring access to assets located in areas that are easily accessible to others

- penetration testing on "live" systems
- monitoring of networks with diverse communication methods and protocols
- changing access controls on thousands of devices and networks that may be physically located in very remote regions

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

How organizations utilize standards or guidelines in the implementation of these practices is dependent on the resources, maturity and compliance requirements of the organization.

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

Existence of a resource allocation methodology depends on the maturity of the organization.

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

Organizations in the energy sector may have formal or informal escalation processes. Sector organizations may be required by regulators to ensure such processes are established. NERC CIP-009-3 requires recovery plans for Bulk Electric System (BES) organizations. Similarly, the PMAs adhere to NIST requirements that include escalation processes for cybersecurity risks.

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

Standards should be formalized and best practices identified in close consultation with privacy professionals. The practices should not impose risks to privacy or civil liberties.

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

There are international implications of this Framework for the Energy Sector. The US grid interfaces with Canada and Mexico. Implications should be considered during development of the Framework but cannot be assessed until it is developed.

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

Risks should be managed in a transparent manner. Transparency coupled with privacy stewardship and governance can reduce risks to privacy and civil liberties. Organizations need to abide by international obligations, federal, state and local laws.

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

- Managing interdependencies, e.g., supply chain management
- Business impact analysis
- Employee education, training and awareness