Xcel Energy Response to NIST RFI

Current Risk Management Practices

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

Extensive and disparate compliance requirements, the resource demands and complexity of which may lead organizations to focus on compliance rather than on security. Any practice framework must be risk-based rather than one-size-fits-all, to allow the organization to apply resources to the areas or assets with the highest security risks and not require the same protections (and cost) to protect low-risk areas or assets.

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

Each governing sector seems to develop somewhat unique cyber security regulations and compliance requirements. We see this in the different regulatory bodies and regulations that we, as an electric and gas utility, need to comply with. The regulations focus on the same core set of security risks. The types of devices, information and levels of risk vary across industry sectors.

We have not experienced an empowered manager (or organization) effectively drive cross-sector responsibilities for core cybersecurity risks and controls.

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?

Xcel Energy supports the response submitted by the Edison Electric Institute (EEI) for questions 3-6 and 10 of this RFI.

Xcel Energy places a high priority on managing our cybersecurity risks. Our Board of Directors is provided regular updates on cybersecurity. The diligence to protect our customer and corporate information and critical infrastructure is carried from our Board, through our company executives to our employees. Our executives are engaged and actively working within industry and government to improve security and resiliency. Our CEO is a member of an industry subcommittee recommended by the National Infrastructure Advisory Council (NIAC) which advises the U.S. President through the Secretary of Homeland Security on the security of critical infrastructure sectors and their information systems.

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

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

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

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

Xcel Energy's cybersecurity risk management program is structured around the ISO 27000 series of standards for our framework and the NIST SP800 series of standards for our cyber 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?

As an investor-owned utility that provides electric generation, transmission and distribution as well as gas transmission and distribution, we are subject to cyber security requirements from multiple government agencies including:

Nuclear: NRC (Nuclear Regulatory Commission) NEI (Nuclear Energy Institute) 08-09

Electric: FERC/NERC CIP (Critical Infrastructure Protection), FERC emerging standards for hydroelectric generation

Gas: Department of Homeland Security (DHS) Chemical Facility Anti-Terrorism Standards (CFATS), DHS/Transportation Security Agency Gas Pipeline Security Requirements

Corporate: Sarbanes-Oxley, PCI-DSS (Payment Card Institute Date Security Standard), HHS/HIPAA (Health & Human Services Health Insurance Portability and Accountability Act), additional ad hoc security information requests from state public utilities commissions and attorneys general, state data privacy and data breach regulations.

Additionally, state public utilities commissions may provide oversight of our cyber security performance through state level proceedings.

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

Telecommunications are essential for our transmission and generation operations. These are regulated by NERC and NRC. Water is an essential component of some of our generating facilities and is regulated by DHS. Transportation (rail and gas pipeline) is critical for delivery of fossil fuels to many of our power plants and is regulated by TSA

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

We understand the importance of our cyber systems to our ability to provide reliable electric and gas service to our customers. Each of the state public utilities commissions in our service territories sets and monitors performance metrics. Additionally, we have a responsibility to our shareholders to deliver quality services and ensure a reasonable rate of return.

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?

We provide reports or reviews to multiple regulatory bodies. We are required to report on common compliance & risk management controls for each of the following regulatory bodies. The required documentation and focus for review/audit are different between agencies. Additionally, each regulator has their own process and document requirements for reviews, audits and reports, including suspected or confirmed incidents. Different processes, documentation, and reviews to comply with cybersecurity compliance requirements tailored for each agency is inefficient and redundant. Having a common or more complementary set of regulations and requirements, or at least a common format and frequency, would allow us to more efficiently manage and report on our compliance and risk management operations.

Another issue with the different agencies and reviews is that similar security requirements are interpreted differently between different compliance organizations.

Regulatory agencies we report to include:

NERC CIP: Annual self-certification, periodic confirmation of technical feasibility exceptions (TFEs), self-report and mitigation plans for violations (as needed). Since we are located in three different reliability organizational areas (MRO, SPP, WECC), we have separate reporting for each organization.

FERC Dams Sector requires reporting but only when they are in inspection mode.

DHS: CFATS does not have a reporting period but our company is subject to inspection at anytime. TSA for Gas Pipeline/SCADA cyber security reporting is on an annual basis.

NRC: Documentation to demonstrate compliance must be available upon NRC inspection. Updated cyber security plan is provided along with requests for amendment of license, construction permits, etc.

We may also respond to inquiries related to cyber security from state utilities commissions.

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

Xcel Energy is subject to mandatory CIP standards, under the umbrella of NERC, which is an international organization. NERC audits and requires self-certifications from each of the Xcel Energy operating companies.

The International Standards Organization (ISO) has a robust body of cybersecurity standards. ISO perform assessments as part of their certification process.

We believe mature cybersecurity frameworks and standards already exist through ISO and NIST standards. Instead of creating another set of standards, we recommend updates to existing standards to better align cybersecurity standards across both national and international standards.

Use of Frameworks, Standards, Guidelines, and Best Practices

1. What additional approaches already exist?

The NIST 800-series guidelines appear comprehensive, and seem to form the basis for the efforts of other federal agencies (including DHS and NIST's Smart Grid group). We endorse a single set of regulations/standards based on a body of controls and guidelines. Should there be legitimate industry sector-specific variations, they should be documented within those standards and/or as a supplement to them.

Another suggestion is to create a standardized controls-based framework that supports a well organized risk-based approach to information security and compliance. Leveraging an existing framework and organization like ISO 27001 and ISO 27002 would provide a logical consistent framework with existing best practices.

2. Which of these approaches apply across sectors?

All of the approaches noted above could apply across all sectors.

3. Which organizations use these approaches?

Xcel Energy uses this approach.

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

While we recommend selection of an existing (rather than creation of a new) framework, doing so may result in additional work for organizations that have modeled their cybersecurity programs on a different framework.

There are costs associated with any additional requirements, voluntary or mandatory, and entities in some sectors may have difficulty building a business justification for the added costs.

Leveraging existing ISO and NIST standards will minimize the changes required of organizations to follow the framework. The biggest changes will be the ongoing maturation of organizations to move to a risk based cybersecurity management program.

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

The use of risk-based criteria for determination of applicability of any new standards.

The industry is currently moving to a risk based approach to managing cyber security. Ensuring the cybersecurity framework is consistent with a controls based risk management approach could facilitate ease of implementation, measurement and benchmarking of effectiveness.

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

The approaches suggested would be consistent across sectors but allow for sector-specific controls around higher risk areas.

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

Due to the different levels of maturity across and within sectors, there likely will need to be sector-specific analysis of the current state of security controls and timeline for adherence to new standards. Each sector should identify specific control areas and relativity to sector assets but the overall framework should be consistent with the standard framework. We should avoid industry-specific variants of the entire framework, which adds complexity and hinders cross-sector collaboration.

8. What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?

Agencies and coordinating councils are essential bodies to assist their members in understanding the business need and cost drivers for the framework, as well as facilitating the risk assessment process to determine the applicability of the framework within the sector. The sector agencies can be consultative in applying the standard framework to a sector as well as promoting consistency in review/audits and measurements across sectors.

9. What other outreach efforts would be helpful?

We need alignment around a common cross sector cybersecurity framework and related standards.

Specific Industry Practices

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

Yes, both as required by existing regulations and as a matter of security best practices.

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

Elements of all of those practices are embedded in security standards and practices.

Elements of ISO 27000/27001/27002 are embedded in the security standards and practices – but are not followed closely.

ITIL (Information Technology Infrastructure Library) has been adopted for information systems management practices. IT audit uses COBIT (Control Objectives for Information and Related Technology) as a basis for their activities.

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

There is no silver bullet for security – in order to remain agile in the face of evolving threats, industry needs to have the flexibility to deploy a multi-faceted security program which includes not only the practices listed, but also robust personnel screening, training and awareness programs.

The process of managing a controls-based security program that prioritizes risks and integrates regular controls testing with continual improvements allows for the checks and balances necessary to ensure security risks are managed appropriately.

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

These are sound practices for all industries. Some elements may not be applicable for certain types of devices, due to the technical infeasibility of including them in their scope or the lack of applicability (for example, we have no privacy concerns with substation relays).

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

None alone is significantly challenging. However, any one-size-fits all set of regulations or practices is difficult to implement when there are variable levels of risks associated with types of devices and network zones, where the costs may exceed the benefits of risk mitigation. Therefore we advocate strongly that the framework include a risk-based approach to defining applicability.

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

Currently, standards and guidelines are used as the basis for controls that are applied within the business. Where regulations exist, they are applied according to the expectations of the regulator. Where regulations do not exist, they are applied according to baseline and risk-based security practice expectations.

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

Xcel Energy has played an active role in NERC standards development. The NERC program includes mechanisms for changing the standards as the environment and threats change. This is a key element to any standards program, especially one dealing with cybersecurity.

Creating standards is a very time-consuming, resource-intensive process. Xcel Energy encourages NIST to look at existing standards and frameworks (from sources including NIST and ISO) rather than try to re-invent something specifically for this exercise.

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

Yes. Xcel Energy has a critical incident response process that includes involvement of local, regional and federal entities. This process and detailed plans, are consistent with NERC standards.

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

Minimal risk as long as the privacy and security of personal information shared outside the company can be appropriately managed.

Xcel Energy takes seriously its duty to protect personal information collected from our customers, shareholders and employees. The company has internal policies and procedures that incorporate generally accepted privacy principles and applicable regulations. Additionally, we are active participants in state and federal level initiatives examining privacy issues, such as: (1) Minnesota Public Utilities Commission, In the Matter of a Commission Inquiry into Privacy Policies of Rate-Regulated Energy Utilities, Docket No. E,G-999/CI-12-1344; (2) NIST SGIP Privacy Subgroup (both 1.0 and the upcoming 2.0); and (3) Department of Energy's current effort to develop a Voluntary Code of Conduct for customer privacy.

Xcel Energy takes extensive proactive steps to secure information it has collected about its employees, shareholders and customers. Our comprehensive risk-based cybersecurity program protects the systems holding this information just as it protects our operational systems.

We believe it to be extremely unlikely that any technical information related to security incidents would also contain personal information pertaining to customers, employees and shareholders. However, as discussed in our response to Question #11 below, we support the development of appropriate security and privacy controls for the sharing of any personal information in the context of reporting a security incident.

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

Not applicable, Xcel Energy operates only in the United States of America.

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

As stated in response to question #9, we do not anticipate many instances where providing information related to a potential or actual cyber security threat will also require the utility to release an individual's personal information. However, in the event that such information is required, we believe that privacy and security controls for the data release must exist and that such controls would need to effectively limit access to such information and protect the individual's ongoing privacy. Such controls should be developed in advance, to ensure the timely and secure provision of such information when, if ever, it is necessary.

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

All owners and operators of critical infrastructure face risk from the supply chain. Purchasing hardware and software potentially introduce security risk into the organization. Creation of a voluntary vendor certification program may help drive innovation and better security in the components that are essential to delivery of critical infrastructure services.

Consistent with our industry response through EEI, other practices used by industry include:

- *Integration of physical security practices, enterprise IT, and energy control systems*
- *Robust personnel screening, training and awareness programs*
- *Threat intelligence and monitoring practices, including information sharing*
- *Configuration and vulnerability management practices*
- *Separation of control systems from Internet facing systems*
- *Removable media control and sanitization*

- *Change control processes to ensure changes to the IT infrastructure are performed in a controlled and coordinated manner and do not negatively impact cybersecurity*
- *Procurement protections to ensure products or services of prospective vendors are vetted prior to being approved for use*
- *Decommissioning practices such as wiping devices/media*
- *Forensics analysis*