414 Nicollet Mall

Minneapolis, MN 55401

1-800-895-4999

xcelenergy.com

COMMENTS OF XCEL ENERGY SERVICES INC. ON THE PRELIMINARY CYBERSECURITY FRAMEWORK

Docket No.: 130909789-3789-01

December 13, 2013

I. Introduction

Xcel Energy Services Inc. ("XES"), on behalf of the Xcel Energy Operating Companies (collectively "Xcel Energy"),[1] respectfully submits these comments in response to the Request for comments entitled *Request for Comments on the Preliminary Cybersecurity Framework* issued by the National Institute of Standards and Technology ("NIST") in Docket No. 130909789-3789-01 78 *Fed. Reg.* 64478 (October 29, 2013).

Xcel Energy is a vertically integrated utility that owns and operates transmission and generation assets in 10 states, including approximately 1,000 substations and over 80 owned generating plants, including nuclear, coal, natural gas, oil, hydro, biomass, wind, and solar facilities. In addition, a number of generating plants owned by third parties are interconnected to Xcel Energy's transmission system; and Xcel Energy interconnects

[1] The Xcel Energy Operating Companies are Northern States Power Company, a Minnesota corporation ("NSPM"); Northern States Power Company, a Wisconsin corporation ("NSPW") (and with NSPM jointly the "NSP Companies"); Public Service Company of Colorado ("PSCo"); and Southwestern Public Service Company ("SPS"). XES is the service company for Xcel Energy Inc. holding company system, and *inter alia*, represents the Xcel Energy Operating Companies in various federal regulatory proceedings.

with numerous entities that own and operate electric generation and transmission facilities.

Xcel Energy is in the business of delivering cost-effective and reliable electricity to its retail and wholesale customers. As such Xcel Energy is committed to ensuring the protection, resiliency, and reliability of the critical infrastructure that it owns and operates. Xcel Energy has invested—and continues to invest—millions of dollars in infrastructure protection, resiliency, and reliability improvements. These investments address not only enhancements required by the standards adopted by the North American Electric Reliability Corporation (NERC) but also enhancements that Xcel Energy has voluntarily implemented in furtherance of its own business objectives.

Xcel Energy also supports the goal of ensuring the protection, resiliency, and reliability of critical infrastructure assets owned and operated by others but relied upon by Xcel Energy. We appreciate the opportunity to participate in the process of building the Framework.

Xcel Energy assisted in the development of and supports the Energy Sector comments submitted by the Edison Electric Institute ("EEI") in this docket. These comments are intended to be complementary by providing greater detail to the broad themes in the Energy Sector filing.

II. Executive Summary

Below is a summary of Xcel Energy's comments and concerns with the Preliminary Cybersecurity Framework (the 'Framework'). We are also providing suggested edits to the Framework document using the separate Preliminary Cybersecurity Framework Comments Template (the 'Comments Template').

A. Focus the Framework on critical infrastructure

The scope of the Executive Order 13636, *Improving Critical Infrastructure Cybersecurity* ('EO') is critical infrastructure ('CI'), not all business processes and risks. This focus becomes lost when the Framework engages in a more general discussion of business risk management practices without subsequently leading organizations to define their role in management of risks to CI. As a result, the Framework must be modified to continuously reinforce, within the language of the Core, that the scope is limited to systems and assets essential to CI functions.

B. Focus the Core on security outcomes and risk-based use of the Framework

Organizations should be expected to apply concepts in the Framework based on the risk associated with individual systems and assets supporting CI. It is resource-prohibitive to manage and protect all of an organization's assets in an identical manner, and doing so will likely dilute the EO efforts to encourage improvements in critical infrastructure cybersecurity.

C. Connect the elements of the framework more clearly

1) Within the document, a general discussion of risk management is followed by discussion of Risk Tiers and Profiles, then introduction of the Core. It is not clear how an organization is expected to tie these elements together.
2) Appendix B, Methodology to Protect Privacy and Civil Liberties for a Cybersecurity Program, is not integrated within the Framework.

D. Align Framework implementation with existing programs

The Framework should recognize that some sectors have already invested significantly in the processes espoused in the Framework, and support implementation of the Framework in a manner that is consistent with established programs. Encouragement of coordination among Sector Specific Agencies (SSAs) in their implementation approaches will also benefit organizations with operations in multiple sectors by reducing complexity.

E. Focus the scope of the privacy and civil liberties content and integrate into the Framework

Privacy and civil liberties are important considerations for the Framework because failure to consider these issues could constitute a barrier to adoption. Core cybersecurity processes and controls, however, must be implemented in a manner consistent with the organization's relative privacy risks and existing protection programs. The privacy program principles outlined in Appendix B are overly broad, do not factor relative risk or existing privacy programs, and for these reasons are likely to extend beyond addressing the cybersecurity concerns that were called for by the EO.

III. Comments

A. Focus the Framework on protection of critical infrastructure

Throughout the Framework, organizations are asked to consider 'business purposes' and 'business objectives', which form an important foundation to a risk management program. The Framework needs to drive organizations to subsequently assess and act based on the specific risks related to systems and assets that support CI as defined in the EO[2]. A risk-based approach focused on the systems and assets essential to critical

[2] Critical infrastructure is defined as the "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." EO 13636 Sec. 2, Patriot Act of 2001.

infrastructure functions enables organizations to identify and prioritize the protection, detection, response, and recovery activities that will help improve critical infrastructure cybersecurity.

Not all systems and assets within each entity within the 16 critical infrastructure sectors are critical to the nation's economy, health, safety, and security and therefore not all systems and assets should be within the scope of the Framework.

Absent this clarification, organizations may interpret that all business systems and assets (not just those tied to CI) should follow the guidance within the Framework, at what is likely to be a substantial cost. An organization that does spread its limited resources over all its business assets may not adequately protect the subset that are essential to critical infrastructure functions.

NIST should edit the document, as suggested in the Comments Template, to stress its application to CI. That includes adding qualifiers such as 'critical infrastructure' to the Category and Subcategory descriptions throughout the Core.

B. Focus the Core on security outcomes and risk-based use of the Framework

Once an organization has identified those systems and assets that support CI functions, it should further assess the risk associated with individual systems and groups of assets. Some assets supporting CI are more heavily relied upon than others for the confidentiality, availability and integrity of the nation's critical functions. The impact of the loss of CI functions provided through certain assets varies widely within an organization, within a sector, and across sectors. Only through this further assessment of risk can an organization determine where its cybersecurity resources are best applied.

Similarly, the applicability of individual Core categories and subcategories will vary due to the nature of CI risks associated with the organization and with the types of systems or assets supporting CI functions.

Our edits in the Comments Template suggest several areas where the Framework Core should specify outcomes from the application of processes and controls *based on risk*. Absent these qualifiers, organizations may balk at the expectation that they expend scarce resources protecting all systems, assets and information equally, including protecting business systems that are neither tied to nor required for the operation of critical infrastructure.

C. Connect the elements of the framework more clearly

1. The document starts with a general discussion of risk management, which is followed by the introduction of Risk Tiers and Profiles, without clearly identifying at what level an organization is expected to assess their Tier or establish a Profile. For example, section 3.2 indicates that a Profile should be used to describe the state of 'specific cybersecurity activities'. Are Subcategories assumed to contain 'activities', so the Profile would belong at the Subcategory level? An example might help to clarify the application of these components of the Framework.
2. Appendix B, Methodology to Protect Privacy and Civil Liberties for a Cybersecurity Program, is not integrated within the Framework. Often,

organizations have separate IT security and privacy functions. Without more closely integrating the privacy elements with the Core, there is a risk that IT security professionals may not incorporate key privacy points buried in the Appendix.

D. Align Framework implementation with existing programs

The Framework should recognize and reflect that some sectors have already implemented risk and maturity models and voluntary cybersecurity standards. In Section 3.0, NIST should encourage the sectors to coordinate with their Sector-Specific Agencies, through their Sector Coordinating Councils to review the Framework and develop implementation guidance to integrate existing and future efforts "to address sector-specific risks and operating environments."[3] This will enable the Energy Sector to leverage and integrate cybersecurity improvements already underway into the Framework. Also, at the sector-level, cybersecurity risk management can be tailored to unique sector characteristics and leverage expertise from across the sector to increase efficiency and properly leverage asset owner and operator resources to use the Framework to reduce cyber risk to CI.

As an investor-owned utility that provides electric generation, transmission and distribution as well as natural 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

[3] Executive Order 13636, Improving Critical Infrastructure Cybersecurity Sec. 8(b).

- Electric: FERC/NERC CIP (Critical Infrastructure Protection), FERC Security Program for Hydropower Projects

- 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 Data 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.

The extent of current regulation adds complexity to our security program and our operational environment. Within the document, encouraging simplification and synchronization of sector implementation plans will help organizations to devote more focused resources to analyzing and addressing specific CI security risks.

E. Focus the scope of the privacy and civil liberties content

Rather than focus on opportunities to minimize the privacy risks of the cybersecurity processes within the actual Framework, the Appendix B instead outlines the elements of a full-scale organizational privacy program that appears to operate independent of the Framework. This raises a number of concerns.

First, the program outlined in Appendix B does not appear to address variables in: (1) the type of data collected and related privacy risks; or (2) unique aspects of the organization's operations that impact the use of data. These are necessary components of developing a comprehensive and effective approach to privacy risk and appropriate information management. For this reason, Appendix B does not provide the necessary flexibility to work within an organization's existing privacy program and may create inefficiencies that could pose a barrier to adoption of the Framework.

More troubling, the issues identified in Appendix B far exceeds the scope of the EO. Instead of focusing on where adoption of the Framework may intersect with an organization's existing privacy or information governance program, it assumes that a separate program is necessary. We believe that a more efficient and effective approach would be to identify points within the Framework where privacy may be impacted, and provide guidance on various ways to mitigate these issues. This would allow an organization to evaluate options based on the uniqueness of its own operations and its current privacy program before integrating these options directly into its implementation of the Framework.

We recommend revisions to Appendix B that reflect the principles in the alternative privacy methodology proposed by Harriet Pearson of Hogan Lovells, reflecting sentiment from a range of industries. The approach simplifies the content in Appendix B by focusing on privacy considerations directly resulting from the cybersecurity activities described in the Framework.

This alternative methodology also averts an otherwise expanded scope resulting from the proposed definition of 'Personally Identifiable Information' (Appendix E, Glossary). The Framework should defer to sectors and individual organizations to use definitions of protected information that are relevant for their environment and align with applicable legal and regulatory requirements. The data elements captured by entities varies between sectors (as does the relative sensitivity and risk of that data), so a onesize-fits-all definition of protected information or privacy requirements may prove burdensome without yielding incremental privacy/civil liberty protections.

CONCLUSION

The utility industry is unique in that it has been subject to NERC oversight and regulation with respect to Cybersecurity, and like Xcel Energy, many utilities are already subject to regulation from many different federal agencies (e.g. Nuclear Regulatory Commission, NERC). Acknowledging our dependencies on other CI sectors, we support efforts to drive improvements in cybersecurity in all sectors.

To encourage voluntary use of the Framework, NIST must make changes so that the document clearly communicates that:

- The scope of the framework is critical infrastructure
- The elements of the document (core, risk tiers, profiles and the appendices) clearly fit together so an organization understands how to apply the Framework
- Risk to CI functions drives the applicability of elements of the Core to different organizations, systems and assets
- Sector-specific agencies will play a significant role in implementation of the Framework, resulting in minimal disruption of existing risk management and regulatory constructs within and across sectors
- Cybersecurity activities will minimize impact to privacy and civil liberties.

Xcel Energy appreciates NIST's careful consideration of these comments, those within the Comments Template, and the Energy Sector comments submitted by EEI.

Date: December 13, 2013

Respectfully submitted,

[Elizabeth Mairs]