Duke Energy comments for Developing a Framework to Improve Critical Infrastructure Cybersecurity
Prepared by Ed Goff 4/5/2013 3:41 PM

The Edison Electric Institute (EEI), on behalf of its members, has submitted comments to NIST. Duke Energy generally supports the comments submitted by EEI. Duke Energy appreciates the opportunity to offer additional limited comments below with respect to the Cybersecurity Framework request for information (RFI) questions on which the National Institute of Standards and Technology (NIST) specifically requested 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?

    - Information sharing – getting timely, actionable intelligence.
    - Compliance culture versus security culture – existing mandatory compliance standards have resulted in greater emphasis proving adherence to standards versus improving security and managing risk.
    - Testing/validating security – there are improvement opportunities with supply chain vulnerabilities. Duke Energy (DE) is working to manage risk in the space with more application and component testing/penetration testing. It is not feasible for every entity to test everything and it is not prudent for every entity to test the same products.

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

    - Overlapping/redundant/conflicting standards or regulations will create negative unintended consequences.
    - Focusing on the fundamental controls important for the greatest return in security.
    - Some sectors already have mature regulatory compliance standards that may not be fully recognized by the new framework.

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?

    - DE is implementing the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2).
    - DE cybersecurity risk management is based on NIST 800-30.
    - DE utilized the Department of Homeland Security (DHS) Cyber Resilience Review
    - DE senior management sponsors and expects adherence with internal policies and standards. Policies and standards are published on an internal portal for broad awareness. Numerous methods of training and communications are utilized to

disseminate and promote awareness and education (e.g. computer based training, email, articles, management presentations, etc.).

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

    - The cybersecurity risk management function is aligned under the Chief Information Officer (CIO) under the Director of Information Technology (IT) Compliance & Process Oversight.

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

    - DE is implementing the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2).
    - Cybersecurity risk management is based on NIST 800-30.
    - NERC Critical Infrastructure Protection (CIP) assets follow risk management requirements from CIP 002-009.

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

    - The cybersecurity risk program is designed to work with and provide input to the overall enterprise risk management program.

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

    - NIST 800-30 Guide for Conducting Risk Assessments.
    - NIST 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.
    - NIST 800-53 Security and Privacy Controls for Federal Information Systems and Organizations.
    - Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2).
    - DHS Cyber Resilience Review.
    - 3rd Party Security Assessments and penetration testing.

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?

    - Electric Disturbance Events (OE-417)
    - NERC CIP 002-009
    - Electricity Sector Information Sharing and Analysis Center (ES-ISAC)
    - Payment Card Industry (PCI) Data Security Standard.
    - Chemical Facility Anti-Terrorism Standards (CFATS)
    - TSA Pipeline Security Guideline.
    - State Identity Theft Protection laws.
    - State Law enforcement and the Federal Bureau of Investigation

- Nuclear Energy Institute Cyber Security Plan

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

   - As part of DE Business Continuity program, interdependence analysis is performed on high risk systems and assets and plans are created to mitigate interdependencies.
   - An improvement opportunity is greater understanding and coordination with all interdependent critical infrastructures.

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

    - Numerous metrics are utilized to measure success in detecting and addressing cybersecurity risks (e.g. blocked malicious email, detection/blocking different types of network attacks, vulnerability management, access management, patch management, etc.)
    - Senior management and the board are regularly engaged and challenge teams and processes to demonstrate appropriate security posture is maintained including continuous improvement.
    - Annual updates to Business Continuity plans.
    - Periodic testing of Disaster Recovery and Incident Response plans and practices.

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?

    - DE is subject to certain regulatory reporting requirements of DOE and NERC.
    - The improvement opportunity is feedback in the form of timely, actionable intelligence. Recent improvements in the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) are welcome. Currently, there is more proactive and transparent 2-way sharing of indicators and proposed mitigation.

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

    - An improvement opportunity exists to leverage NIST to maintain a single cybersecurity standards family.
    - Numerous standards are utilized throughout the DE cybersecurity program.
    - Internal and external assessments are performed regularly to ensure adherence.

<u>Use of Frameworks, Standards, Guidelines, and Best Practices</u>

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?

    - NERC CIP 002-009.
    - NIST 800-30 Guide for Conducting Risk Assessments.
    - NIST 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.
    - NIST 800-53 Security and Privacy Controls for Federal Information Systems and Organizations (Final Public Draft).
    - NIST 800-82 Guide to Industrial Control System Security (ICS).
    - NISTIR 7628. Guidelines for. Smart Grid Cyber Security
    - Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2).

2. Which of these approaches apply across sectors?

    - NIST 800-30 Guide for Conducting Risk Assessments.
    - NIST 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.
    - NIST 800-53 Security and Privacy Controls for Federal Information Systems and Organizations.
    - NIST 800-82 Guide to Industrial Control System Security (ICS).

3. Which organizations use these approaches?

    - Many critical infrastructure sector entities utilize the NIST 800 series guidelines.

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

    - Guidelines and best practices are not written to be mandatory enforceable compliance standards. It is problematic when guidelines and best practices are used improperly by external reviewers as requirements.
    - Even though many existing standards, guidelines, and best practices have good content, implementation guidance could be clearer.

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

    - Add implementation guidance including multiple use-cases for different entity size and business type. Guidance should be flexible, risk-centric, goals-based and process-oriented. Guidance should avoid being overly prescriptive.

- Include appendix in all standards and guidelines that map to other foundational standards, guidelines, and best practices.

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

    - These approaches do not account for sector-specific needs. DE's implementation of these standards includes adapting them for our use.

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

    - We expect the new framework to utilize existing standards to the extent possible.

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

    - Implementation guidance.
    - Education and training.
    - Ensuring there is no overlap, redundant, and/or conflicting requirements.
    - Ensuring there are no double jeopardy situations.

9. What other outreach efforts would be helpful?

    - Supplier education and awareness to ensure alignment with supplier's offerings and the needs of critical infrastructure entities.
    - Collaborate with other critical sectors in the creation of the new Framework (e.g. framework workshops, cross sector analysis)
    - Reach out to NERC, TSA, DHS and Nuclear Energy Institute (NEI) to ensure existing standards are utilized to the extent possible in the new Framework.

<u>Specific Industry Practices</u>

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?

    - Training and awareness.
    - Foundational controls from NIST 800-53, 800-82, 800-30, NISTIR 7628, NEI and NERC CIP.
    - Risk Management.
    - People, process and technology mix of controls/process to meet business needs and manage risk.
    - Security Principles: Defense-in-depth, Separation of duties and Least Privilege
    - Supply chain – improvement opportunities include more thorough testing and validation, vendor monitoring and updated cybersecurity procurement language.
    - Access Management.

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

    - These are addressed in standards already.

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

    - Training – cybersecurity focused and cross training between Operational Technology and Information Technology.
    - Threat management – timely, actionable intelligence.
    - Exercises – significant cyber events that impact substantial generation or involve bulk customer information breach are critical to test plans and capabilities. The training value of this is strong and hard to measure.
    - Supply Chain – updated procurement language, supplier monitoring practices, more and improved hardware and software testing (including binary code analysis).

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

    - These are applicable to the electric sector.

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

    - Day-to-day Threat Management including Advanced Persistent Threat mitigation.
    - Risk mitigation of Operational Technology (OT) and Information Technology connectivity and increased us of commercial-off-the-shelf (COTS) hardware and software in OT solutions.
    - Access Management and network security due to increased hosted solutions and 3rd party support/maintenance models.
    - Vulnerability management, asset management, change control, and configuration management of control systems components.

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

    - All internal policies, standards, procedures and practices leverage appropriate standards and guidelines from NIST, NERC, and NEI.

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

    - Policies and standard have assigned owners and stakeholders responsible for maintaining assigned documents.
    - Formal Enterprise Technology Plan processes and architecture support the formal Investment Governance program that prioritizes and funds the Cybersecurity Program.

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

    - Yes. This is part of the DE Crisis Management and Computer Incident Response Team programs.

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

    - DE has an internal team responsible for privacy. Privacy is assessed regularly in the company and within projects that utilize sensitive privacy information where appropriate controls are implemented.
    - Systems containing this information are maintained to high cybersecurity standards and are routinely assessed as part of our routine vulnerability management program.

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

    - This will need to be assessed as the framework is completed. There will be differences in what can be implemented in our international entities.

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

    - Similar to other sensitive information currently used. The risk will be assessed and appropriate controls will be implemented and monitored for compliance.

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

    - No