

Illinois Commerce Commission Cybersecurity Policy Session

July 21, 2016



The NIST Framework -- Intent

- Framework for Improving Critical Infrastructure Cybersecurity
 - Despite the name, applicable to any organization or business
- A voluntary, risk-based approach to manage cybersecurity risk, in a cost-effective way, based on business needs
- The framework is not regulation
 - There is no compliance requirement



It's about **MANAGING RISKS** and making **SOUND INVESTMENTS** in cybersecurity efforts

The NIST Framework -- In Practice

Determine or confirm your **BUSINESS CONTEXT**

What constitutes your threat?
Environment, legal and regulatory requirements; business objectives and constraints; and key services, service delivery and security goals

Develop, adopt, or confirm your **TARGET PROFILE**

- Two key steps:
1. Determine WHICH subcategories are most important to you within your business context
 2. Determine a desired Tier level for each of the important subcategories



Determine **INVESTMENTS** and an **ACTION PLAN**

Select controls or practices for further investment, prioritize them, and develop a plan to implement

Perform a **GAP ANALYSIS**

... between your Current and Target Profiles

Assess your **CURRENT PROFILE**

Assess what Tier describes your practices in each of the key subcategories

NERC CIP – History

- NERC CIP standards address the security of cyber assets critical to the operation of the grid.
- The first version of NERC CIP adopted in 2008.
- The standards have been repeatedly revised since their creation.
- NERC CIP Version 6 became effective on April 1, 2016.

NERC CIP – Standards

- Cyber System Categorization
- Security Management Controls
- Personnel & Training
- Electronic Security Perimeters
- Physical Security of Cyber Systems
- System Security Management
- Incident Reporting & Response Planning
- Recovery Plans for Cyber Systems
- Configuration Change Management & Vulnerability Assessments
- Information Protection
- Physical Security of Transmission Stations

NERC CIP Version 6 – Key Changes

- Requires covered entities to develop plans and implement cybersecurity controls to protect transient devices and removable media (e.g., thumb drives) and train personnel on the risks associated with them.
- FERC’s Order approving NERC CIP Version 6 directs NERC to develop a Supply Chain Management standard.
 - FERC stated, “The supply chain enables opportunities for adversaries to directly or indirectly affect the management or operations of companies that may results in risks to the end user. Supply chain risks may include the insertion of counterfeits, unauthorized production, tampering, theft, or insertion of malicious software, as well as poor manufacturing and development processes.”

NERC CIP Enforcement

- FERC has delegated to NERC authority to monitor and enforce compliance.
- NERC conducts audits to assess NERC CIP compliance. Violations can be self-reported.
- NERC's May 2013 Reliability Coordinator Compliance Analysis Report showed 140 NERC CIP violations since 2008.
- NERC can issue severe penalties -- as high as \$1 million per incident.
- According to an October 2014 report, NERC had issued \$160 million in fines for NERC CIP violations between October 2009 and October 2014.

Supply Chain Guidance

- DOE's Cybersecurity Procurement Language for Energy Delivery Systems
- Topics include:
 - Logging and Auditing
 - Reliability and Adherence to Standards
 - Communication Restrictions*
 - Supplier Personnel Management
 - Malware Detection and Protection
 - Problem Reporting
 - Documentation and Tracking of Vulnerabilities*

Supply Chain Guidance

- Specific Examples of Recommended Language
 - Communication Restrictions
 - The Supplier shall provide a means to document that network traffic is monitored, filtered, and alarmed, and provide filtering and monitoring rules.
 - The Supplier shall document all remote access entry pathways and ensure they can be enabled or disabled.
 - Documentation and Tracking of Vulnerabilities
 - The Supplier shall provide, within 30 days after product delivery, summary documentation of uncorrected security vulnerabilities in the procured product.
 - This includes documentation of vulnerabilities that have not been publicly disclosed or that have been identified after product delivery.

Information Sharing

- The Electricity Sector Information Sharing and Analysis Center or “ES-ISAC” provides a forum for energy companies to collect and share with one another critical cyber threat information, including vulnerabilities, analyses, warnings, and protective strategies.
- NERC has clarified that ES-ISAC has no responsibility for NERC CIP compliance, and has prohibited ES-ISAC personnel from conveying to compliance personnel information regarding potential NERC CIP violations.
- Further, the recently enacted Cybersecurity Information Sharing Act of 2015 or “CISA” provides protections from civil liability, regulatory enforcement, and public disclosure rules to entities that share cyber threat indicators.

Illinois Commerce Commission Cybersecurity Policy Session

**THANK YOU!
QUESTIONS?**

Jennifer Rathburn

jennifer.rathburn@quarles.com

(414) 277-5256