

Opening Remarks, FERC Technical Conference
Brent Castagnetto, Manager Cyber Security Audits & Investigations
Washington DC, April 29 2014

Introduction:

Good afternoon, my name is Brent Castagnetto, I am the Manager of Cyber Security Audits & Investigations at the Western Electricity Coordinating Council. I appreciate the opportunity to discuss the NIST Security Risk Management Framework (RMF), NIST Cyber Security Framework (CSF), and the Critical Infrastructure Protection Reliability Standards (CIP v5). The goal of my remarks is to highlight each and identify additional control objectives that should be considered in future revisions of the CIP Standards.

Overview:

Reliance on technology, communication, and interconnectivity of Information Technology and Industrial Control Systems has changed and expanded potential vulnerabilities and increased risk to the reliable operation of the Bulk Power System.

Remarks:

CIP version 5, NIST Risk Management Framework, and NIST Cyber Security Framework require identification, categorization, and protection of information systems and industrial control systems.

The NIST Risk Management Framework leverages a significant number of Federal Information Security Management Act (FISMA) publications in the form of standards and guidelines that dictate its overarching framework to ensure information systems meet the minimum cyber security control objectives identified in NIST SP 800-53. The objective of the Risk Management Framework is to provide an effective structure for selecting and applying the appropriate security controls for Federal information systems.

The NIST Cyber Security Framework builds on the concepts specified in the NIST SP 800-53 and uses components from:

- Control Objectives for Information and Related Technology (COBIT 5)
- International Society of Automation (ISA-62443)
- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC 27001:2013)

The Framework Core consists of five concurrent and continuous functions:

Identify, Protect, Detect, Respond, and Recover. When considered together, these functions provide a high-level, strategic view of the lifecycle of an organization's management of cyber security risk.

As directed by the Commission, the CIP version 5 Standards Drafting Team worked to ensure version 5 of the CIP Standards leveraged the NIST Risk Management Framework.

This is apparent from the CIP-002-5 identification and classification of BES Cyber Systems, and through controls specified in CIP-005-5, CIP-007-5 and CIP-010-1.

The CIP Standards can be further strengthened through application of additional control objectives listed in the NIST frameworks, for example:

- NIST SP 800-53 Contingency Planning (CP-8) requires an organization to develop primary and alternate telecommunications service agreements that contain priority of-service provisions. This level of planning is not currently required in CIP-009-5 and would strengthen registered entity's ability to remain connected or reconnect its critical systems more rapidly when recovering from an incident or disaster.
- NIST SP 800-53 Physical and Environmental Protection (PE- 9 – PE-15) requires an organization to ensure protection of power equipment and power cabling, processes to ensure an orderly shutdown of information systems in the event of a primary power loss. Additional control objectives not currently found in CIP v5 or the proposed physical security protection Standard (CIP-014-1) include: fire protection, temperature and humidity controls, and water damage protection. Taking an all hazards approach, these controls would strengthen a registered entity's ability to protect against and mitigate physical and environmental related vulnerabilities.
- NIST SP 800-53 System and Communications Protection (SC-8 - SC-13) and NIST Cyber Security Framework Protection, Data Security (PR.DS-6) both require an organization to ensure data transmission integrity and confidentiality, through the use of trusted communication paths, server certificates, and cryptography. Today's threats and vulnerabilities are more sophisticated and complex than ever before, and the use of malware targeting data exfiltration is growing at an exponential rate, which is one of the greatest threats facing our industry. Leveraging these control objectives will help ensure both data at rest and in transit are managed in a secure manner.
- NIST Cyber Security Framework Protection, Protective Technology (PR.PT-4) requires an organization to ensure protections are applied to communications and control networks. This should be considered by the standards drafting team in its efforts to address the commission's remaining concerns with Order 791.

The aforementioned control objectives and protections are only sample areas that may be leveraged to augment the CIP version 5 Standards. Cyber security controls should be based on risk and must be considered with the security triad taken into context and priority for our industry: Availability, Integrity and Confidentiality.

Close:

There is no silver bullet for security of the Bulk Power System. Achieving long-term security and reliability will require more than mandatory enforceable standards or voluntary frameworks. The security of the Bulk Power System will require a more robust risk-based approach. We must approach security controls and frameworks as pieces of a holistic solution, applied in a manner commensurate to the risk profile of that which we are working to protect.

I'd like to thank the Commission and Commission Staff for providing me the opportunity to share my perspective, and look forward to a meaningful dialogue and discussion as part of this panel.

Brent Castagnetto
Manager, Cyber Security Audits and Investigations
WECC