

FERC NOPR on NERC CIP Standards

An Acronymious Discussion

Presented by Dave Anderson to the RSSC, September 19, 2007



- History
- NOPR Overview
- Proposed Changes (Themes)
- Other points of note
- Implications
- Questions/Discussion

- Officially published August 6, 2007
- 193 pages
- Focuses entirely on CIP-002 through CIP-009
- Contains much discussion and many proposals :
 - FERC will approve all 8 Cyber Security Standards
 - Implementation Timetable will be approved
 - FERC will direct NERC to modify each Standard to address perceived deficiencies – *The bar is being raised.*
 - Some changes to be made *before* the first compliance date (possibly inconsistent with the Reliability Standards development process)

- Defence in Depth – 2 or more layers (physical and logical)
- Small entities could be used as a vector of attack
- Doctrine of Mutual Distrust
- Inappropriate emphasis on the existence of documentation rather than identifying a requirement that addresses the underlying (real) goal.
 - “substantive” compliance is required
 - For instance, it is not enough to draft a plan. It must be implemented
- Some increased emphasis on the “how” rather than just on the “what”

- Too much opportunity to “escape”
 - Removal of the “Reasonable Business Judgment” escape clause
No more exceptions based on an entity’s “acceptance of risk”
 - Exceptions based on “technical feasibility” only
 - Must develop and implement interim steps to address resulting vulnerability
 - Must develop and implement a remediation plan
 - Must be formally accepted by senior management
 - Exceptions to be approved by third party (Regional Entity?, NERC?)
 - *These changes wanted prior to compliance audits in 2009*

- There needs to be external oversight that provides a “wide area” view:
 - Compliance with Standards
 - Consistency, effect, and acceptability of exceptions
 - Information collection, analysis, and reporting
 - process to review and *approve* critical asset lists
 - Data is a critical cyber asset
 - Market data is needed for the *proper* operation of critical cyber assets
- } Ergo, market systems are Critical Cyber Assets
- Consider improper use of assets, not just potential loss

- Security policies should cover more ground than the requirements of the CIP Standards
 - These extended policies may be subject to compliance monitoring
- Change control & configuration management
 - Verify all changes
 - Changes documented within 30 days
 - Detect unapproved changes
- Training & Personnel Risk Assessments
 - Before access to Critical Cyber Assets is allowed
 - More detailed training(!)
- More frequent review of security logs
 - Manual
 - Weekly

- More thorough vulnerability testing
 - “Live” testing on production systems
 - Differences between test environments and production environment to be documented
- Improved incident response and recovery
 - System backups to be verified operational before storage
 - More rapid reporting of incidents (1 hour)
 - “Full operational exercises” to test incident response procedures
 - “Full operational exercises” of system recovery (disaster recovery)
 - “Forensic” data collection following cyber incidents
 - More rapid transfer of “lessons learned”
- Violation Risk Factors to be increased

- FERC expects NERC to continue to improve the Standards to better protect the Bulk Power System
 - Address this in ERO's Reliability Standards Development Process
 - Possible push towards NIST standards
 - FERC may revisit as part of assessing NERC's performance
- FERC will look into interdependency with other sectors (eg. Telecom) in other proceedings and with other agencies

- The bar is definitely being raised
- An increased focus on the *how* rather than just the *what*
- Significantly larger role for Regional Entities
 - Growth of bureaucracy
 - Competition for resources
 - Concentration of information
 - Critical path for approvals
 - Dilution of responsibility and conflict of interest (approvals, provision of assistance)
 - Liability issues
 - Adversarial climate

- FERC's wording suggests an intent to extend the reach of the Standards:
 - More entities
 - Data, not just systems
 - Improper use, not just unavailability
 - “Proper” operation rather than “reliable” operation (precursor to extension to Market Systems?)
 - Compliance with Corporate policies, not just requirements in the standards

Questions and Discussion