

Morgan Lewis

EEI Fall 2008 Legal Conference
Boston, Massachusetts
Stephen M. Spina
November 1, 2008



www.morganlewis.com



Overview

- Reliability Standards Enforcement Framework
- Critical Infrastructure Protection (CIP) Standards
- NERC Response to FERC Directives
- Current Trends in CIP Violations
- Emerging Issues
- Federal Legislation



Reliability Enforcement Framework

- Section 215 of the Federal Power Act requires NERC to develop mandatory and enforceable Reliability Standards, subject to FERC review and approval.
- Once approved, the Reliability Standards may be enforced by NERC, subject to FERC oversight.
- FERC may independently enforce Reliability Standards.



Reliability Enforcement Framework

- NERC delegates compliance and enforcement of Reliability Standards to Regional Entities.
- Reliability Standards became mandatory and enforceable in June, 2007.
- The original Reliability Standards submitted to FERC did not include CIP Reliability Standards (except for CIP-001 – Sabotage Reporting).
- CIP-002 through CIP-009 approved by FERC in Order No. 706 (effective April 7, 2008).



CIP Reliability Standards

- CIP Reliability Standards require users, owners and operators of the Bulk Power System to safeguard “critical cyber assets.”
- Process:
 - Develop methodology to identify “critical assets” (e.g. generators, substations, and control centers).
 - Apply the methodology to create list of critical assets.
 - Use the list of critical assets to determine associated “critical cyber assets.”



CIP Reliability Standards

- CIP Reliability Standards:
 - CIP-001 – Sabotage Reporting
 - CIP-002 – Critical Cyber Asset Identification
 - CIP-003 – Security Management Controls
 - CIP-004 – Personnel & Training (Background Checks)
 - CIP-005 – Electronic Security Perimeters
 - CIP-006 – Physical Security of Critical Cyber Assets
 - CIP-007 – Systems Security Management
 - CIP-008 – Incident Reporting and Response Planning
 - CIP-009 – Recovery Plans for Critical Cyber Assets



CIP Reliability Standards

- Order No. 706 approved the CIP Reliability Standards but required modifications.
- FERC directed NERC to remove references to “reasonable business judgment” and “acceptable risk” from the standards.
- NERC also directed to develop specific conditions necessary to invoke “technical feasibility” exception.



CIP Reliability Standards

- Technical Feasibility Exception:
 - Recognizes the difficulty with replacement of legacy equipment before the end of its useful life.
 - FERC states, however, that replacement equipment should meet the CIP Reliability Standard requirements.
 - The technical feasibility exception may include “technically safe” and “operationally reasonable.”
 - The exception does not release entity from requirements but rather requires alternative obligation.



CIP Reliability Standards

- Technical Feasibility Exception Framework:
 - Develop, document and implement a mitigation plan that achieves comparable level of security.
 - Include a remediation plan and timeline for eliminating the use of the exception.
 - Exception requires the approval of a “senior manager.”
 - Provide notice to Regional Entity of any technical feasibility exception as part of self-certification with review by Regional Entity during audit process.



NERC Response

- FERC, among other things, required NERC to:
 - Submit a work plan for modifications required by FERC and prepare modifications to CIP Reliability Standards.
 - Prepare a technical feasibility exceptions report.
 - Prepare a critical asset methodology guidance document.



NERC Response

- NERC's efforts on this are on-going.
 - NERC appointed Mike Assante as Chief Security Officer.
 - NERC held a Cyber Security Summit in September.
 - NERC guidance document on critical asset identification methodology due in December.
 - NERC team formed to revise standards; scheduled to submit revised standards to FERC by the end of March, 2009.



CIP Standards – Violations

- CIP-001 was mandatory and enforceable in June 2007.
- Only CIP-001 was enforceable at the time the original Notices of Penalty were filed with the Commission.
- Of the 37 Notices of Penalty filed to date, 17 (46%) contained violations of CIP-001 (Sabotage Reporting).



CIP Standards – Violations

- Of the 17 violations of CIP-001:
 - 11 were for violations of all 4 Requirements in CIP-001.
 - 1 was for a violation of Requirement R1 (recognition and awareness procedures).
 - 2 were for violations of Requirement R2 (interconnection communication procedures).
 - 3 were for violations of Requirement R4 (FBI communication contacts and procedures).



CIP Standards – Violations

- Self-Certifications regarding CIP compliance were submitted in July. Entities must continue to self-certify every six months.
- Regions have begun to identify possible violations in the self-certifications:
 - CIP-004 R2 – Training
 - CIP-004 R3 – Background Checks
 - CIP-004 R4 – Access
 - CIP-008 R1 – Cyber Security Incident Response Plan
 - CIP-009 R2 – Recovery Plans



Emerging Issues

- Development of Critical Asset Identification Methodology – no clear guidance at this point.
- Sabotage Reporting – several reported violations of CIP-001 in the initial notice of penalties filed with FERC by NERC. Why?
- Vendor Issues:
 - Background checks
 - Requirement to maintain lists of those with access to critical cyber assets
- Document retention issues.
- Replacement of legacy equipment.



Legislation

- Chairman Kelliher:
 - FERC authority over cybersecurity is insufficient to deal with emerging threats.
 - The timeline for developing Reliability Standards through the NERC process takes too long.
- House held hearings, but legislation did not emerge.
- Congress may address issue early in 111th Congress.