

Summary of the FERC notice of proposed ruling on Cyber Security Standards



On July 19, FERC released the notice of proposed ruling (NOPR) on Cyber Security Standards (CIP) CIP-002-1 through CIP-002-9. FERC accepted all the 8 Cyber Security Standards as being mandatory and enforceable.

Highlights of the FERC NOPR include:

- Annual certification during the CIP implementation plan is not enough – more frequent certifications during various stages of the implementation are required. These certifications would not be indicative of compliance / non-compliance but more of a formal guidance program.
- Henceforth, NERC’s Readiness Audits will have a Cyber security assessment section.
- FERC has directed NERC to remove the phrase “reasonable business judgment ” language in the CIP standards before compliance starts in 2009. The reasoning being that business convenience cannot excuse compliance with mandatory reliability standards.
- The meaning of the phrase “where technically feasible” would also be narrowed down to existing facilities/assets only. FERC also wants NERC to quantify instances when entities invoke “technical feasibility” issues.
- FERC requires NERC to eliminate the “acceptance of risk” option for the CIP standards. FERC believes that this could provide flexibility to entities in deciding their risk management policies.
- FERC wants NERC to monitor National Institute of Standards and Technology (NIST) criteria which are more stringent than the CIP standards – FERC could decide later on to enforce the more stringent NIST standards.
- NERC and Regional Entities will provide reasonable technical support to entities in order to help them determine whether their assets are critical to the bulk power system.
- 43 of the 162 Violation Risk Factors (VRFs) need to be revised. FERC has indicated that these requirements should be given a higher priority than the current priorities listed for these

requirements. For example, FERC has indicated that a requirement relating to identification of cyber assets (CIP-002-1, R3) must be a “HIGH” priority and not a “MEDIUM” which it currently is.

FERC has also recommended that NERC revise the certain requirements or add new requirements to strengthen these standards. FERC’s directives on individual standards include:

- On CIP-002-1 (Critical Cyber Asset Identification),
 - o Regional Entities must provide guidance for risk-based assessment guidelines.
 - o The standard must include requirement for external review and approval of critical assets from entities who have a regional perspective or a broad system view.

- On CIP-003-1 (Security Management Controls),
 - o Entities must submit exception reports to the responsible Regional Entities.
 - o Entities must have strong change management policies in place.
 - o NERC must provide directions on how entities must adopt a “mutual distrust” posture in order to control access to its systems from the outside world.

- On CIP-004-1 (Personnel and Training),
 - o Personnel must be trained before access to critical cyber assets.
 - o Personnel risk assessment must be completed especially for newly-hired employees and contractors before providing access to critical cyber assets.
 - o NERC must address “joint-use” concerns – concerns on entities sharing the same set of resources.

- On CIP-005-1 (Electronic Security Perimeter (s)),
 - o Adoption of security measures for protecting the area and systems outside the Electronic Security Perimeter (ESP).
 - o Access logs must be reviewed more frequently than the present every 90 days cycle.
 - o The phrase “Strong Controls” must specify use of digital certificates, two-factor authentication etc.

- On CIP-006-1 (Physical Security of Critical Cyber Assets),
 - o NERC must specify that there should be at least two different security procedures while establishing a Physical Security Perimeter around critical cyber assets.
 - o A readily accessible critical cyber asset must be tested every year with a one-year record requirement for retention of testing, maintenance, and outage records.
 - o A non-readily accessible critical cyber asset must be tested every three years with a three-year record requirement for retention of testing, maintenance, and outage records.

- On CIP-007-1 (Systems Security Management),
 - o Removal of “Acceptance of Risk” language.
 - o “Technical Feasibility” exceptions must be reported to the appropriate regional entities.
 - o Requirements must be firm such that there is no opportunity for unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it.
 - o Changes resulting from modifications to systems or controls shall be documented within a 30-day time period.
 - o Incident response logs to be retained for 3 years.

- On CIP-008-1 (Incident Reporting and Response Planning),
 - o One hour cyber security incident reporting to ES ISAC (Electricity Sector Information Sharing and Analysis Center) mandated.
 - o A “full operational exercise” must be carried out every 3 years.

- On CIP-009-1 (Recovery Plans for Critical Cyber Assets),
 - o NERC must modify this in order to incorporate use of good forensic data collection practices.
 - o Recovery plans to be updated within 30 days on indication of a weakness or problem with the cyber security incident recovery plan.

The complete notice of proposed ruling is located at:

<http://www.ferc.gov/whats-new/comm-meet/2007/071907/E-4.pdf>.