

RSSC Members,

As you may be aware, FERC, on July 19th, has proposed the adoption of new reliability standards for cyber security in the bulk power system.

NERC developed the proposed reliability standards (CIP-002-1 through CIP-009-1) and submitted them to the Commission for approval on August 28, 2006. In December 2006, Commission staff issued a preliminary analysis of the cyber security reliability standards, and allowed for public comment. In the NOPR, the Commission proposes to approve the eight cyber security reliability standards. The NOPR also calls for NERC to develop modifications to address specific concerns identified by the Commission. The complete document is located at: <http://www.ferc.gov/whats-new/comm-meet/2007/071907/E-4.pdf>

The proposed standards require certain users, owners and operators of the grid to establish plans, protocols and controls to safeguard physical and electronic access to systems, to train personnel on security matters, to report security incidents, and to be prepared to recover information.

A brief summary of the NOPR is attached alongside for your information. Please note that the IESO will be working closely with all the affected market participants regarding the actual interpretation and application of this NOPR.

Brief Summary of the FERC NOPR on Cyber Security Standards (CIP)

On July 19, FERC released the 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 judgement” 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 wants 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),
 - Regional Entities must provide guidance for risk-based assessment guidelines.
 - 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),
 - Entities must submit exception reports to the responsible Regional Entities.
 - Entities must have strong change management policies in place.
 - 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),
 - Personnel must be trained before access to critical cyber assets.
 - Personnel risk assessment must be completed especially for newly-hired employees and contractors before providing access to critical cyber assets.
 - NERC must address “joint-use” concerns – concerns on entities sharing the same set of resources.
- On CIP-005-1 (Electronic Security Perimeter (s)),
 - Adoption of security measures for protecting the area and systems outside the Electronic Security Perimeter (ESP).
 - Access logs must be reviewed more frequently than the present every 90 days cycle.

- The phrase “Strong Controls” must specify use of digital certificates, two-factor authentication etc.
- On CIP-006-1 (Physical Security of Critical Cyber Assets),
 - NERC must specify that there should be at least two different security procedures while establishing a Physical Security Perimeter around critical cyber assets.
 - 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.
 - 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),
 - Removal of “Acceptance of Risk” language.
 - “Technical Feasibility” exceptions must be reported to the appropriate regional entities.
 - 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.
 - Changes resulting from modifications to systems or controls shall be documented within a 30-day time period.
 - Incident response logs to be retained for 3 years.
- On CIP-008-1 (Incident Reporting and Response Planning),
 - One hour cyber security incident reporting to ES ISAC (Electricity Sector Information Sharing and Analysis Center) mandated.
 - A “full operational exercise” must be carried out every 3 years.
- On CIP-009-1 (Recovery Plans for Critical Cyber Assets),
 - NERC must modify this in order to incorporate use of good forensic data collection practices.
 - Recovery plans to be updated within 30 days on indication of a weakness or problem with the cyber security incident recovery plan.