FEDERAL ENERGY REGULATORY COMMISSION
NEWS

July 19, 2007
Docket Nos. RM06-22-000, RM06-16-003,
RM06-16-001

NEWS MEDIA CONTACT
Celeste Miller - 202.502.8680

Commission Proposes Adoption of New Reliability Standards For Cyber Security in the Bulk Power System

The Federal Energy Regulatory Commission today proposed to approve a set of reliability standards to help safeguard the nation's bulk electric power supply system against potential disruptions from cyber attacks.

The North American Electric Reliability Corporation (NERC) developed the proposed reliability standards 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 today's Notice of Proposed Rulemaking (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 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.

"Reliability of the bulk power system requires our attention to security issues as well as ensuring that the system serves consumers during peak-demand times," FERC Chairman Joseph T. Kelliher said. "These proposed standards are intended to provide the adequate safeguards and training to help us do that."

The NOPR seeks industry comment on the following eight Critical Infrastructure Protection (CIP) standards:

- Critical Cyber Asset Identification: Requires the identification of an entity's critical assets and critical cyber assets using a risk-based assessment methodology.
- Security Management Controls: Requires an entity to develop and implement security management controls to protect critical cyber assets.
- Personnel and Training: Requires personnel with access to critical cyber assets go through identity verification, criminal background checks and employee training.
- Electronic Security Perimeters: Requires the identification and protection of an electronic security perimeter and access points. The security perimeter is to encompass the critical cyber assets.
- Physical Security of Critical Cyber Assets: Requires the creation and maintenance of a physical security plan that ensures all cyber assets within an electronic security perimeter are kept in an identified physical security perimeter.

- Systems Security Management: Requires an entity to define methods, processes, and procedures for securing the systems identified as critical cyber assets, as well as the non-critical cyber assets within the perimeter.

- Incident Reporting and Response Planning: Requires the identification, classification and reporting of cyber security incidents related to critical cyber assets.

- Recovery Plans for Critical Cyber Assets: Requires the establishment of recovery plans for critical cyber assets using established business continuity and disaster recovery techniques and practices.

Comments on the NOPR are due 60 days after publication in the *Federal Register*.

In a related order, the Commission denied rehearing of its Final Rule on Mandatory Reliability Standards for the Bulk-Power System, issued April 16. The order clarifies that the Commission has not definitively defined the extent of the facilities covered by the statutory term Bulk-Power System. The Commission intends to address concerns regarding the scope of the term "Bulk-Power System" in future proceedings.

Finally, the Commission also approved NERC's proposal to create a new category of Joint Registration Organizations that will accept compliance responsibility on behalf of their members. These organizations may include joint action agencies, generation and transmission cooperatives or similar organizations, and may accept full compliance responsibility or divide compliance responsibility with its members, so long as there are no gaps or undue overlaps in coverage.

(30)

R-07-43