



FEDERAL ENERGY REGULATORY COMMISSION

NEWS

January 17, 2008

Docket No. RM06-22-000

NEWS MEDIA CONTACT

Celeste Miller- 202.502.8680

FERC Approves New Reliability Standards for Cyber Security

The Federal Energy Regulatory Commission (FERC) today approved eight new mandatory critical infrastructure protection (CIP) reliability standards to protect the nation's bulk power system against potential disruptions from cyber security breaches.

These reliability standards were developed by the North American Electric Reliability Corporation (NERC), which FERC has designated as the electric reliability organization (ERO).

"Today we achieve a milestone by adopting the first mandatory and enforceable reliability standards that address cyber security concerns on the bulk power system in the United States," FERC Chairman Joseph T. Kelliher said. "The electric industry now can move on to the implementation of the standards in conjunction with improvement of these standards in order to increase the security and reliability of the bulk power system."

Additional actions in today's final rule direct the ERO to develop modifications to these reliability standards, via its reliability standards development process, and then submit them to FERC for approval. The modifications directed for development concern various oversight and technical issues pertaining to cyber protections. These include removal of language that allowed variable implementation of standards based on "reasonable business judgment" and a new framework of accountability surrounding exceptions based on technical feasibility.

The final rule also directs NERC to monitor the development and implementation of cyber security standards by the National Institute of Standards and Technology (NIST) to "determine if they contain provisions that will protect the Bulk-Power System better than the CIP Reliability Standards," FERC said. But FERC did not direct NERC to adopt the NIST standards because that could lead to possible delays in putting into place any mandatory and enforceable standards.

The mandatory reliability standards require certain users, owners and operators of the bulk power system to establish policies, plans and procedures to safeguard physical and electronic access to control systems, to train personnel on security matters, to report security incidents, and to be prepared to recover from a cyber incident.

The eight CIP reliability standards address the following topics:

- Critical Cyber Asset Identification;
- Security Management Controls;
- Personnel and Training;
- Electronic Security Perimeters;
- Physical Security of Critical Cyber Assets;





- Systems Security Management;
- Incident Reporting and Response Planning; and
- Recovery Plans for Critical Cyber Assets.

The eight reliability standards were submitted to FERC for approval on Aug. 28, 2006. In December 2006, FERC staff issued a preliminary analysis of the cyber security reliability standards, and allowed for public comment. On July 20, 2007, FERC issued a Notice of Proposed Rulemaking proposing to approve the standards, proposing future modifications, and seeking public comment.

The final rule, “*Mandatory Reliability Standards for Critical Infrastructure Protection*,” takes effect 60 days from the later of either the date Congress receives the agency notice of the rule, or the date the rule is published in the *Federal Register*.

R08-1

(30)