Federal Energy Regulatory Commission
January 17, 2008
Open Commission Meeting
Statement of
Chairman Joseph T. Kelliher

Item E-2, Mandatory Reliability Standards for Critical Infrastructure (Docket No. RM06-22-000)

"Today the Commission approves final cyber security standards that will improve the reliability of the bulk power system. Specifically, we approve the eight cyber security standards in the proposed rule issued last July.

We have been very deliberate in our approach. As a first step, on December 11 2006, Office of Electric Reliability staff issued a preliminary assessment of the cyber security standards proposed by the Electric Reliability Organization. We also developed an extensive record in this proceeding, exceeding 1,200 pages.

We approve the proposed cyber security standards because we find they will improve bulk power system reliability and meet the statutory standard. But we also conclude there is a need to strengthen these standards, and we invoke our authority under section 215(d)(5) and direct the Electric Reliability Organization to submit to the Commission proposed modifications to certain provisions of the approved cyber security standards. In particular, we direct the Electric Reliability Organization to modify provisions relating to reasonable business judgment and acceptance of risk. These modifications will strengthen the reliability standards we approve today, and improve our defenses against cyber threats.

The reliability standard provisions in the Energy Policy Act of 2005 were designed to limit our vulnerability to the kind of reliability threats that have caused major regional blackouts in the past. For example, one common feature of past regional blackouts was poor vegetation management. The reliability standards we approved last year address that threat, as well as other similar threats, such as poor relay maintenance. Making voluntary standards mandatory and enforceable has already improved compliance.

Cyber security is a different kind of threat, however. This threat is a conscious threat posed by a single hacker or even an organized group that may be deliberately trying to disrupt the grid.

FERC will act to assure cyber security of the transmission grid, to the full extent of our legal authority. The statutory process for establishing cyber security standards has challenges, but we are working within the established process. That is shown by our order today.

I want to be very clear that FERC is committed to assuring reliability of the bulk power system and guarding against cyber security threats."