

Press Release

FOR IMMEDIATE DISTRIBUTION

CONTACT: Kelly Ziegler

609.452.8060

kelly.ziegler@nerc.net

Strengthened Cyber Security Standards Approved

PRINCETON, N.J., May 6, 2009 — Eight revised cyber security standards for the North American bulk power system were approved by the North American Electric Reliability Corporation's (NERC) independent Board of Trustees today. Today's action represents the completion of phase one of NERC's cyber security standards revision work plan which was launched in July 2008. Work continues on phase two of the revision plan, with version three standards already under development.

The revised standards were passed by the electric industry last week with an 88% approval rating, evidence of the industry's strong support for NERC's standards development process and the more stringent standards.

The standards are comprised of approximately 40 "good housekeeping" requirements designed to lay a solid foundation of sound security practices that, if properly implemented, will develop the capabilities needed to secure critical infrastructure from cyber security threats. Roughly half of those requirements were modified to clarify or strengthen the standards in this initial, expedited revisions phase.

Today's revisions begin to address concerns raised by the Federal Energy Regulatory Commission in its Order No. 706, in which it conditionally approved the standards currently in effect. The revisions notably include the removal of the term "reasonable business judgment" from the standards.

Entities found in violation of the standards can be fined up to \$1 million per day, per violation in the U.S., with other enforcement provisions in place throughout much of Canada. Audits for compliance with 13 requirements in the cyber security standards currently in effect will begin on July 1, 2009.

"The approval of these revisions is evidence that NERC's industry-driven standards development process is producing results, with the aim of developing a strong foundation for the cyber

security of the electric grid,” commented Michael Assante, Vice President and Chief Security Officer at NERC. “We applaud the work of the standards drafting team leading this effort and look forward to presenting phase two of the revisions to the board for approval early in 2010.”

“It’s important to note, however, that these standards are not designed to address specific, imminent cyber security threats,” he continued. “We firmly believe carefully crafted emergency authority is needed at the government level to address this gap.”

The revised Critical Infrastructure Protection reliability standards are available at:
http://www.nerc.com/docs/standards/sar/CIP_Standards_Redline_to_last_posting_2009Feb24.zip

The drafting team leading NERC’s cyber security standards revision efforts is comprised of 24 cyber security experts from across the electric industry. View the team members online at:
http://www.nerc.com/docs/standards/sar/Drafting_Team_Roster_External_Version.pdf

NOTE TO MEDIA:

More information on NERC’s Standards Development Process is available at:
http://www.nerc.com/fileUploads/File/Training/Webinar-NERC-102_Standards_Process.pdf

The North American Electric Reliability Corporation (NERC) is an international regulatory authority for electric reliability of the bulk power system in North America. NERC develops and enforces reliability standards; assesses adequacy annually via a 10-year forecast and winter and summer forecasts; monitors the bulk power system; and educates, trains, and certifies industry personnel. NERC is a self-regulatory organization, subject to oversight by the U.S. Federal Energy Regulatory Commission and governmental authorities in Canada. Learn more at www.nerc.com.

###