

► **Get the white paper**



Print This Article

<< Return to [NERC president: Emergency cybersecurity help needed](#)

## NERC president: Emergency cybersecurity help needed

[Angela Moscaritolo](#)

May 08 2009

Efforts of the North American Electric Reliability Corp. (NERC) to secure the nation's power grid against cyberthreats cannot substitute for additional emergency authority at the federal level, urged Richard Sergel, president and CEO of NERC, in [testimony](#) during a Senate hearing on cybersecurity Tuesday.

“The federal government should be given additional, carefully crafted emergency authority to address specific, imminent security threats,” Sergel said.

Sergel said NERC supports legislation [introduced last week](#), called *The Critical Infrastructure Protection Act*. The legislation would give the Federal Energy Regulatory Commission (FERC) authority to issue emergency rules or orders if a cyberthreat is perceived as imminent (FERC is the U.S. agency responsible for overseeing electric rates and natural gas pricing).

Sergel said the highest "priority gap" in the nation's cybersecurity protection is the lack of emergency authority and the new legislation would address that gap. In his testimony, Sergel also discussed the “significant progress” NERC has made to improve protection for the North American bulk power system against cyberthreats.

This week, NERC approved a revised set of cybersecurity standards for the bulk power system that clarify and strengthen those currently in effect, Sergel said.

NERC previously developed the cybersecurity standards that were [approved by FERC](#) in January 2008. These standards govern asset identification, management controls, personnel and training, perimeters, physical security, systems management, incident response and reporting and disaster recovery. One of the revisions approved this week eliminate the right for organizations to use "reasonable business judgment" as a reason for not complying with the guidelines, according to a [news release](#) from NERC.

The revisions were approved by the electric industry last week and by NERC's board of trustees Wednesday. Next, the revised standards will go to FERC for expected approval in early 2010.

Entities in violation of the standards can be fined up to \$1 million per day per violation in the United States, with other enforcement provisions in place throughout much of Canada. Audits for compliance with certain cybersecurity standards will begin on July 1, 2009, the NERC news release said.

“What continues to be missing from [Sergel's] testimony, and from the NERC standards, is that to effectively feed FERC intelligence to exercise its emergency authorities, it needs threat intelligence both from federal

government intelligence agencies and from the private sector itself that owns and operates electric grid assets,” Brian Ahern, president and CEO of vendor Industrial Defender, told SCMagazineUS.com in an email Thursday.