

## Critics say bill to protect electric grid from cyberattacks lacks teeth

By Jill R. Aitoro 04/29/09

A bill expected to be introduced in the House and Senate this week would help protect the computers that control the country's power grid, but it does not go far enough, security experts said on Wednesday.

The legislation would give federal regulatory agencies more power, but would not prompt owners and operators of electrical facilities to do their part to enhance cybersecurity, critics said. The bill also should be expanded to address other components of the nation's critical infrastructure, such as transportation and water, they added.

The measure -- which represents a joint effort by Senate Homeland Security and Governmental Affairs Chairman Joseph Lieberman, I-Conn., and House Homeland Security Chairman Bennie Thompson, D-Miss. -- would amend the 1935 Federal Power Act to provide "additional legal authorities to adequately protect the critical electric infrastructure against cyberattack." It would require the Federal Energy Regulatory Commission, which administers security standards for most of the nation's power plants, to establish within 120 days of its enactment interim cybersecurity standards to replace existing guidelines deemed inadequate.

The legislative effort follows a report earlier this month that intelligence officials discovered malicious software on computers that control the nation's power grid.

"We need a baseline standard of practice to drive toward measurable uniformity in the security of this essential national asset," said Gregory Garcia, who was assistant secretary of cybersecurity and telecommunications at the Homeland Security Department during the Bush administration and now runs his own information security consulting firm, Garcia Strategies. "This bill could move us in that direction, provided FERC leverages standards already adopted or in [the] process [of being adopted], rather than starting a whole new regime that could meet resistance and delay uptake."

Under the 2005 Energy Policy Act, the North American Electric Reliability Corporation develops standards for power plants and FERC approves them. Jacob Oclott, staff director of the House Homeland Security Subcommittee on Emerging Threats, Cybersecurity, Science and Technology, said the interim FERC standards would remain in effect until NERC has a chance to introduce replacement rules.

"We are not eliminating the current standards-setting regime," Oclott said. "We are creating a system whereby FERC can immediately modify inadequate cyber standards."

Alan Paller, director of research at the SANS Institute, said the bill was "almost perfect," but questioned NERC's ability to establish and enforce standards quickly. NERC has the legal authority to enforce reliability standards with users, owners and operators of the bulk power system. But some argue its enforcement efforts are too weak.

"NERC members, many of whom do not have a deep understanding of how cyberattacks work, are spending endless hours on discussion -- while the house is burning," Paller said. "The legislation should set deadlines for the [standards-making] process and say that NERC must vet the people's knowledge and skills so clueless people don't put the entire nation at risk."

Michael Jacobs, who served as information assurance director at the National Security Agency until his retirement in 2002, said owners and operators of electrical facilities should be required to take more safety measures.

"The bill focuses entirely on requirements of the government -- there's nothing in there that obligates or enables the owners and operators of these facilities to upgrade their security," Jacobs said. "There ought to be an obligation to put in place the necessary barriers to prevent an intruder from getting to the control systems themselves."

He recommended white list software programs, which allow administrators to establish a list of e-mail addresses or domain names that have permission to send messages and computing commands to the control system. Any messages or commands delivered from different addresses or domains would be rejected.

Jacobs also noted that the bill fails to address network security of other segments of the nation's critical infrastructure. "The same threats apply to water systems, transportation systems and energy systems of all types," he said. "In terms of a hierarchical order, yes -- the electrical grid powers everything. But if you're able to maintain that, then hackers will just start attacking other places."

Tom Kellermann, vice president of security awareness at Core Security Technologies and former senior data risk management specialist for the World Bank treasury security team, agreed that the requirements should be expanded, but said that could be accomplished in separate legislation.

"This bill represents a paradigm shift -- one which champions government leadership per critical infrastructure security," he said. "It illustrates that the threat is real and that reactive cybersecurity cannot be tolerated when it comes to protecting our electric infrastructure."

---

**COMMENT ON THIS ARTICLE IN THE FORUM**

---