

**House and Senate Homeland Security Chairmen Introduce Bill
to Dramatically Increase FERC's Cyber Security Authority**

May 1, 2009

Yesterday, Senate Homeland Security and Governmental Affairs Committee Chairman Joseph Lieberman (I-CT) and House Homeland Security Committee Chairman Bennie Thompson (D-MS) introduced a bill that would dramatically increase the authority of the Federal Energy Regulatory Commission (FERC) to respond to cyber threats to the nation's power grid. Under the proposed bill, the Critical Infrastructure Protection Act (H.R. 2195 and S. 946), FERC would have the authority to immediately respond to cyber threats identified by the Department of Homeland Security (DHS). In introducing the bill, Senator Lieberman stated: "We rely on cyberspace for so much of what is at the heart of our way of life. And our systems are not protected. We are focusing on the electricity cyber structure today because electricity is what so many critical sectors of the economy depend on."

The proposal is a direct response to recent events and threats, including news reports noting that the U.S. electrical system has been "routinely penetrated and compromised" by foreign actors, and the ongoing industry efforts to connect grid control systems to open networks. In addition, the bill notes that industry compliance with the existing Critical Infrastructure Protection (CIP) Reliability Standards has been problematic, as revealed by the recent North American Electric Reliability Corporation (NERC) report indicating that only 23% of utilities reported having Critical Cyber Assets. The bill suggests that this indicates that "many utilities are underreporting their assets, potentially to avoid compliance requirements."

To address these threats, the bill:

- Requires DHS to report to both Congress and FERC on the vulnerabilities of the country's critical electric infrastructure and how to address them.
- Requires FERC, after receiving this report, to issue rules designed to protect critical electric infrastructure, and refine them on an ongoing basis.
- Grants FERC authority to issue, without prior notice or hearing, any emergency rules or orders that it determines, after consulting with DHS, "must be issued immediately to protect critical electric infrastructure from an imminent threat or vulnerability." Such an emergency rule or order would only be effective for 90 days unless FERC grants an opportunity for comment and subsequently affirms the rule or order.
- Requires FERC to issue, within 120 days, according to regular notice and comment procedures, interim cyber-security measures to supplement or replace the CIP Reliability Standards

developed by NERC. These interim measures could be replaced in the future by revised CIP Reliability Standards.

FERC's jurisdiction under this new authority would be very broad, covering "any entity that owns, controls, or operates critical electric infrastructure." What constitutes "critical electric infrastructure" would be determined by FERC in consultation with DHS, and could include any physical or cyber assets related to generation, transmission, distribution, or metering of electric energy if FERC determines that attacks on such assets, whether alone or in combination with attacks on other assets, would threaten or harm security, economic security, or public health or safety.

While this is the most significant of the recent cyber-security bills regarding the utility industry introduced in Congress in recent days, a number of other such bills have been introduced, including H.R. 2165, proposed earlier this week by John Barrow (D-GA), which also proposes to increase FERC's authority to address cyber threats; S. 778, proposed by John Rockefeller (D-WV), which would establish the Office of the National Cybersecurity Advisor; and S. 773, also proposed by Senator Rockefeller, which would centralize the U.S. response to cyber security for all critical infrastructure.

For further information on the information discussed in this LawFlash, please contact any of the following Morgan Lewis attorneys:

Washington, D.C.

John D. McGrane	202.739.5621	jmcgrane@morganlewis.com
Floyd L. Norton, IV	202.739.5620	fnorton@morganlewis.com
Stephen M. Spina	202.739.5958	sspina@morganlewis.com
Lawrence J. Chandler (Nuclear)	202.739.5780	lchandler@morganlewis.com

About Morgan, Lewis & Bockius LLP

Morgan Lewis is an international law firm with more than 1,400 lawyers in 22 offices located in Beijing, Boston, Brussels, Chicago, Dallas, Frankfurt, Harrisburg, Houston, Irvine, London, Los Angeles, Miami, Minneapolis, New York, Palo Alto, Paris, Philadelphia, Pittsburgh, Princeton, San Francisco, Tokyo, and Washington, D.C. For more information about Morgan Lewis, please visit www.morganlewis.com.

This LawFlash is provided as a general informational service to clients and friends of Morgan, Lewis & Bockius LLP. It should not be construed as, and does not constitute, legal advice on any specific matter, nor does this message create an attorney-client relationship. These materials may be considered Attorney Advertising in some states. Please note that the prior results discussed in the material do not guarantee similar outcomes.

© 2009 Morgan, Lewis & Bockius LLP. All Rights Reserved.