ReedSmith

Client Alert

Global Regulatory Enforcement

Electric Grid Cyber Threat Concerns Raised Last Week During an Intense Push for General Cybersecurity Legislation

If you have questions or would like additional information on the material covered in this Alert, please contact one of the authors:

Amy S. Koch
Partner, Washington, D.C.
+1 202 414 9223
akoch@reedsmith.com

Amy Mushahwar
Senior Associate,
Washington, D.C.
+1 202 414 9295
amushahwar@reedsmith.com

Christine E. Nielsen
Associate, Washington, D.C.
+1 312 207 6459
cnielsen@reedsmith.com

…or the Reed Smith lawyer with whom you regularly work.

Since three cyber security bills passed the House in April (H.R.2096, H.R.3523, and H.R.3834), all eyes have been on Washington for cyber security developments in the Senate. This past week there were several. The week began with a hearing on Tuesday, July 17, by the U.S. Senate Committee on Energy and Natural Resources "to examine the status of action taken to ensure that the electric grid is protected from cyber attacks," inviting witnesses from the Federal Energy Regulatory Commission (FERC), the Government Accountability Office (GAO), North American Electric Reliability Corporation (NERC), and the Public Utilities Commission of Ohio. On Thursday morning, an editorial from President Obama appeared in the *Wall Street Journal* urging the Senate to pass a cyber security compromise bill. Then, late on Thursday, Sen. Lieberman released the text of a compromise proposal. We provide our download of the week's events below.

Wednesday's Senate Energy and Natural Resources Committee Electric Grid Hearing: Wednesday's hearing was in response to an article June 14 in CNET titled "Disaster awaits U.S. power grid as cyber security lags." The fear, the mechanism for creating digital signatures for authentication, is insufficient (especially for those control systems on the electric grid). The article noted, as have others that the U.S. electric grid has already become a bull's eye for Chinese and Russian cyber attacks.

Lawmakers admitted that the U.S. grid is not as secure as it could be despite efforts such as the NERC's promulgation of new Critical Infrastructure Protection (CIP) standards several years ago. For example, the electric industry uses process control systems that lack a proficient, organization-wide, incident-reporting mechanism, which makes them less sensitive to advanced persistent cyber

threats. Arguably, one of the most serious vulnerabilities to the electric industry is the vulnerability of the supervisory control and data acquisition (SCADA) systems, which control electric assets from a central command center. Originally, SCADA systems were used to control processes for a single site. However, advances in computer technology and the restructuring of the U.S. electric industry have created a more interconnected environment, and SCADA systems have become more vulnerable to cyber attacks.

The Committee invited witnesses from FERC, the GAO, NERC, and the Public Utilities Commission of Ohio. All witnesses agreed that legislation should include flexible cyber security standards, a more robust enforcement mechanism for those flexible standards, and a plan to better share information between the government and the electric utility industry.

Preparing for and preventing every type of cyber attack is impossible, but given the more interconnected environment that industry now faces, information sharing is a crucial step to recognizing and repairing network threats and vulnerabilities, especially as technology evolves. Information sharing includes the government divulging information it has on known cyber threats, as well as the industry divulging its own vulnerabilities. Currently, the government does not turn over certain information unless the receiving party has the appropriate security clearance, and industry is reluctant to report its own vulnerabilities for fear of reprisals. This lack of information flow stymies progress, and leaves all systems vulnerable to attack. In addition, witnesses from FERC and NERC both pointed to their lack of enforcement authority as a barrier to acting quickly in the event of a large cyber event to the electric grid that threatens national security. Many other cyber security threats and vulnerabilities were also discussed, including physical threats, such as EMP (electromagnetic pulse) attacks or solar flares, sabotage of overseas IT supply chain manufacturing, and the lack of well-trained cyber security workers.

The bottom line of this hearing: lawmakers concurred that legislative action is warranted. Three bills were of particular importance in this hearing: S.1342, the Grid Cyber Security Act; S.3342, the SECURE IT Act; and S.2105, the Cybersecurity Act of 2012. All three bills address the concerns voiced by the witnesses at Tuesday's hearing, with a specific emphasis on sharing information between government and industry. The proposed pieces of legislation address industry concerns by prohibiting federal entities with which cyber threat information is shared, from using that information in a regulatory enforcement action against the voluntarily disclosing company. The Grid Cyber Security Act, sponsored by Committee Chair Jeff Bingaman (D N.M.), places FERC in charge of

revamping the current cyber security system for the electric grid and authorizes enforcement of persons subject to FERC jurisdiction. The SECURE IT Act, sponsored by Sen. John McCain (R-Ariz.), assigns cyber security tasks to various agencies and cyber security centers, and includes what was described by co-sponsor Sen. Lisa Murkowski (R Alaska) as "flexible standards" for information sharing. In Sen. Murkowski's view, the SECURE IT Act strikes the right balance between enforcement by federal regulators and strong self-regulation by an industry that believes cooperation is the key to addressing this problem. The Cybersecurity Act of 2012, sponsored by Sen. Joe Lieberman (I-Conn.) and co-sponsored by one Republican and three Democrats, places the Department of Homeland Security in charge of creating one cyber security center and creating and enforcing risk-based security standards, which Sen. Murkowski labeled as "prescriptive."

Thursday Morning's Presidential Call for Cyber Security Legislation: In a very rare presidential editorial published by the *Wall Street Journal*, President Obama explained the national security necessity of effective cyber security protocols, and "urge[d] the Senate to pass the Cybersecurity Act of 2012 and Congress to send [him] comprehensive legislation so [he] can sign it into law." Echoing the expressed needs of the witness panel at the Senate's Energy and Natural Resources Committee Electric Grid Hearing, the president sought legislation with an effective information-sharing system between the federal government and private industry. President Obama also mentioned the need for responsible liability protection for companies engaged in good faith security information-sharing activities.

Late Thursday Night: Sen. Lieberman Released His Revised Cybersecurity Act of 2012 On Thursday, July 19, Senator Lieberman released a revised version of the Cybersecurity Act of 2012 with changes to the information-sharing and critical infrastructure sections, which he hopes will draw the support of both parties. In response to the Republican criticism of the original bill's mandatory security standards for the private sector, the revised bill establishes "an incentives-based voluntary cyber security program for critical infrastructure to encourage owners to adopt voluntary outcome-based cybersecurity practices." Those owners who choose to become certified under the bill's Voluntary Cybersecurity Program for Critical Infrastructure will enjoy benefits such as liability protection, an expedited security clearance process, and public recognition. The revised bill also addresses prior privacy and civil liberty concerns, ensuring that cyber security information shared with the government would be given directly to civilian agencies and not to military agencies.

Where Do We Go From Here? Although there has been much doubt that the Senate would be able to come together to pass a cyber security bill before the August 6 recess, recent developments make it clear that passing the Cybersecurity Act of 2012, impacting all critical infrastructure, is a priority. Sen. Lieberman, who has

announced he will be retiring at the end of the year, is using the full weight of his 40-year political career to get this bill passed. The bill's revision was the product of many political compromises, and its bipartisan co-sponsorship could foreshadow similar support in Congress. These developments could mean movement in the otherwise stymied Congress, which has already eased into the election season. We will monitor the progress of the legislation and update you as events evolve.