SUTHERLAND

LEGAL ALERT

February 22, 2011

Legislation Introduced to Address Vulnerabilities of Power Grid to Cyber Threats

Recently proposed federal legislation seeks to prevent and mitigate the impacts of cybersecurity attacks on the critical components of the Nation's electrical infrastructure. In particular, the "SHIELD Act" aims to secure the bulk-power system and electrical infrastructure critical to the defense of the United States against the threat of a malicious electromagnetic pulse (EMP) or natural geomagnetic disturbance (GMD) that could cause widespread and long-lasting disruption, damage or destruction of electrical equipment. Other legislation proposes greater coordination among federal agencies in identifying and protecting against cyber threats, while seeking to safeguard privacy and civil liberties. These proposals are among other recent initiatives by the federal government to address the vulnerabilities of the power grid to cyber threats.

SHIELD Act

Introduced on February 11, 2011 by Congressman Trent Franks (R-Arizona), the Secure High-voltage Infrastructure for Electricity from Lethal Damage Act (H.R. 668) (SHIELD Act) focuses on the threat posed by malicious EMPs (such as nuclear arms attacks) and natural GMDs (such as solar flares) to the physical reliability of the Nation's electrical infrastructure. Similar to last year's proposed Grid Reliability and Infrastructure Defense Act (GRID Act), the SHIELD Act would (among other things):

- Authorize the Federal Energy Regulatory Commission (FERC), upon identification of an imminent grid security threat arising from malicious EMPs or natural GMDs, to issue orders to the North American Electric Reliability Corporation (NERC), the Regional Entities charged with enforcing the mandatory NERC Reliability Standards, and users, owners and operators of the bulk-power system to take emergency measures to protect the reliability of the bulk-power system and/or defense critical electric infrastructure;
- Authorize FERC to provide for cost recovery of "substantial costs" incurred in compliance with such emergency orders;
- Authorize FERC to issue rules or orders to protect against grid security vulnerabilities to malicious EMPs where FERC determines that the NERC Reliability Standards do not provide for sufficient protection; FERC's rules or orders would be rescinded upon approval of a sufficient NERC Reliability Standard;
- Require NERC to propose, within one year, Reliability Standards addressing "reasonably foreseeable" EMPs and GMDs, based upon FERC's specification of the "nature and magnitude" of such threats; such Reliability Standards would be required to balance the attendant risks and mitigation costs;
- Require NERC to propose, within two years, Reliability Standards addressing the availability of "large transformers" capable of restoring reliable operations after an EMP or GMD event; such Reliability Standards would be required to balance risks and costs and would require entities that own or operate large transformers to ensure adequate availability of large transformers in the event they are destroyed or disabled by an EMP or GMD occurrence; and
- Require the President to identify up to 100 critical defense facilities that would be subject to FERC rules and orders prescribing measures to take to protect against malicious EMPs, subject

to the owners of the facilities agreeing to incur the costs necessary to comply with the FERC rules and orders.

Other Cybersecurity Legislation

Also proposed in Congress is the Senate's Cyber Security and American Cyber Competitiveness Act of 2011 (S. 21), which is currently in committee. S. 21 calls for further legislation to protect critical electrical infrastructure against cyber attacks, with a focus on the threat of man-made cyber attacks, America's increasing dependence on information technology, and a growing need for cooperation among federal agencies and integration of cybersecurity efforts.

Most recently, on February 17, 2011, Senators Joe Lieberman (I-Connecticut), Susan Collins (R-Maine), and Thomas Carper (D-Delaware) introduced the Cyber Security and Internet Freedom Act of 2011 (S. 413), a comprehensive Internet cybersecurity protection bill. Among other things, S. 413 would establish a new Office of Cyberspace Policy within the Executive Office of the President to coordinate and oversee, in conjunction with a new National Center for Cybersecurity and Communications within the Department of Homeland Security, federal policies and activities on cyberspace "security and resiliency," including protection of the computer systems of the Nation's critical infrastructure, prioritization of national cybersecurity strategies, and access to and sharing of cybersecurity-related law enforcement, intelligence and terrorism information. S. 413 also would strengthen the federal government's ability to set, monitor compliance with, and enforce standards and policies for securing federal and civilian systems and the sensitive information that they contain. Like the SHIELD Act, S. 413 would authorize the President, within prescribed limits, to declare cyber emergencies, in response to which covered entities would be required to implement plans to mitigate impacts on "covered critical infrastructure" (*i.e.*, systems and assets that could cause "national or regional catastrophic effects" if disrupted or destroyed).

Recent Cybersecurity Regulatory Initiatives

Federal administrative agencies also have been active in addressing cybersecurity and reliability concerns. For example, on February 8, 2011, FERC held a reliability technical conference (Docket No. AD11-6) to discuss priorities for addressing risks to the reliability of the bulk-power system. Electric power stakeholders expressed their growing concerns with cybersecurity threats against the Nation's bulk-power system and steps being taken by regulators to combat these increasingly prominent threats. There was a general call for improved communication and constructive collaboration among stakeholders as cybersecurity standards are developed and implemented. Comments regarding matters discussed during the conference are due to FERC by March 21, 2011.

Notwithstanding these efforts, FERC has come under fire from other federal agencies for its handling of cybersecurity-related matters. In a January 2011 audit report, the Government Accountability Office criticized FERC for not developing a coordinated approach to addressing cybersecurity concerns and monitoring compliance efforts among federal, state and local regulators. Also in January 2011, the Inspector General of the Department of Energy (DOE) released an audit report finding that the FERC-approved cybersecurity standards (the Critical Infrastructure Protection, or CIP, Reliability Standards) and general FERC oversight of those guidelines have been inadequate, citing a need to shift FERC's regulatory focus away from overly burdensome documentation requirements to allow industry participants to better allocate resources to mitigate higher-risk threats.

In an effort to better coordinate federal regulatory initiatives, on February 1, 2011 the DOE announced a collaborative grid cybersecurity initiative with NERC and the National Institute of Standards and

Technology (NIST). The collaborative effort aims to create a risk management process guideline for the electric industry that provides the flexibility needed for utilities to effectively and efficiently understand and manage cybersecurity risks, and to address risks at the organization, mission and business process, and information security levels. While FERC is invited to participate in the effort, it is not identified as a member of the initiative's leadership team.

Conclusion

As amply demonstrated by the legislative and administrative initiatives discussed above, the potential vulnerabilities of the Nation's electrical infrastructure continue to capture the attention of Congress and federal regulators. The policies, standards and requirements that will ultimately be established remain to be seen. With many federal agencies, statutes and regulations involved – both currently and as proposed – conflicts and ambiguities among the various agencies have arisen, others surely will follow, and they likely will remain unresolved in the absence of definitive legislation. Meanwhile, energy companies and other entities potentially subject to new and/or modified cybersecurity and reliability requirements face unknown compliance obligations and associated costs. The recent legislative proposals and regulatory initiatives appear to be a step in the right direction, but more work remains to provide clearer direction and greater coordination among federal efforts to address the potential vulnerabilities of the electric grid to cybersecurity threats.

■ ■ ■

If you have any questions about this Legal Alert, please feel free to contact any of the attorneys listed below or the Sutherland attorney with whom you regularly work.

Daniel E. Frank	202.383.0838	daniel.frank@sutherland.com
Alexandra D. Konieczny	202.383.0854	alexandra.konieczny@sutherland.com
Jennifer J. Kubicek	202.383.0822	jj.kubicek@sutherland.com