October 2012

Recent Federal Government Activity on Cybersecurity

The absence of congressional action on cybersecurity legislation has spurred efforts by various entities to exert influence over cybersecurity policy. This client alert will focus on some of those efforts, including Federal Energy Regulatory Commission (FERC) creation of a new cybersecurity office, North American Electric Reliability Corporation (NERC) action on cybersecurity Critical Infrastructure Protection (CIP) standards, continuing legislative developments concerning cybersecurity and anticipated White House executive orders on cybersecurity.

Cybersecurity has been one of the highest-profile topics in Washington this year. Yet, despite considering multiple cybersecurity bills, Congress left Washington for the upcoming elections without passing legislation. The chief architect of one such cybersecurity bill, Senator Joe Lieberman (I-CT), has expressed his view that legislation will not likely pass during the lame-duck session following the elections.

The main disagreement over cybersecurity legislation relates to granting the Department of Homeland Security (DHS) authority to set mandatory cybersecurity standards for critical infrastructure, accompanying liability protection, and, to a lesser degree, civil liberty concerns associated with public-private cybersecurity threat information exchanges.

With no new legislation forthcoming, officials are exploring cybersecurity policy options under existing authorities.

- **FERC Announces New Cybersecurity Office:** FERC has announced it is creating a new Office of Energy Infrastructure Security (OEIS) focused on potential physical and cybersecurity risks to energy facilities under its jurisdiction. According to FERC, OEIS will develop recommendations, provide assistance, participate in interagency efforts and conduct outreach with the private sector on physical and cybersecurity threats. OEIS will be led by Joseph McClelland, who has been Director of the Office of Electric Reliability since its formation in 2006.

- **NERC Activity on Cybersecurity:** NERC announced on October 1 that it is moving ahead with developing version 5 of its cybersecurity CIP standards. Balloting on the new version 5 CIP standards will be open until October 12. More information on the CIP standards can be found here. In addition, on October 3 the director of the NERC Electricity Sector Information Sharing and Analysis Center (ES-ISAC) distributed a letter to the electric industry. The letter informs the industry about developments and future actions in furtherance of the ES-ISAC's role in cyber security, in which it undertakes to ensure grid reliability through improved information sharing and analysis and coordinated sector readiness and triage response. The letter positions ES-ISAC as a "bridge" between peer industry members, and between the U.S. and Canadian governments, and requests industry commitment and participation in collaboration and information sharing in order for ES-ISAC to fulfill this role.

- **Senator Rockefeller Fortune 500 CEO Letter:** Senator John Rockefeller (D-WV), Chairman of the Senate Committee on Commerce, Science, and Transportation, recently sent a letter to the CEOs of Fortune 500 companies seeking information about company cybersecurity practices as well as those companies' views on federal legislation related to cybersecurity. Among other things, the letter asks the CEOs about each company's cybersecurity best practices, how those

practices are implemented, the federal government's involvement in developing those practices and whether the CEOs are concerned about the federal government becoming involved in a cybersecurity standards-setting process. The letter requests responses from the CEOs to the inquiries by October 19. While the letter does not have legal authority requiring action, it is a sign of continued congressional efforts on cybersecurity. The letter can be read here.

- **Cybersecurity Executive Order:** The White House has said it is working on an Executive Order (EO) patterned on Senator Lieberman's cybersecurity bill. While a draft has not been publicly released, the EO is said to establish a consultative process, led by DHS, to develop voluntary cybersecurity standards for critical infrastructure. Some have questioned whether, absent congressional action, the president can mandate voluntary cybersecurity standards. However, reports indicate the EO encourages departments and agencies to use existing authority to implement the voluntary cybersecurity standards. The EO also provides guidance to federal government bodies regarding information sharing.

- **CIP Presidential Decision Directive:** The Administration also reportedly is drafting a separate CIP Presidential Decision Directive (PDD) to update the 2003 Homeland Security Presidential Directive-7. A PDD carries significant influence as it is an EO developed through the National Security Council. The draft CIP PDD reportedly focuses on integrating DHS physical and cybersecurity activities, along with updating the National Infrastructure Protection Plan. Officials indicate the draft CIP PDD also addresses challenges faced by the public-private partnerships that were developed to confront national security interests in critical infrastructure and key resources.

Taken together, these developments suggest a piecemeal approach to cybersecurity in lieu of congressional action. Cybersecurity already presents difficult legal and compliance issues. These complexities will continue to be compounded by competing claims of jurisdiction and expertise as players with differing goals and objectives assert roles in cybersecurity policy.

For its part, FERC's creation of OEIS signals increased Commission action on energy cybersecurity issues. OEIS's establishment, in and of itself, does not substantively change electric utility compliance obligations. However, this development may indicate FERC intends to respond to presidential and congressional pressure with greater emphasis on cybersecurity or more aggressive investigations of cybersecurity incidents, and perhaps more substantial penalties. The new office may raise concerns within the electric utility industry that OEIS may attempt to strengthen the control of FERC in an arena currently structured for leadership by NERC and industry. Furthermore, while cybersecurity at FERC has been confined to the electric reliability program, OEIS's application to all FERC-jurisdictional "energy facilities" may suggest the Commission is seeking to expand its influence on cybersecurity practices beyond electricity to natural gas and oil pipeline industries. On the other hand, the industry could consider OEIS to be a benefit if it is able to head off electricity sector cybersecurity regulatory efforts by agencies with less sector-specific experience. Indeed, with appropriate input, OEIS could potentially be an effective voice for industry concerns in any interagency processes.

Going forward, dealing with these and similar issues in other industries will require a multifaceted approach that takes into account the policies, jurisdictional claims and bureaucratic interests of the relevant regulatory and executive agencies, as well as applicable legislative policies and actions, or lack thereof. The team at Hunton & Williams offers diverse experience and knowledge, positioning the firm to assist with all dimensions of cybersecurity concerns in the current technical and political environment.

- **Homeland Security:** The Homeland Security practice offers innovative solutions to the complex laws and policy issues that increasingly confront the private sector. The practice brings together a wealth of experience in security regulations, critical infrastructure, business continuity, crisis management, cybersecurity, internal investigations and government relations.

- **Regulated Markets and Energy Infrastructure:** The Regulated Markets and Energy Infrastructure practice provides high-quality legal services to national and international entities in the energy sector. Our attorneys are active before FERC, NERC and the regional reliability entities, and are involved in regulatory and legislative advocacy on a wide range of energy policy matters.

- **Federal Government Relations:** The Federal Government Relations practice comprises attorneys and legislative professionals committed to representing our clients' interests at all levels of local, regional, national and cross-border governing bodies in the United States and abroad. In this wide-ranging practice, our professionals combines legal and advocacy skills with strategic experience that has been developed over decades of work on an extensive variety of legislative, regulatory and policy projects.

- **Privacy and Data Security:** The Privacy and Data Security practice helps companies manage data at every step of the information life cycle. Hunton & Williams has been ranked as the top law firm globally for privacy and data security by *Computerworld* magazine each of its four surveys of more than 4,000 corporate privacy leaders.

- **Internal Investigations:** Hunton & Williams Partner John Delionado's internal investigations practice focuses on complex commercial litigation with an emphasis on internal investigations and cybersecurity matters. John has led investigations into potential cyber intrusions, cyber extortions and computer breach events for Fortune 500, major multinational and health care companies, including investigation into two of the largest reported credit card hacking events in retail history.

Contacts

John J. Delionado
jdelionado@hunton.com

Frederick R. Eames
feames@hunton.com

Eric M. Hutchins
ehutchins@hunton.com

Maida Oringher Lerner
mlerner@hunton.com

C. King Mallory, III
kmallory@hunton.com

Mark W. Menezes
mmenezes@hunton.com

Ted J. Murphy
tmurphy@hunton.com

Aaron P. Simpson
asimpson@hunton.com

Lisa J. Sotto
lsotto@hunton.com

Linda L. Walsh
lwalsh@hunton.com

Evan D. Wolff
ewolff@hunton.com

William F. Young
byoung@hunton.com