The CYBERSECURITY LAW REPORT

www.cslawreport.com Volume 2, Number 23 November 16, 2016

ENERGY

WilmerHale Attorneys Explain the Evolving Cybersecurity Environment of the Energy Sector

By Amy Terry Sheehan

Congress and federal agencies have dramatically strengthened cybersecurity requirements and authorities in the energy sector in recent years, with additional efforts underway. WilmerHale attorneys Jonathan Cedarbaum, Jason Chipman and Nathaniel Custer detailed these governmental efforts in an interview with The Cybersecurity Law Report, and discussed how the energy sector is responding to the changes. See also "*How the American Energy Industry Approaches Security and Emphasizes Information Sharing*" (Mar. 2, 2016).

CSLR: What are the most significant cybersecurity threats facing the energy sector?

WilmerHale: Governments and groups working in collaboration with them have made analyzing cyber vulnerabilities in energy production and distribution systems a high priority. Russian, Iranian, and Chinese hackers have demonstrated their capability to use cyber exploits to control and disrupt power grids, generation facilities, and sophisticated natural resource extraction operations. A recent Booz Allen Hamilton report collecting research on the December 2015 Russian attack on the Ukrainian electric grid, for example, provides an accessible description of how weaponized malware can be targeted at industrial control and supervisory control and data acquisition (SCADA) systems. The North American Electric Reliability Corporation (NERC) has also warned recently of distributed denial of service (DDOS) attacks in the energy sector. And the enormous rise of ransomware attacks has affected energy companies, too.

[See "*Energy Industry Demonstrates Public-Private Cybersecurity Coordination*" (Oct. 14, 2015).]

CSLR: What are the roles of the Federal Energy Regulatory Commission (FERC) and NERC?

WilmerHale: Under the Energy Policy Act of 2005, FERC has oversight authority for the country's bulk power system (i.e., the power grid). When it comes to cybersecurity, FERC has authority to promulgate mandatory regulations to protect the grid. FERC has designated NERC as the entity directly responsible for creating security rules for the bulk power system, subject to FERC's approval. These rules are promulgated through Critical Infrastructure Protection (CIP) standards. The CIP standards address more than just cybersecurity, but they do include cybersecurity-specific requirements.

CSLR: What recent legislation relevant to the sector has been passed?

WilmerHale: In 2015, Congress passed the Cybersecurity Act of 2015 and the Fixing America's Surface Transportation Act, both of which relate, in part, to cybersecurity in the energy sector.

[See "*Opportunities and Challenges of the Long-Awaited Cybersecurity Act of 2015*" (Jan. 6, 2016).]

CSLR: What is the purpose or focus of the Fixing America's Surface Transportation Act (FAST) Act?

WilmerHale: The FAST Act is a broad law intended to address many challenges to, and provide investment in, the nation's transportation infrastructure. In the realm of energy sector cybersecurity, the FAST Act includes several important provisions. First, the Act calls on the Secretary of Energy to adopt procedures for improved coordination within the federal government, with state and local governments, and with the industry to guard against and respond to disruptions to the country's oil and natural gas infrastructure.

The CYBERSECURITY LAW REPORT

www.cslawreport.com Volume 2, Number 23 November 16, 2016

Second, it authorizes the President to declare a "grid security emergency" when he determines that critical electric infrastructure or defense-critical electric infrastructure is being or imminently may be disrupted. The Secretary of Energy may then issue emergency orders to respond to the grid security emergency.

Third, the Act designates the Department of Energy as the lead cybersecurity agency for the energy sector. Fourth, it directs FERC to promulgate a regulatory framework for designating and protecting from disclosure "Critical Electric Infrastructure Information" drawing on its experience with Critical Energy Infrastructure Information. FERC issued its notice of proposed rulemaking on this in June 2016.

CSLR: What requirements does the FAST Act impose on the energy sector?

WilmerHale: The FAST Act does not itself impose any requirements on the industry with respect to cybersecurity in the energy sector. Elements of the FAST Act, however, do provide new authority to the Secretary of Energy. As the head of the lead cybersecurity agency for the energy sector, the Secretary of Energy has several duties and obligations, including: (i) coordinating with the Department of Homeland Security and other agencies responsible for cybersecurity; (ii) collaborating with owners of critical infrastructure associated with the energy sector; and (iii) collaborating with state and local and independent agencies. The Secretary of Energy has additional authority to issue emergency orders if and when the President declares a grid security emergency. In addition, as noted above, the FAST Act authorizes FERC to issue rules governing Critical Electric Infrastructure Information.

CSLR: Under what circumstances is the Emergency Presidential Authority to be used?

WilmerHale: The FAST Act defines two basic sets of circumstances that qualify as a "grid security emergency": (i) "a malicious act using electronic communication or an electromagnetic pulse, or a geomagnetic storm event" that has the potential to disrupt electronic devices and communications networks in a way that has significant adverse effects on the reliability of "critical electric infrastructure" or "defense critical electric infrastructure"; and (ii) a direct physical attack that causes significant adverse effects on critical electric infrastructure or defense critical electric infrastructure. The President may declare a grid security emergency when he or she determines that such conditions exists, or that there is an imminent threat that they will exist.

CSLR: What changes did The Cybersecurity Act of 2015 introduce for the energy sector?

WilmerHale: The Cybersecurity Act of 2015 authorizes any entity to share "cyber threat indicators" or "defensive measures" with another private entity or the government, subject to a variety of privacy protections. Cyber threat indicators or defensive measures shared pursuant to the Cybersecurity Act of 2015 may overlap with the category of Critical Electric Infrastructure Information that may be shared pursuant to the FAST Act. Unlike the Critical Electric Infrastructure Information provisions of the FAST Act, which are only applicable to specially designed data, the sharing provisions of the Cybersecurity Act apply to any set of data that satisfies the definition of "cyber threat indicator" or "defensive measure" under the law. Consequently, energy sector companies may in the future be more inclined to share cybersecurity information pursuant to the Cybersecurity Act of 2015.

CSLR: What happens once a grid security emergency is declared?

WilmerHale: A directive from the President that there is a grid security emergency in turn empowers the Secretary of Energy to take certain action. The FAST Act provides that the Secretary of Energy may "with or without notice, hearing, or report, issue such orders for emergency measures as are necessary in the judgment of the Secretary to protect or restore the reliability of critical electric infrastructure or of defense critical electric

infrastructure during such emergency." Orders issued by the Secretary expire after 15 days. The Secretary may be reissue emergency orders after those 15 days, but only if the President determines that the grid security emergency continues to exist.

CSLR: What is the National Infrastructure Protection Plan (NIPP) process?

WilmerHale: NIPP is a collective effort across the federal government and other public and private stakeholders to manage the risk to the critical infrastructure of the United States. The NIPP does this by collecting information to identify and prepare for threats to the nation's infrastructure; reduce vulnerabilities in critical assets, systems, and networks; and mitigate the potential consequences of adverse events. By naming the Department of Energy as the lead cybersecurity agency for the energy sector, the FAST Act may cement the Secretary of Energy's role in the NIPP process for those sectors that relate to the country's energy infrastructure.

CSLR: What is Critical Electric Infrastructure Information? How is it treated differently and why?

WilmerHale: The FAST Act requires FERC, in consultation with the Secretary of Energy, to promulgate regulations establishing procedures for certain information to be designated as Critical Electric Infrastructure Information. Once designated, Critical Electric Infrastructure Information will be exempt from disclosure under the Freedom of Information Act and will be specially protected from dissemination when received by government personnel. Critical Electric Infrastructure Information data can be much broader than information about cybersecurity threats – it can conceivably include data about physical vulnerabilities, layout, schematics, etc. – but it is likely to include network data and information about cyber vulnerabilities.

FERC's Notice of Proposed Rulemaking (NPRM) shows how the agency plans to fulfill this obligation under the FAST Act. FERC plans to incorporate Critical Electric Infrastructure Information into its existing system for similarly handling Critical Energy Infrastructure Information, while also updating the regulations governing that program. Critical Electric Infrastructure Information is broader than Critical Energy Infrastructure Information, and FERC's NPRM states that the definition of the former subsumes the latter. The NPRM also lays out FERC's plans for how Critical Electric Infrastructure Information will be designated, including issues such as the duration of the designation, the treatment of FERC-created data, and judicial review of designation decisions. The NPRM also shows FERC's intention for defining the duty imposed on FERC in handling Critical Electric Infrastructure Information so as to effectuate the FAST Act's requirement that such information not be disclosed without authorization.

CSLR: What actions has NERC taken?

WilmerHale: Earlier this year, with FERC's approval, NERC updated the Critical Infrastructure Protection (CIP) standards that relate to cybersecurity. This was done largely because of concerns about growing threats to the electrical grid.

CSLR: What steps must energy sector companies take to meet the CIP standards?

WilmerHale: The updated CIP standards require that facilities employ electronic security measures like encryption, firewalls, or multi-factor authentication to safeguard their networks. Facilities must also protect their computer systems against suspicious removable media like USB drives. Utilities must monitor physical access to and around their compounds by a combination of employing security guards and screening personnel, maintaining visitor logs, and utilizing motion sensors, badge readers, and electronic locks. Facilities must develop a test response plan that outlines how the facility will recover from a cyber-attack. Facilities must train their employees on managing cybersecurity events and on the test response plan. If a reportable cybersecurity event does occur, a utility must provide timely notification to the Electricity Information Sharing and Analysis Center (E-ISAC).

CSLR: How does the energy sector utilize the NIST framework? What other standards or frameworks does it use?

WilmerHale: In 2013, President Obama issued Executive Order 13636, Improving Critical Infrastructure Cybersecurity. EO 13636, which was accompanied by a Presidential Policy Directive, instructed the National Institute of Standards and Technology (NIST) to establish voluntary cybersecurity standards and for the Department of Homeland Security to identify critical infrastructure entities where a cyber attack "could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security." The NIST Framework is not specific to the energy sector, but energy companies are among those that use the NIST Framework as a critical benchmark to establish compliance with an established cybersecurity standard.

CSLR: How does the energy sector (public and private) utilize information sharing?

WilmerHale: The energy sector has three ISACs: the Electricity ISAC, or E-ISAC; the Oil & Natural Gas ISAC, or ONG-ISAC; and the Downstream Natural Gas ISAC, or DNG-ISAC. Each provides a platform for companies in those industries to share cyber threat information rapidly among members and with government partners. Members who share cyber threat data may also receive briefings from the government about developing threats, access to malware samples, and other data that may be useful for responding to particular threats. In November 2015, E-ISAC led GridEx-III, the largest grid security simulated exercise to date, and planning for GridEx-IV begins this week. In collaboration with relevant government agencies, energy companies participate on the Electricity Subsector Coordinating Council and the Oil and Natural Gas Subsector Coordinating Council, which address threats that go beyond, but also include, cybersecurity.

CSLR: How are the public and private sectors working together within the energy industry to strengthen cybersecurity? How does the private sector work with law enforcement (i.e., the FBI)?

WilmerHale: The past 24 months have seen growing outreach from federal executive branch agencies to notify energy-sector companies about developing or potential threats. The FBI often reaches out to utilities thought to be facing special cyber threats, and the Department of Homeland Security has expanded its Industrial Control System Emergency Response Team, which "works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among federal, state, local, tribal, and territorial governments and control systems owners, operators, and vendors." NERC also provides cyber alerts to electricity companies.