Energy Sector Alert Series: Cybersecurity Developments in the Energy Sector

NOVEMBER 4, 2016

In this eight-week alert series, we are providing a broad look at current and emerging issues facing the energy sector. Lawyers from across the firm are discussing issues ranging from cybersecurity, antitrust and intellectual property to the impact of both Brexit and the upcoming presidential election on the energy industry. Read our recent publications, including articles from a previous alert series published earlier this year. This WilmerHale Client Alert was also published in Law360 on December 12, 2016.

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.[1] Responding to these kinds of threats and others, Congress and federal agencies have dramatically strengthened cybersecurity requirements and authorities in the energy sector in recent year, and additional efforts are under way. Some of the most important recent developments include (i) enactment of the Cybersecurity Act and the FAST Act in December 2015; (ii) adoption of new critical infrastructure protection (CIP) standards under the direction of the Federal Energy Regulatory Commission (FERC) and the North American NERC; and (iii) growing efforts by industry to coordinate private sector responses to the threat. Several of those efforts, particularly ones that may be important for energy-sector companies to know about so that they can evaluate changes in the regulatory environment and potential government resources available to address cybersecurity, are described here.

I. Cybersecurity Legislation and the Energy Sector

Over the past 12 months, Congress has shown itself to be keenly focused on cybersecurity threats related to the energy sector with several pending bills focused on research for better grid-related cyber resiliency and Department of Energy authorities. Two developments in the past year, however, merit special attention. First, in December 2015, Congress created new emergency authorities for the President in the event of a cybersecurity crisis through the so-called Fixing America's Surface Transportation Act (FAST Act). Second, also in December 2015, Congress enacted the Cybersecurity Act of 2015 to encourage private sector and government cooperation to confront cybersecurity

threats, particularly threats to critical infrastructure such as the electrical grid. For many years the United States has lacked any broad consensus for how to establish better cybersecurity standards. Both the FAST Act and the Cybersecurity Act of 2015 are largely premised on the idea that existing guidance and regulations are not enough, that critical infrastructure in the United States is at risk, and, simply put, more needs to be done. While the Cybersecurity Act of 2015 is premised on voluntariness, the law forbids government use of voluntarily provided information as the basis for regulatory action, the cybersecurity provisions of the FAST Act open the door for unilateral regulatory action by authorizing the issuance of emergency orders.

A. The FAST Act

The FAST Act has three particularly significant provisions aimed at improving cybersecurity for the electrical sector. Each provision is described below.

(i) Emergency Presidential Authority

The Act allows the President to declare a "grid security emergency."[2] Once such an emergency has been declared, 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.[3]

The Act states that an order promulgated pursuant to this authority may apply to any (i) electric reliability organization, (ii) electric regional entity, or (iii) any user or owner or operator of "*critical electric infrastructure*" or of "*defense critical electric infrastructure*." These categories are likely to cover a very large amount of the electrical sector in the United States. "Critical electric infrastructure" is defined under the Act as:

> system or asset of the bulk-power system, whether physical or virtual, the incapacity or destruction of which would negatively affect national security, economic security, public health or safety, or any combination of such matters.[4]

The definition of "defense critical electric infrastructure" is even broader. The Act defines this category as:

> any electric infrastructure located in any of the 48 contiguous States or the District of Columbia that serves a facility designated by the Secretary pursuant to subsection (c), but is not owned or operated by the owner or operator of such facility.[5]

Subsection (c), in turn, directs the Secretary of Energy to designate "critical defense facilities," which are defined as facilities located in the 48 contiguous United States that are critical to the defense of the United States and vulnerable to a disruption of the supply of energy.[6] Put another way, the Act requires the Secretary of Energy to designate critical defense facilities and then, once those designations are in place, any "electrical infrastructure" that is especially important for maintaining power at those facilities may be the subject of an emergency regulation pursuant to the Act's emergency provisions.

These new emergency powers can apply to more than just a cyber-attack. The law allows a grid emergency to be declared in the event of a damaging geomagnetic storm, use of an electromagnetic pulse, or other assault on key electricity infrastructure, among other things. The authority is also familiar territory. Like the Communications Act of 1934, which includes similar provisions for the promulgation of emergency regulations in the event of a war,[7] the FAST Act provisions cast broad authority for the creation of new regulations to confront unanticipated problems in the future.

(ii) DoE as Lead Sector Specific Agency

The Act makes the Department of Energy the lead cybersecurity agency for the energy sector, and assigns the Secretary of Energy 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.[8] This portion of the Act is designed to put make the Secretary of Energy the primary federal coordinator of cybersecurity protection efforts for the energy sector, and may cement the Secretary's role in the National Infrastructure Protection Plan (NIPP) process.[9]

(iii) Critical Electric Infrastructure Information

The 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 (CEII) which shall be exempt from disclosure under the Freedom of Information Act and will be specially protected from dissemination when received by government personnel.[10] CEII 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.

The Act does not require any information sharing,[11] but it does provide broad liability protection for any voluntary sharing of CEII information that does occur.[12] Still, it is not clear on the face of the new law how regulations to be promulgated for designating and sharing CEII will ultimately relate to separate authorities that FERC already has to designate information as “critical energy infrastructure information.”[13] But given the existence of immunity protections and the possibility that CEII can be used to protect sensitive data generally, the creation of a new category of CEII will certainly be viewed as potentially significant for many energy companies in the coming years.

B. Cybersecurity Act of 2015

The relationship between CEII sharing provisions may be partly overtaken by the regime to be established pursuant to the Cybersecurity Act of 2015 for sharing “cyber threat indicators.” 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.[14] In this regard technical information about cyber threats (i.e., 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 CEII provisions of the FAST Act, which are only applicable to specially designed CEII 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.

II. Changing Energy Sector Cybersecurity Standards

Pursuant to the Energy Policy Act of 2005, FERC designated the North American Electric Reliability Corporation (NERC) as the entity responsible for creating security rules in the United States for the bulk power system.[15] These rules are promulgated through Critical Infrastructure Protection (CIP) standards that include cybersecurity specific requirements.[16]

Earlier this year, FERC updated CIP standards related to cybersecurity, largely because of concerns about growing threats to the electrical grid.[17] In particular, the CIP cybersecurity standards outline the minimum capabilities that utilities must develop to guard against cyber-attacks. For example, facilities must employ electronic security measures like encryption, firewalls, or multi-factor authentication to safeguard their networks.[18] They must also protect computer systems against suspicious removable media like USB drives.[19] Utilities must monitor physical access to and around their compounds by retaining security guards, screening personnel, maintaining visitor logs, or utilizing motion sensors, badge readers and electronic locks.[20]

The new standards also establish how utilities may effectively respond to cyberattacks. All facilities must train employees on managing cybersecurity events.[21] They must also develop and test response plans that outline how the facility will recover from a cyber-attack.[22] And in the event of a reportable cybersecurity incident, utilities must provide timely notification to E-ISAC.[23]

While the Department of Energy does not directly establish cybersecurity rules, it does, through a variety of forums, promulgate guidance and pursues efforts to encourage energy sector organizations to build cybersecurity into their network architecture. In 2013, President Obama issued Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*.[24] 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 DHS 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."[25] The NIST Framework has become a critical benchmark for many companies across multiple critical infrastructure sectors, including energy companies, to establish compliance with an established cybersecurity standard.[26] Some agencies are beginning to mandate compliance with other NIST standards as a condition of doing business with the government.[27]

At the state and local level, energy sector companies encounter an entirely different set of regulators. State and local utility commissions or other regulatory bodies generally regulate the local power distribution system. In 2013, the National Association of Regulatory Utility Commissioners (NARUC) published its *Resolution Regarding Cybersecurity Awareness and Initiatives*, which advised among other things:

> NARUC continues to encourage member commissions to become increasingly knowledgeable about cybersecurity threats to the relevant utility and pipeline sectors and to maintain an open dialogue with their regulated utilities to ensure adequate resources and expertise are being applied to deter, detect, and respond to cyber-attacks.[28]

And many state commissions have indeed responded to these growing concerns. For example, in April 2016, the Connecticut Public Utilities Regulatory Authority published new cybersecurity standards applicable to utilities in the state,[29] and it is likely that other state authorities will continue to revise existing standards to add more cybersecurity requirements in the coming years.

III. Voluntary Cybersecurity Initiatives

The regulations described above are important, but they are also relatively narrow. For many energy companies the marketplace is as important a source of cybersecurity guidance as regulators. NERC, the Department of Energy, and others have continued to focus attention on cooperative arrangements to encourage companies responsible for various parts of the grid to improve their security practices and to be better prepared to deal with an emergency.

Many of these efforts involve the Electricity Information Sharing and Analysis Center (E-ISAC), a public-private partnership through which companies in the energy sector share cyber threat information with one another and with the government. The E-ISAC is the primary information-sharing group for cyber threat data and helping members prepare for responding to cybersecurity events. For example, From November 18–19, 2015, E-ISAC led GridEx-III, the largest grid security simulated exercise to date.[30] 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.

The past 24 months has also seen growing outreach from federal executive branch agencies to notify energy-sector companies about developing or potential threats. The Federal Bureau of Investigation often reaches out to utilities thought to be facing special cyber threats. Likewise, 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."[31]

* * *

Energy companies are going to continue to encounter a fluid and changing environment relative to cybersecurity regulations, executive branch initiatives, and threats to their digital assets. Companies should ensure that they stay aware of developments in this area and, in light of the many threats companies may face take steps to prepare to respond to cyber threats that may be encountered in the future.

---

[1] *See* Evan Perez, *U.S. Investigators Find Proof of Cyberattack on Ukraine Power Grid*, CNN (Feb. 3,

2016); www.theblaze.com/stories/2015/12/21/ap-investigation-u-s-power-grid-vulnerable-to-foreign-hacks-public-often-kept-in-the-dark/.

[2] *See* Fixing America's Surface Transportation Act, Pub. L. No. 114-94 (hereinafter FAST Act) § 61003(a).

[3] *Id*.

[4] *Id*.

[5] *Id*.

[6] *Id*.

[7] *See* 47 U.S.C. § 606(a) (establishing Presidential power to prioritize communications activities during a war); 606(d)(empowering the President to suspend or amend regulations during a threat of war). During World War I the President was empowered "in time of war or public peril or disaster" to close, control, or take over and use all the radio stations within the jurisdiction of the United States." Act of August 13, 1912, 37 Stat. at L., 302 (Sec. 2).

[8] FAST Act § 61003(c).

[9] For a description of the NIPP and the related Presidential policy directives establishing sector specific agencies for various critical infrastructure sectors, see www.dhs.gov/national-infrastructure-protection-plan.

[10] FAST Act Section 61003(c)

[11] *Id*.

[12] *Id*.

[13] For more information about critical energy infrastructure information, see www.ferc.gov/legal/ceii-foia/ceii.asp.

[14] The Cybersecurity Act of 2015 was enacted as Division N in the Fiscal Year 2016 omnibus spending bill. The Act took effect on the date of its enactment (December 18, 2015). Title I of the Act, which includes the authorization and liability protections for cybersecurity monitoring, information-sharing, and use of defensive measures, will remain in effect with respect to any action authorized by or information obtained pursuant to it during the period ending on September 30, 2025.

[15] A thorough description of FERC authorities is available at www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity.asp.

[16] The Nuclear Regulatory Commission (NRC) has its own authority to regulate security standards for certain nuclear facilities. Toward that end, in January 2010, the NRC published *Cybersecurity Guidelines for Nuclear Facilities*, which provides instructions for how NRC licensees and license applicants can satisfy cybersecurity rules applicable to this highly regulated sector. A copy of the NRC guidance can be found at pbadupws.nrc.gov/docs/ML0903/ML090340159.pdf. According to the NRC website, the guidance "includes 'best practices' from such organizations as the International Society of Automation, the Institute of Electrical and Electronics Engineers, and the National Institute of Standards and Technology, and the Department of Homeland Security." Nuclear Regulatory Commission, *Backgrounder on Cyber Security* (Dec. 2014).

[17] *See, e.g.*, 18 C.F.R. Part 40 (Revised Critical Infrastructure Protection Reliability Standards) (Jan. 26, 2016).

[18] Cyber Security – Electronic Security Perimeter(s), CIP-005-5. All CIP standards cited are available at www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

[19] Cyber Security – Systems Security Management, CIP-007-6.

[20] Cyber Security – Systems Security Management, CIP-006-6.

[21] Cyber Security – Personnel and Training, CIP-004-6.

[22] Cyber Security – Recovery Plans for BES Cyber Systems, CIP-009-6.

[23] Cyber Security – Incident Reporting and Response Planning, CIP-008-5.

[24] *See* Jonathan Cedarbaum and Leah Schloss, *Implementation of the Cybersecurity Executive Order and President Policy Directive: Timetable and Processes*, 12 Privacy and Security Law Report 673 (Apr. 22, 2013).

[25] E.O. 13,636 (Feb. 12, 2013) at Section 9.

[26] *See* Energy Sector Cybersecurity Framework Implementation Guidance (Jan. 5, 2015).

[27] *See, e.g.*, 80 Fed. Reg. 81472 (Dec. 30, 2015).

[28] Resolution Regarding Cybersecurity Awareness and Initiatives, July 24, 2013.

[29] Connecticut Public Utilities Cybersecurity Action Plan, April 2, 2016.

[30] *See* NERC, *Grid Security Exercise: GridEx III Report* (March 2016). *See also* NERC, *Electricity ISAC*, (last visited Nov. 2, 2016) (describing the functions and role of E-ISAC); E-ISAC, *Understanding your E-ISAC* (June 2016) (background information on E-ISAC).

[31] www.brymar-consulting.com/wp-content/uploads/Misc/ICS-CERT_140520.pdf.

Authors

Jason C. Chipman

PARTNER

jason.chipman@wilmerhale.com

+1 202 663 6195