Morgan Lewis

insight

energy

Electric Utilities and the Cybersecurity Executive Order: Anticipating the Next Year

Stephen M. Spina & J. Daniel Skees

Electric Utilities and the Cybersecurity Executive Order: Anticipating the Next Year

By Stephen M. Spina & J. Daniel Skees[1]

America must also face the rapidly growing threat from cyber-attacks. We know hackers steal people's identities and infiltrate private e-mail. We know foreign countries and companies swipe our corporate secrets. Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, and our air traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy.

That's why, earlier today, I signed a new executive order that will strengthen our cyber defenses by increasing information sharing, and developing standards to protect our national security, our jobs, and our privacy. Now, Congress must act as well, by passing legislation to give our government a greater capacity to secure our networks and deter attacks.

–President Barack Obama
State of the Union Address
February 13, 2013

Cyber attacks are increasingly becoming a regular part of an electric utility's day-to-day business risks. News agencies provide an ongoing stream of reports on the increasing sophistication and danger of these attacks: 30,000 workstations disabled by a malicious virus at a Saudi oil firm[2], a generator's control system infected by malware carried on a USB drive[3], and a generator restart delayed for three weeks by a malware inadvertently uploaded to control systems by a technician.[4] Of the cyber incidents reported to the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team ("ICS-CERT") between October 2011 and September 2012, forty-one percent of incidents involved the energy sector, by far the largest number of incidents by sector.[5]

This does not mean that the electric industry is unprepared for this threat. Unlike most U.S. industries, the electric industry has dealt with cybersecurity regulation since the Federal Energy Regulatory Commission ("FERC") approved the initial batch of Critical Infrastructure Protection ("CIP") Reliability Standards developed by the North American Electric Reliability Corporation ("NERC") in January 2008.[6] These

[1] Stephen M. Spina is a partner and J. Daniel Skees is an associate at Morgan, Lewis & Bockius LLP in the firm's Washington, D.C. office. The views presented in this article are solely those of the authors, and do not represent the views of Morgan, Lewis & Bockius LLP.

[2] John Leyden, *Hack on Saudi Aramco hit 30,000 Workstations, oil firm admits*, THE REGISTER (Aug. 29, 2012, 09:18 GMT), http://www.theregister.co.uk/2012/08/29/saudi_aramco_malware_attack_analysis/.

[3] U.S. DEP'T OF HOMELAND SEC., ICT-CERT MONITOR 1–2 (October/November/December 2012), *available at* http://ics-cert.us-cert.gov/pdf/ICS-CERT_Monthly_Monitor_Oct-Dec2012.pdf.

[4] *Id*.

[5] For example, critical manufacturing was four percent of reported incidents and the water industry (the second highest) was fifteen percent of reported incidents. *Id.* at 5.

[6] *Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No. 706, 122 FERC ¶ 61,040 (2008), *order denying reh'g and granting clarification*, Order No. 706-A, 123 FERC ¶ 61,174 (2008), *order on clarification*, Order No. 706-B, 126 FERC ¶ 61,229 (2009), *order denying clarification*, Order No. 706-C, 127 FERC ¶ 61,273 (2009) .

Standards have been revised four times since then, and are widely seen as providing a base line of protection for electric industry cybersecurity. Although not without critics,[7] the across-the-board implementation of the CIP Reliability Standards by the electric industry places it well ahead of some other sectors of the U.S. economy that have operated essentially unregulated in this area.

Despite those existing mandatory protections, President Obama's recent executive order on cybersecurity (the "Executive Order" or "Order") will nevertheless likely bring significant changes to cybersecurity regulation in the electric industry. Although only in the earliest stages at this time, final implementation over the next year may result in the wider application of cybersecurity requirements to facilities that, up until now, have escaped regulation. Another potential outcome is that implementing the Executive Order could results in revisions to the NERC-developed CIP Reliability Standards to provide additional protections not currently addressed by those requirements.

This will likely result in increased costs to the industry, but at the same time could provide an opportunity to improve cybersecurity in a cost-effective manner. Currently, the National Association of Regulatory Utility Commissioners ("NARUC") has undertaken an effort to educate the states regarding the costs associated with cyber attacks.[8] Cyber risks and the threats they pose will only continue to grow, making increased security costs inevitable. But as any utility with long experience in CIP compliance will recognize, the funds expended on cybersecurity can be spent either efficiently or inefficiently. The electric industry can leverage its experience over the next year to encourage the development of a voluntary Cybersecurity Framework that values security over compliance and investments over documentation. Few other industries have a track record of cybersecurity regulation that can provide such value to the nation as it moves along this path.

This experience should not be wasted; it should instead serve as a guidepost to regulators, across industries, to ensure that President Obama's executive order results in meaningful, cost-effective security improvements, not simply additional regulatory costs.

1. The Failure of the Legislative Solution

For some time, there has been a bipartisan consensus that additional measures are necessary to protect the nation's critical infrastructure against cyberattacks that could cripple essential facilities and services. Consensus on the problem, however, has not led to consensus on the solution.

The Democratic legislative proposals, typified by the Cybersecurity Act of 2012,[9] focused on a mandatory cybersecurity compliance regime overseen by the Department of Homeland Security ("DHS"). It required DHS to identify critical infrastructure facilities for each industry, followed by the creation of cybersecurity performance requirements for each sector. Identified critical asset owners would then need to implement cybersecurity protections to meet the DHS-developed performance requirements and certify their implementation of those protections on a yearly basis or undergo a third-party assessment. These steps to meet the performance requirements would be supplemented by increased information-sharing between the federal government and private sector.

---

[7] *See, e.g.*, Jay Abshier & Phil Marasco, *How Can the NERC CIP Standards Be Improved?*, CONTROL GLOBAL (Dec. 6, 2010), http://www.controlglobal.com/articles/2010/NERCCIPStandards1012.html (criticizing the CIP Reliability Standards for focusing too heavily on documentation and failing to address key vulnerabilities, meaning that a utility can be compliant with the Reliability Standards, but still "very vulnerable" to cyberattacks).

[8] NARUC, CYBERSECURITY FOR STATE REGULATORS 2.0: WITH SAMPLE QUESTIONS FOR REGULATORS TO ASK UTILITIES (Feb. 2013).

[9] Cybersecurity Act of 2012, S. 2105, 112th Cong. (2012).

The Republican legislative approach, typified by Senator McCain's proposed Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act ("SECURE IT Act"), emphasized improved information sharing between the government and the private sector so that private industry could become aware of emerging threats far more quickly. In many ways, the SECURE IT Act was a reaction to what Republican senators saw as overreaching in the competing Democratic proposal, as it avoided any new cybersecurity standard authority while still implementing improvements to enhance security.

Neither approach was successful in 2012; this ultimately led President Obama to do as envisioned by the platform adopted by the Democratic Party at its 2012 convention and direct increased cybersecurity protections though his executive authority.[10] With no expectation that the new Congress would pass cyber legislation, the President signed Executive Order 13636 shortly before giving his State of the Union address, sidestepping the legislative impasse in a split Congress.[11] It remains possible that Congress will pass cybersecurity legislation this session,[12] but, as in any legislative prediction, the smart money is always on nothing—or at least nothing comprehensive.

2. The Executive Order

The Executive Order directs the Department of Homeland Security ("DHS") to identify critical infrastructure and encourage the designated owners and operators to adopt a voluntary cybersecurity program, called the Cybersecurity Framework, that will be developed by the National Institute of Standards and Technology ("NIST"). As reflected in the President's State of the Union Address, electric system infrastructure is certain to be identified as critical by DHS. What this means for the electric sector remains to be seen, but it is a near certainty that more security measures for more assets will be necessary.

(a) Identification of Critical Infrastructure

Over the first five months, DHS must use a risk-based approach to identify critical infrastructure that, if subject to a cyber attack, could have "catastrophic" effects on health, safety, the economy, or national security.[13] This analysis must be undertaken in consultation with various stakeholders, including consultations with "Sector-Specific Agencies,"[14] which for the energy sector is the Department of Energy ("DOE").[15] The other stakeholders involved in the consultative process include the owners and operators of critical infrastructure themselves, the Critical Infrastructure Partnership Advisory Council,[16] the Sector Coordinating Councils,[17] other agencies, state and local governments, universities, and other experts.[18]

---

[10] "President Obama has supported comprehensive cybersecurity legislation that would help business and government protect against risks of cyber attacks while also safeguarding the privacy rights of our citizens. And, going forward, the President will continue to take executive action to strengthen and update our cyber defenses."

[11] Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013) [hereinafter Exec. Order].

[12] For example, Senator Rockefeller recently introduced S. 31, entitled the "Cybersecurity and American Cyber Competitiveness Act of 2013," which outlines the "Sense of Congress" on the need for cybersecurity legislation addressing information sharing, increased cyberprotections, and private-public partnerships.

[13] Exec. Order § 9(a).

[14] *Id.* §§ 6, 9(a).

[15] Memorandum, The White House, Office of the Press Secretary, Presidential Policy Directive – Critical Infrastructure Security and Resilience, Presidential Policy Directive/PPD-21 (Feb. 12, 2013) (identifying DOE as the Sector-Specific Agency for the energy sector). Under Section 9(b) of the Executive Order, DOE is required to provide DHS with any information DHS needs for this analysis. The nuclear industry is carved out of DOE oversight, and instead DHS itself serves as the designated "sector-specific agency" for nuclear critical infrastructure.

[16] This group was established by DHS to coordinate federal infrastructure protection programs with state, local, and private infrastructure protection efforts.

[17] Also established by DHS as part of its National Infrastructure Protection Plan, Sector Coordinating Councils ("SCC") are self-organized coordination and planning entities that represent their respective industries. The Electricity SCC and Oil and Natural Gas SCC comprise the Energy SCC.

Once DHS identifies what it considers critical infrastructure using a "consistent, objective criteria," it will privately notify the relevant owners and operators of its determinations. This notification will include an explanation for its decision and an opportunity for the asset owners and operators to seek reconsideration in the event they disagree with the designation. The list of identified critical infrastructure will be reviewed and updated on an annual basis, and will be provided to the President.[19]

Because the vulnerability of the electric system to cyberattacks has been a constant source of concern for the President and Congress, DHS is likely to identify a significant number of electric assets as critical infrastructure under the Executive Order. DHS has not, as of this writing, indicated publically whether it will apply bright-line criteria to identify classes of assets that are *per se* critical infrastructure, or whether these decisions will be made on a facility-by-facility basis. Given the short deadlines and the obligation to use "consistent, objective" criteria, it is likely that some sort of bright-line criteria will be necessary, at least to cull the enormous number of electric infrastructure assets into a more manageable group.[20]

(b) Development of Voluntary Standards

The owners and operators of the identified critical infrastructure will then be encouraged to adopt a voluntary framework of cybersecurity protections termed the "Cybersecurity Framework." The Department of Commerce will direct the National Institute of Standards and Technology ("NIST") to develop the Cybersecurity Framework over the course of the next year using a notice-and-comment process.[21] The Cybersecurity Framework is intended to draw upon voluntary consensus standards and current industry best practices to the extent possible in developing "standards, methodologies, procedures, and processes" for addressing cyber risks.[22] The Cybersecurity Framework is intended to help owners and operators of critical infrastructure determine, analyze, and manage the cyber risks to its protected assets in a technologically neutral manner.[23] The Framework must take into consideration threat information provided by national intelligence agencies and be informed by the performance goals for the protection of critical infrastructure established by DHS. It must mitigate concerns about the confidentiality of business information, as well as privacy and civil liberty concerns.[24] The Cybersecurity Framework will also include measures for assessing ongoing compliance with the Framework.[25]

Although NIST is required to develop the Cybersecurity Framework through a consultative process with stakeholders, including the various federal, state, and local agencies, as well as the asset owners and operators, the Executive Order also provides for explicit public comment procedures. Within eight months, NIST must publish a preliminary Cybersecurity Framework, and the final Cybersecurity Framework will be due within a year.[26] The Framework will be reviewed and updated from time to time based on feedback from critical infrastructure owners and operators, changes in technology and risks, and the experience of implementing the Framework.[27]

---

[18] Exec. Order § 6.
[19] *Id.* § 9(a).
[20] It is possible that the bright-line criteria for identifying Critical Assets under the Version 4 CIP Reliability Standards may serve as a model. *See* N. AM. ELEC. RELIABILITY CORP., CIP-002-4, CRITICAL CYBER ASSET IDENTIFICATION 6, *available at* http://www.nerc.com/files/CIP-002-4.pdf.. The Version 4 Standards were approved in *Version 4 Critical Infrastructure Protection Reliability Standards*, Order No. 761, 139 FERC ¶ 61,058 (2012).
[21] Exec. Order § 7.
[22] *Id*. § 7(a).
[23] As stated in the Executive Order, the Cybersecurity Framework must provide a "prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk." *Id.* § 7(b).
[24] *Id.* § 7(c).
[25] *Id.* § 7(b).
[26] *Id.* § 7(e).
[27] *Id.* § 7(f).

The NIST notice and comment process, as well as the ongoing consultative process with stakeholders, should provide interested electric utilities with an opportunity to provide significant policy guidance and technical expertise to NIST. NIST has already begun its outreach efforts, providing notice that it intends to issue a public Request for Information ("RFI") to guide the development of the Framework.[28] The RFI will ask for feedback on a number of areas, including existing practices for managing cyber risks, the suitability and use of existing standards and publications that address cybersecurity needs, and the core cybersecurity practices implemented within specific agencies.

While acknowledging that the Cybersecurity Framework will apply to a wide variety of entities with vastly differing missions, NIST has explained that "there are core cybersecurity practices that can be identified and that will be applicable to a diversity of sectors and a spectrum of quickly evolving threats. Identifying such core practices will be a focus of the Framework development process."[29] The consultative process will include ongoing stakeholder engagement with the goal of developing the Framework through a "voluntary consensus-based process."

(c) Adoption of Voluntary Standards

Once NIST finishes developing the Cybersecurity Framework, DHS must develop a voluntary Cybersecurity Framework compliance program for the owners and operators of designated critical infrastructure.[30] The Executive Order does not outline the nature of the voluntary program or how it will operate, leaving that to the discretion of DHS, but does explain that sector-specific implementation guidance can be developed by each Sector-Specific Agency, along with "supplemental materials" to address the unique operating environments and cyber risks facing each sector.[31]

The voluntary compliance approach presents a key difference from the legislative proposals. Without new statutory authority, DHS cannot impose across-the-board requirements to mandate implementation of the Cybersecurity Framework. Instead, compliance will be pieced together through mandatory applicability, where possible, incentives, and a voluntary program to capture those critical infrastructure owners and operators that cannot be subjected to a mandatory cybersecurity regime in the absence of new legislation. DHS will look for ways to incentivize compliance under existing law.[32] The Executive Order also directs the relevant agencies to determine whether the Cybersecurity Framework could be incorporated into federal contracting obligations.[33]

The only enforcement-like tool is the mandatory compliance reporting that each Sector-Specific Agency will produce. For the energy industry, DOE will report to the President on an annual basis to describe which owners and operators of critical infrastructure are implementing the voluntary Cybersecurity Framework.[34] This level of executive notice could likely prove a powerful tool to encourage compliance. Not only will companies want to be reported as implementing the Framework, noncompliance and noncooperation could prove problematic in the event of a cyberattack.

In practice, it will be difficult for utilities who are notified that they own or operate critical infrastructure to avoid implementing the NIST Cybersecurity Framework. In addition to the methods described above, the Executive Order directs the agencies with authority over critical infrastructure to determine whether their

---

[28] NAT'L INST. OF STANDARDS AND TECH., FRAMEWORK FOR REDUCING CYBER RISKS TO CRITICAL INFRASTRUCTURE (2013), *available at* http://www.nist.gov/itl/upload/rfi_02_12_13.pdf.
[29] *Id.*
[30] Exec. Order § 8(a).
[31] *Id.* § 8(b).
[32] *Id.* § 8(d).
[33] *Id.* § 8(e).
[34] *Id.* § 8(c).

current regulatory requirements are sufficient to address cyber risks and whether they have the "clear authority to establish requirements based upon the Cybersecurity Framework" to protect their sector's critical infrastructure.[35] If their current regulatory requirements are insufficient, they must propose actions to mitigate the identified risk.[36]

The Federal Energy Regulatory Commission ("FERC") is an independent regulatory agency and therefore not directly subject to the Executive Order, but it is "encouraged to engage in a consultative process" with DHS, DOE, and other stakeholders to address these issues.[37] Based on a reading of the Executive Order, it is entirely possible that FERC could determine that new CIP Reliability Standards are necessary to implement the Framework.

(d) Cybersecurity Information Sharing

Outside of the Cybersecurity Framework requirements, the Executive Order also addresses the need for increased information sharing with private industry about threats to critical infrastructure identified by the intelligence community. Under the order, DHS, the Attorney General, and the Director of National Intelligence are required to improve their ability to share threat information with targeted entities.[38] This would take place through the creation of unclassified reports on cyber threats to a specific entity, which would be shared directly with that entity. The Executive Order also directs these agencies to provide classified reports to entities targeted by specific threats. This information would be shared with individuals at targeted entities who have appropriate authorizations. Furthermore, the Executive Order directs DHS to expedite its processing of security clearances to make that sharing possible.[39]

This program should allow utility security personnel to receive far more detailed threat information specific to their utility than they have traditionally received. Although the extent to which this information will be timely and actionable remains to be seen, it will certainly raise a utility's understanding of the specific cyber threats it faces.

(e) Civil Liberties

To address civil liberty concerns, the Executive Order establishes an oversight and reporting role for DHS's Chief Privacy Office and Officer for Civil Rights and Civil Liberties, and also directs other participating agencies to conduct assessments of their own activities under the Executive Order.[40]

Although the Order cannot provide additional protection from Freedom of Information Act requests for information submitted by private entities, it directs the agencies involved in the Executive Order activities to protect that information from disclosure "to the fullest extent permitted by law."[41] Consistent with this directive, any sensitive security information provided by utilities to any government agency under this Executive Order should take advantage of the relevant agency's information protection programs, such as the DHS Protected Critical Infrastructure Information ("PCII") Program[42] and FERC's Critical Energy Infrastructure Information ("CEII") Program.[43]

---

[35] *Id.* § 10(a).
[36] *Id.* § 10(b).
[37] *Id.* § 10(e).
[38] *Id.* § 4(a)-(b).
[39] *Id.* § 4(d).
[40] *Id.* § 5.
[41] *Id.* § 5(d).
[42] *See* 6 C.F.R. § 29 (2012).
[43] *See* 18 C.F.R. § 388.112-113 (2012).

(f) What the Executive Order Cannot Do

Although the Executive Order is far-reaching in addressing many of the same topics addressed by previously proposed cybersecurity legislation, there are many objectives it cannot legally fulfill. It does not provide mandatory and enforceable cybersecurity requirements (although it could be used to justify mandatory Reliability Standards). It does not provide liability protections for entities that implement the Cybersecurity Framework to protect them against claims related to cybersecurity attacks so as to encourage compliance or the exchange of cybersecurity-related information with the federal government or other entities.[44] It also fails to allocate any funds to encourage any of its initiatives.

Because of these holes that cannot be filled by executive actions, both parties continue to seek a legislative solution.

3. Existing and Future Cybersecurity Regulation in the Electric Industry

As the Edison Electric Institute stressed immediately after the publication of the Executive Order, the electric industry already receives significant protections under the CIP Reliability Standards: "As the only industry subject to mandatory and enforceable cybersecurity standards, the electric power sector already is taking significant steps to protect the electric grid and to work closely with the government to prevent, detect, and respond to cyber threats."[45]

The CIP Reliability Standards have been an increasing focus of both NERC, which is charged with developing them,[46] and FERC, which must review and approve the Standards before they can become mandatory.[47] The CIP Standards address those cyber assets that are essential to the operation of identified bulk-power system critical infrastructure, such as control centers, transmission substations, and generators, which are termed "Critical Assets."[48] Once these cyber assets are identified as "Critical Cyber Assets," they must receive the full panoply of CIP protections, including cyber protections, physical protections, cyber and physical access limitations, security training for appropriate personnel, and the development and implementation of incident response and asset recovery plans.[49] Violations of these Reliability Standards are punishable by fines of up to $1,000,000 per violation per day.[50]

The compliance history of the CIP Reliability Standards continues to be problematic. Of the dozens of Reliability Standards in effect, the CIP Reliability Standards are by far the most violated Standards. NERC's most recent statistics indicate that for calendar year 2012, the top three most-violated Reliability Standards

---

[44] *See, e.g.*, H. CYBERSECURITY TASK FORCE, 112TH CONG., RECOMMENDATIONS OF THE HOUSE REPUBLICAN CYBERSECURITY TASK FORCE 9, 11, http://thornberry.house.gov/uploadedfiles/cstf_final_recommendations.pdf. The Task Force explained that liability protections should address concerns related to "antitrust issues, liability, an exemption from the Freedom of Information Act ('FOIA'), protection from public disclosure, protection from regulatory use by government, and whether or not a private entity is operating as an agent of the government."

[45] Press Release, Edison Elec. Inst., EEI Statement on Obama Executive Order on Cybersecurity (Feb. 13, 2013), http://www.eei.org/newsroom/pressreleases/Releases/Pages/130213.aspx. *See* Press Release, Nat'l Rural Elec. Coop. Ass'n, NRECA Statement on White House Release of Cybersecurity Executive Order (Feb. 13, 2012), http://www.nreca.coop/press/Statements/Pages/NRECAStatementonWhiteHouseReleaseofCybersecurityExecutiveOrder.aspx.

[46] *See* 16 U.S.C. § 824o(d).

[47] *See id.* § 824o(d)(2).

[48] N. AM. ELEC. RELIABILITY CORP., CIP-002-3, CRITICAL CYBER ASSET IDENTIFICATION 2, *available at* http://www.nerc.com/files/CIP-002-3.pdf.

[49] These requirements are currently contained in Reliability Standards CIP-003-3 through CIP-009-3. On April 1, 2014, the Version 4 CIP Reliability Standards will go into effect pursuant to Order No. 761. *Version 4 Critical Infrastructure Protection Reliability Standards*, Order No. 761, 139 FERC ¶ 61,058 (2012). That order removes the discretion of entities to identify Critical Assets using their own methodology, but leaves the relevant cybersecurity measures unchanged.

[50] 16 U.S.C. 825o-1(b).

are CIP Standards, as are seven of the top twelve.[51] Not only are the compliance costs imposed by the CIP Reliability Standards widely considered high, the penalties for violating these obligations have also become more severe.

This compliance history has led to concerns within the electric industry that the Executive Order could have similar results on a broader basis, imposing significant compliance costs on the industry. Although implementation of the Executive Order is still in its earliest phases, these fears are well grounded.

4. The Scope of the Executive Order

One strong possibility is that the Executive Order will bring into the scope of cybersecurity regulation a broader array of electric infrastructure than is currently covered by the CIP Reliability Standards. This results from the jurisdictional limitations in the existing Federal Power Act provisions for Reliability Standards and the lack of such limitations in the Executive Order.

Under the Federal Power Act, Reliability Standards apply only to the "bulk-power system."[52] Although the Commission has taken the position that the term "bulk-power system" is potentially broader than NERC's traditional definition of the "bulk electric system,"[53] the Commission has decided to use the "bulk electric system" definition to delineate, for now, the scope of the facilities subject to Reliability Standards.[54] That definition is dependent on regional variations introduced by the Regional Entities and encompasses "the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher."[55] The definition excludes "radial transmission facilities serving only load with one transmission source."[56] This is consistent with the statutory limitation on the scope of Reliability Standards, which does not include local distribution facilities.[57]

This definition is soon to be replaced by a new definition recently adopted by FERC, which is intended to remove the Regional Entity discretion from the application of the bulk electric system definition and to add more bright-line clarity on types of facilities that are excluded or included by the definition.[58] The new definition captures transmission facilities and real and reactive power resources operated at 100 kV or higher, but excludes, again consistent with the statutory limitations on FERC's authority, any local distribution facilities. In addition, the new definition will exclude any radial systems emanating from a single transmission interconnection that serve only load or minor generation and will also exclude local networks used to distribute power to load rather than moving power across the interconnected electric system.

As reflected in the language of the statute, Reliability Standards are intended to protect the operations of the interconnected transmission system within the U.S., but not to preserve service to specific end users. Reliability Standards are intended to provide for "reliable operation of the bulk-power system,"[59] and that is achieved if the system is operated within thermal, voltage, and stability limits in such a manner that

---

[51] *See* N. AM. ELEC. RELIABILITY CORP., KEY COMPLIANCE TRENDS (Jan. 8, 2012), http://www.nerc.com/files/BOTCC-%20Key%20Compliance%20Trends-%20January%202%202013%20-Mike%20Farzaneh%20reviewed.pdf.

[52] 16 U.S.C. § 824o(b)(1) (requiring "users, owners, and operators of the bulk-power system" to comply with Reliability Standards).

[53] *Mandatory Reliability Standards for the Bulk-Power System*, Order No. 693, 118 FERC ¶ 61,218, at P 76 (2007), *order or reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

[54] *Id.* at P 75.

[55] *See* N. AM. ELEC. RELIABILITY CORP., APPENDIX 5B - STATEMENT OF COMPLIANCE REGISTRY CRITERIA 5 (Jan. 31, 2012), *available at* http://www.nerc.com/files/Appendix_5B_RegistrationCriteria_20120131.pdf.

[56] *Id.*

[57] 16 U.S.C. § 824o(i)(1).

[58] *See Revisions to Electric Reliability Organization Definition of Bulk Electric System and Rules of Procedure*, Order No. 773, 141 FERC ¶ 61,236 (2012).

[59] 16 U.S.C. § 824o(a)(3).

"instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance."[60] Load loss can occur while still meeting this level of reliability.

Because of these limitations, the critical infrastructure identified by DHS under the Executive Order will likely encompass a broader array of assets than are currently protected by the CIP Reliability Standards, particularly those assets used only to serve load. For example, because of statutory limitations, distribution facilities providing power to critical facilities such as hospitals, military installations, government facilities, prisons, and the like are not covered by the CIP Reliability Standards and therefore receive no mandatory protection even though the provision of power to these end users is critical to health, safety, and national security. Because the DHS process may focus on the effects of the loss of critical infrastructure on these vital national interests rather than the voltage level of the relevant facilities, it could capture facilities that have historically escaped CIP regulation, thereby broadening the assets electric utilities must protect.

5. New CIP Reliability Standards

As stated earlier, another possible result of the Executive Order is the development of new or revised CIP Reliability Standards following the development of the Cybersecurity Framework. Although the security recommendations in the Cybersecurity Framework are still a work in progress, it is unlikely that the final Cybersecurity Framework due in one year will precisely match the contours of the existing CIP Reliability Standards. As a result, FERC will be faced with addressing the differences between the NIST Framework and the existing Standards and making a determination on how to address that difference. The recent creation of a FERC Office of Energy Infrastructure Security ("OEIS") suggests that FERC will not be idle, even if, as an independent agency, it is not bound by the Executive Order. OEIS was created, in part, to work with the owners and operators of energy infrastructure to identify and mitigate cyber threats and to develop recommendations for responding to those threats.[61] Given this objective, FERC is likely to seek, as the Executive Order directs, to "establish requirements based upon the Cybersecurity Framework."[62]

Although FERC's final response will not be apparent until the Cybersecurity Framework is final, FERC undoubtedly has the existing regulatory authority to mandate the implementation of the Cybersecurity Framework for the bulk-power system because it can direct NERC to develop Reliability Standards to address specific matters identified by FERC.[63] In the past, FERC has not shied away from using this authority,[64] and it may well direct NERC to develop Reliability Standards to address any gaps between the NIST Framework and the CIP Standards identified by FERC. Indeed, consistent with its past practice, FERC may also recommend to NERC how it should address those gaps.[65] NERC is entitled to use its own technical expertise, and could provide alternatives addressing the directive that differ from FERC's recommendations, but, in the end, NERC will respond to FERC's directive and propose new or revised CIP Reliability Standards consistent with the Framework.

---

[60] 16 U.S.C. § 824o(a)(4).
[61] Press Release, Fed. Energy Regulatory Comm'n, New FERC Office to Focus on Cyber Security (Sep. 20, 2012), http://www.ferc.gov/EventCalendar/Files/20120920100740-OEIS-News-Release.pdf.
[62] Exec. Order § 10(a).
[63] 16 U.S.C. § 824o(d)(5).
[64] On March 18, 2010, FERC issued several reliability orders directing NERC to revise Reliability Standards in a manner consistent with highly specific directives. *See, e.g.*, *Transmission Relay Loadability Reliability Standard*, Order No. 733, 130 FERC ¶ 61,221 (2010), *order on reh'g and clarification*, Order No. 733-A, 134 FERC ¶ 61,127 (2011); *clarified*, Order No. 733-B, 136 FERC ¶ 61,185 (2011).
[65] *See, e.g., Reliability Standards for Geomagnetic Disturbances*, Notice of Proposed Rulemaking, 141 FERC ¶ 61,045 (2012).

6. Conclusion

The Executive Order's implementation for the electric industry remains a work in progress, but a work that will be largely completed over the next year. Although its final implementation will likely address new facilities not covered by existing cybersecurity regulation and may very well lead to increased regulation through CIP Reliability Standards, the process for developing the Cybersecurity Framework and identifying the critical infrastructure to be protected under that Framework presents a remarkable opportunity for the industry. Only the electric industry has an extensive experience with cybersecurity regulation, including what works, what inefficiencies to avoid, and how worthwhile security improvements can be achieved in a cost-effective manner. That puts the electric industry in a leadership position on this issue, with experience that can be leveraged to the benefit of all of the sectors of critical infrastructure that will be subject to the Cybersecurity Framework.

Constant involvement in the consultative process directed by the Executive Order, including engagement with NIST, DOE, FERC, NERC, and other stakeholders, will allow the electric industry to shape both a superior Framework and the likely effects of that Framework on the industry itself so that, a year from now, the electric infrastructure owners and operators can say that, "in the face of real threats to our security and our economy" as President Obama so aptly noted, they did far more than nothing—they contributed to an approach to infrastructure cybersecurity that provides more security more efficiently than would otherwise have resulted from this process.