Federal Cyber-Security Law and Policy: The Role of the Federal Energy Regulatory Commission

A Paper Prepared for the 2014 Law + Informatics Symposium On Cyber Defense Strategies and Responsibilities for Industry

By Susan J. Court
Principal
SJC Energy Consultants, LLC
Former Director of the Office of Enforcement
Federal Energy Regulatory Commission

February 7, 2014

Introduction

The Federal Energy Regulatory Commission (FERC or Commission) is the only Federal agency that sets standards governing cyber-security for the electric utility industry, including investor owned and publicly owned utilities, and enforces those standards by fining entities, even other Federal agencies, which violate them. Other Federal agencies can address and even penalize companies and individuals for breaches of cyber-security rules, directives, or protocols, but none of them specifies upfront, the way FERC does, how to protect against a cyber-security event on the nation's electric grid. Accordingly, this paper will examine the role that the Commission plays in the Federal government's involvement in cyber-security law and policy. It will first review the background to the Commission's responsibility, then discuss relevant FERC rules and policies, and conclude with an overview of the agency's efforts to enforce those rules and policies and the prospect for an expansion of the Commission's authority.

Background

The Federal Energy Regulatory Commission regulates important aspects of interstate energy transactions, and administers, *inter alia*, the Interstate Commerce Act (with respect to interstate oil pipeline transportation), the Federal Power Act (with respect to the interstate transmission and wholesale sales of electric energy, and the construction of hydroelectric projects), and the Natural Gas Act and the Natural Gas Policy Act (with respect to the interstate transportation and wholesale sales of natural gas and the construction of natural gas and liquefied natural gas facilities).[1] Traditionally, until 2005, the Commission primarily regulated investor-owned companies that provide service to other companies. In 2005, Congress greatly expanded the Commission's authority by enacting the Energy Policy Act (EPAct).[2] As relevant here, EPAct directed FERC to establish a program to ensure the reliability of the U.S. "Bulk-Power System"

[1] *See generally* Interstate Commerce Act, 49 App. U.S.C. §§ 1 *et seq*.; Federal Power Act, 16 U.S.C. §§ 791-828c; Natural Gas Act, 15 U.S.C. §§ 717-717z; Natural Gas Policy Act, 15 U.S.C. §§ 3301-3432.
[2] Energy Policy Act of 2005, Pub. L. No. 109-58, 119 Stat. 594 (2005).

(*i.e.*, the nation's electric grid) by setting standards to apply to the users, owners, and operators of that system.[3] This direction increased the number of entities subject to FERC's Federal Power Act electric jurisdiction from approximately 200 investor-owned electric utilities to over 1,500 organizations, including municipal utilities, Federal power administrations, electric cooperatives, and even the Tennessee Valley Authority and the U.S. Army Corps of Engineers. EPAct also made violations of those standards subject to hefty penalties that could be as high as $1 million a day for the duration of the violations, thereby making FERC an enforcement agency as well as an economic regulator.[4]

The impetus for EPAct's reliability provisions was the massive blackout of the North American electric grid that occurred in August 2003. At the time, it was the second largest blackout in history, affecting an estimated 50 million people.[5] A subsequently prepared report issued jointly by the United States and Canada described the blackout and its impact as follows:

> On August 14, 2003, large portions of the Midwest and Northeast United States and Ontario, Canada, experienced an electric power blackout. The outage affected an area with an estimated 50 million people and 61,800 megawatts (MW) of electric load in the states of Ohio, Michigan, Pennsylvania, New York, Vermont, Massachusetts, Connecticut, New Jersey, and the Canadian province of Ontario. The blackout began a few minutes after 4:00 pm Eastern Daylight Time (16:00 EDT), and power was not restored for 4 days in some parts of the United States. Parts of Ontario suffered rolling blackouts for more than a week before full power was restored. Estimates of total costs in the United States range between $4 billion and $10 billion (U.S. dollars). In Canada, gross domestic product was down 0.7% in August, there was a net loss of 18.9 million work hours, and manufacturing shipments in Ontario were down $2.3 billion (Canadian dollars). [[6]]

The extent of the blackout, hours after it began, can be seen on this satellite picture:

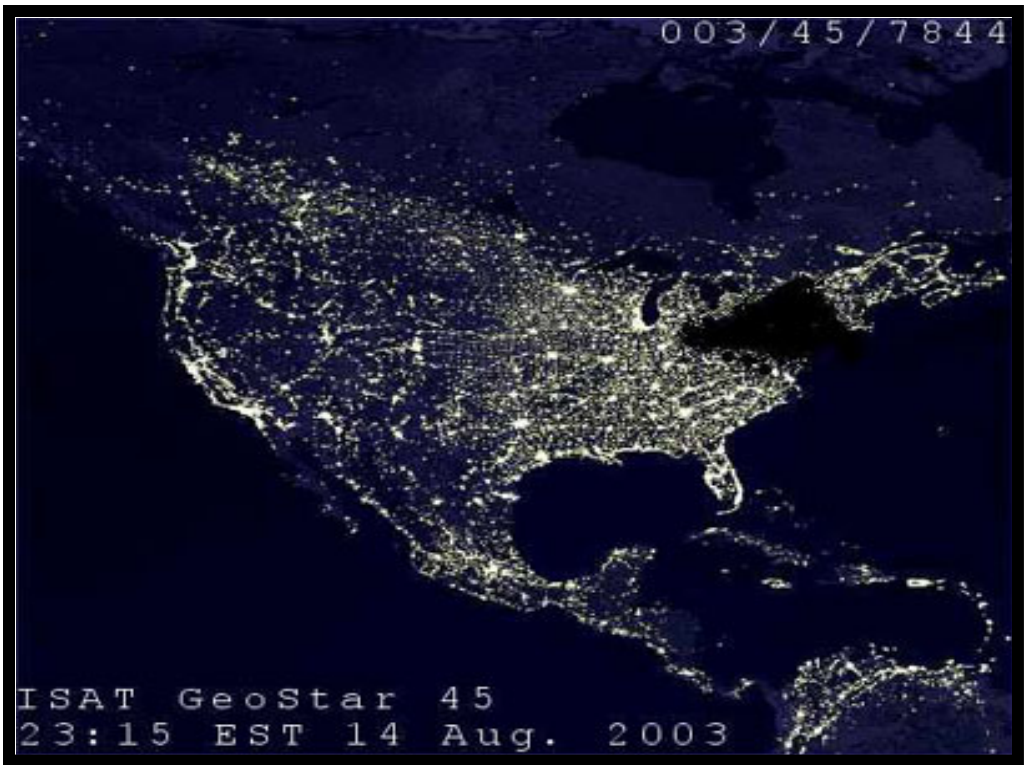
---

[3] *See* Section 1211 of the Energy Policy Act of 2005, Pub. L. No. 109-58, 119 Stat. 594 (2005), *codified at* 16 U.S.C. 824o.

[4] *See* Section 1284 (e) of the Energy Policy Act of 2005, Pub. L. No. 109-58, 119 Stat. 594 (2005), *codified at* 16 U.S.C. 825o-1.

[5] Previously, in 1999, Brazil experienced a larger blackout, affecting an estimated 97 million people. Since 2003, there have been larger blackouts but not in the United States. Brazil and Paraguay experienced a blackout in 2009, affecting 87 million; Java and Bali experienced a blackout in 2005, affecting 100 million people; and India experienced a blackout in 2012, affecting 670 million people.

[6] U.S.-Canada Power System Outage Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada, Causes and Recommendations (April 2004) (Blackout Report), at p. 1 (footnotes omitted).



The Blackout Report also analyzed in great detail the causes of the blackout and made many recommendations. In general, the report found that the blackout was caused by "deficiencies in specific practices, equipment, and human decisions by various organizations that affected conditions and outcomes—for example, insufficient reactive power was an issue in the blackout, but it was not a cause in itself. Rather, deficiencies in corporate policies, lack of adherence to industry policies, and inadequate management of reactive power and voltage caused the blackout, rather than the lack of reactive power."[7] While the origin of the blackout is commonly thought to have been a tree touching a power line of a Cleveland utility (First Energy), the report identified several specific causes, including the utility's failure to assess and understand the inadequacies of its system, operate its system with appropriate voltage criteria, recognize or understand the deteriorating condition of its system, and manage adequately tree growth in its transmission rights-of-way, as well as the failure of the interconnected grid's reliability organizations to provide effective real-time diagnostic support.[8]

[7] Blackout Report, at p. 18. By way of background, a "generator typically produces some mixture of "real" and "reactive" power, and the balance between them can be adjusted at short notice to meet changing conditions. Real power, measured in watts, is the form of electricity that powers equipment. Reactive power, a characteristic of AC systems, is measured in volt-amperes reactive (VAr), and is the energy supplied to create or be stored in electric or magnetic fields in and around electrical equipment. Reactive power is particularly important for equipment that relies on magnetic fields for the production of induced electric currents (e.g., motors, transformers, pumps, and air conditioning.) Transmission lines both consume and produce reactive power." *Id.* at 8.

[8] *Id.*

The Blackout Report also specifically criticized the existing voluntary organization of electric utilities that oversaw the reliability of the electric grid not because it was "an inadequate or ineffective organization, but rather because it ha[d] no structural independence from the industry it represent[ed] and ha[d] no authority to develop strong reliability standards and to enforce compliance with those standards."[9] Accordingly, the report strongly recommended that Federal legislation be enacted to make that happen.[10]

Congress agreed with the Blackout Report, and, less than two years later, enacted EPAct, which, *inter alia*, added a new section 215 to the Federal Power Act (FPA) to provide for a system of mandatory, enforceable Reliability Standards.[11] Briefly, FPA section 215 required the Commission to certify a single Electric Reliability Organization (ERO) to oversee the reliability of the United States' portion of the interconnected North American Bulk-Power System, subject to Commission oversight, and authorized the Commission to approve all ERO actions and, as appropriate, to independently enforce the Reliability Standards.[12] FPA section 215 provided that the ERO would be responsible for developing and enforcing the mandatory Reliability Standards that would apply to all users, owners and operators of the Bulk-Power System, and submit each proposed Reliability Standard to the Commission for approval. The ERO was permitted to delegate its enforcement responsibilities to Regional Entities, subject to the Commission's approval. The ERO or the Regional Entities would then be responsible for monitoring compliance with the Reliability Standards, could direct a user, owner or operator of the Bulk-Power System that violates Reliability Standard to comply with the Reliability Standard, and impose a penalty on a user, owner or operator for violating a Reliability Standard, subject to review by, and appeal to, the Commission.

In the years following the enactment of EPAct, the Commission issued a series of orders that implemented FPA section 215. Four orders issued in 2006 and 2007, in particular, established the Federal, mandatory reliability program for the nation's electric grid.

---

[9] *Id.* at 21.

[10] *Id.*

[11] *See supra* note 3.

[12] FPA section 215 describes the "bulk-power system" as including the facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof), and electric energy from generation facilities needed to maintain transmission system reliability. The term does not include facilities used in the local distribution of electric energy. FERC uses the term "bulk electric system" (BES) for the applicability of the standards, and defines the term generally as the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher. Radial transmission facilities serving only load with one transmission sources are generally not included in this definition. See *Revisions to Electric Reliability Organization Definition of Bulk Electric System and Rules of Procedure*, Order No. 773, 141 F.E.R.C. ¶ 61,236 (2012), *order on reh'g and clarification*, Order No. 773-A, 143 F.E.R.C. ¶ 61,053 (2013), *order on reh'g and clarification*, 144 F.E.R.C. ¶ 61,174 (2013). On June 6, 2013, the Commission extended the effective date of the new definition, until July 1, 2014. *See Revisions to Electric Reliability Organization Definition of Bulk Electric System and Rules of Procedure,* Order Granting Extension of Time, 143 F.E.R.C. ¶ 61,231 (2013).

- On February 3, 2006, the Commission issued Order No. 672, which promulgated regulations, codified in Part 39 of Title 18 of the Code of Federal Regulations, that established the criteria that an entity must satisfy to qualify to be the ERO, procedures under which the ERO may propose new or modified Reliability Standards for Commission review, principles pertaining to the funding of the ERO, procedures governing an enforcement action by the ERO, a Regional Entity, or the Commission, and criteria under which the ERO may enter into an agreement to delegate authority to a Regional Entity for the purpose of proposing Reliability Standards to the ERO and enforcing those standards.[13]

- On July 20, 2006, the Commission issued an order that certified the North American Electric Reliability Corporation (NERC) as the ERO.[14]

- On March 16, 2007, the Commission issued Order No. 693, in which it approved 83 of 107 proposed Reliability Standards developed by NERC, to become effective June 18, 2007.[15] Order No. 693 also added a new Part 40 to the Commission's regulations, 18 C.F.R. Part 40, which stated that the standards applied to all users, owners, and operators of the Bulk-Power System within the United States (other than Alaska and Hawaii) and required that each Reliability Standard identify the subset of users, owners, and operators to which that particular Reliability Standard applies. The new regulations also required that each Reliability Standard approved by the Commission would be maintained on the ERO's Internet website.

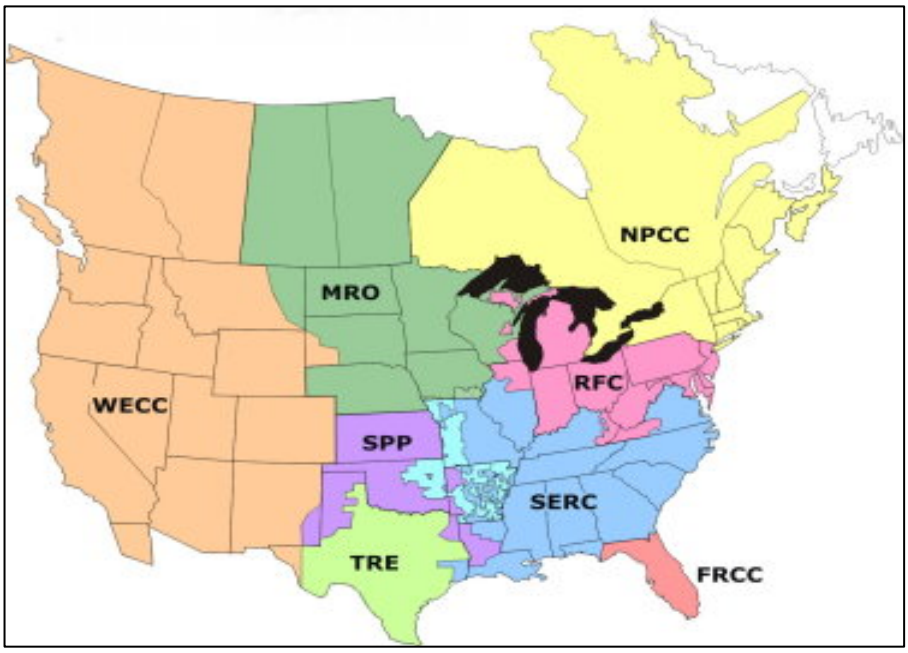
- On April 19, 2007, the Commission issued an order accepting the ERO's agreements with eight Regional Entities and approving those entities' 2007 business plans.[16] As depicted below, the eight Regional Entities are Florida Reliability Coordination Council, Midwest Reliability Organization, Northeast Power Coordinating Council, ReliabilityFirst Corporation, SERC Reliability Corporation, Southwest Power Pool, RE, Texas Reliability Entity, and Western Electricity Coordinating Council.

[13] *Rules Concerning Certification of the Electric Reliability Organization, and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, F.E.R.C. Stats. & Regs. ¶ 31,204, *order on reh'g*, Order No. 682-A, F.E.R.C. Stats. & Regs. ¶ 31,212 (2006).

[14] *North Am. Elec. Reliability Corp.*, 116 F.E.R.C. ¶ 61,062, *order on reh'g and compliance*, 117 F.E.R.C. ¶ 61,126 (2006), *aff'd sub nom. Alcoa, Inc. v. F.E.R.C.*, 564 F.3d 1342 (D.C. Cir. 2009).

[15] *Mandatory Reliability Standards for the Bulk-Power System*, Order No. 693, F.E.R.C. Stats. & Regs. ¶ 31,242, *order on reh'g*, Order No. 693-A, 120 F.E.R.C. ¶ 61,053 (2007).

[16] *North Am. Elec. Reliability Corp., et al*., Order Accepting ERO Compliance Filing, Accepting ERP/Regional Entity Delegation Agreements, and Accepting Regional Entity 2007 Business Plans, 119 F.E.R.C. ¶ 61,060 (2007), *order on compliance filing*, 122 F.E.R.C. ¶ 61,245, *order on compliance filings,* 125 F.E.R.C. ¶ 61,330 (2008).



The April 19 order also approved a Compliance Monitoring and Enforcement Program, which set out the structure and processes to be used by the Regional Entities to enforce the mandatory Reliability Standards.

By way of further background, Order No. 693 identified 14 categories of Mandatory Reliability Standards, including cyber-security standards referred to as Critical Infrastructure Protection (CIP) standards.[17] The other 13 categories are: Resource and Demand Balancing (BAL), Communications (COM), Emergency Preparedness and Operations (EOP), Facilities Design, Connections, and Maintenance (FAC), Interchange Scheduling and Coordination (INT), Interconnection Reliability Operations and Coordination (IRO), Modeling, Data and Analysis (MOD), Nuclear (NUC), Personnel Performance, Training and Qualifications (PER), Protection and Control (PRC), Transmission Operations (TOP), Transmission Planning (TPL), Voltage and Reactive (VAR). The standards apply to the users, owners, and operators of the Bulk-Power System, who are registered by NERC according to the function they perform within that system (and hence are called Registered Entities). Those functions include: Balancing Authority, Distribution Provider, Generator Owner, Generator Operator, Interchange Authority, Load Serving Entity, Planning Authority, Purchasing Selling Entity, Reliability Coordinator, Resource Planner, Reserve Sharing Group, Transmission Owner, Transmission Operator, Transmission Planner, and Transmission Service Provider.

Since the enactment of EPAct, the Commission has approved over 100 mandatory Reliability Standards, which in turn include over 1,000 separate requirements, and NERC has registered 1,646 users, owners, and operators for a total of 4,782 functions.[18]

[17] As defined by NERC for the purposes of the CIP standards, critical infrastructure includes facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.

[18] A complete set of the mandatory Reliability Standards can be found at http://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.pdf (last accessed on October 30, 2013). An overview of registered entities and functions, by region, can be

Critical Infrastructure Protection (CIP) Standards

To date, the Commission has approved 11 CIP mandatory Reliability Standards; however, there have been several versions of these standards in effect since April 2007. Currently, the third version is the law, and will be replaced by the fifth version to be effective in April 2016.[19] The Commission approved the first CIP standard—CIP-001-1 (Sabotage Reporting)—in Order No. 693. As explained there,

> The goal of this standard is to ensure that operating entities recognize sabotage events and inform appropriate authorities and each other to properly respond to the sabotage to minimize the impact on the Bulk-Power System. The Reliability Standard requires that each reliability coordinator, balancing authority, transmission operator, generation operator and load serving entity have procedure for recognizing and for making operating personnel aware of sabotage events, and communicating information concerning sabotage events to appropriate "parties" in the Interconnect.[[20]]

CIP-001-1 became effective on April 7, 2007.[21] Nine months later, on January 18, 2008, the Commission approved eight additional CIP standards in Order No. 706.[22] Subsequently, the Commission approved Version 2 and Version 3 (CIP V3) of these standards, which became effective on April 1, 2010 and October 1, 2010, respectively.[23] The Commission also approved a fourth version, on April 19, 2012, in Order No. 761, but delayed the effectiveness of this version until October 1, 2014, a time by which Version 5 (CIP V5) (discussed in greater detail below) would most likely make compliance with Version 4 unnecessary.[24] In fact, in the order in which

---

found at http://www.nerc.com/pa/comp/Registration%20and%20Certification%20DL/NERC_Compliance_Registry_Matrix_Summary20130930.pdf (last accessed on October 28, 2013). Some of the Registered Entities are Canadian utilities, which are not subject to FERC jurisdiction but rather Canadian Provincial oversight.

[19] CIP standards to protect cyber assets with low impact potential will become effective one year later, in April 2017.

[20] Order No. 693, at P 445. (The capital "P" in FERC citations refers to paragraph numbers, not page numbers.)

[21] CIP-001 was later integrated into EOP-004-2 — Event Reporting. *See North American Electric Reliability Corporation*, 143 FERC ¶ 61,252 (2013).

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

[23] *See North Am. Elec. Reliability Corp.*, 128 F.E.R.C. ¶ 61,291, *order on reh'g*, 129 F.E.R.C. ¶ 61,236 (2009) (approving Version 2); *North American Electric Reliability Corp*., 130 F.E.R.C. ¶ 61,271 (2010) (approving Version 3).

[24] *See Version 4 Critical Infrastructure Protection Reliability Standards*, Order No. 761, 129 F.E.R.C. ¶ 61,058, *order on reh'g,* 140 F.E.R.C. ¶ 61,109 (2012*); Version 4 Critical Infrastructure Protection Reliability Standards; Version 5 Critical Infrastructure Protection Reliability Standards*, *Order Granting Extension of Time*, 144 F.E.R.C. ¶ 61,123 (2013).

the Commission approved CIP V5, the Commission expressly rescinded the fourth version of the CIP standards.[25]

In all versions of the CIP standards, the threshold issue is what assets are subject to the requirements. This issue is addressed primarily in CIP-002, which deals with the identification of **critical cyber assets**. For the purpose of CIP V3, which is the law until April 2016, the analysis involves the definitions of four terms, the first of which is statutory: (1) "reliable operation," which means "operating the elements of the Bulk-Power System within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation or cascading failures of such system will not occur as a result of a sudden disturbance, including a cyber security incident, or unanticipated failure of system elements,"[26] (2) "critical assets," which are "facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System," (3) "cyber assets," which are "programmable electronic devices and communication networks including hardware, software, and data," and finally (4) "**critical cyber assets**," which are "cyber assets essential to the reliable operation of critical assets." Accordingly, as the Commission has consistently held, the accurate identification of critical assets and critical cyber assets is the cornerstone of the CIP Reliability Standards, because "it acts as a filter, determining whether a responsible entity must comply with the remaining CIP requirements in CIP-003-1 through CIP-009-1."[27]

Against this backdrop, the eight CIP Reliability Standards approved in Order No. 706 are:[28]

- **CIP-002-1–Cyber Security–Critical Cyber Asset Identification**, which requires a responsible entity to identify its critical assets and critical cyber assets using a risk-based assessment methodology.[29]

- **CIP-003-1–Cyber Security–Security Management Controls**, which requires a responsible entity to develop and implement security management controls to protect critical cyber assets identified in CIP-002-1.

- **CIP-004-1–Cyber Security–Personnel and Training**, which requires personnel with access to critical cyber assets to have identity verification, a criminal check, and employee training.

- **CIP-005-1–Cyber Security–Electronic Security Perimeters**, which requires the identification and protection of an electronic security perimeter and access points, where

[25] *See Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 145 F.E.R.C. ¶ 61,160 (2013) (Order No. 791), *reh'g pending*, at P 171.
[26] 16 U.S.C. 824o(a)(4).
[27] Order No. 706, at P 234.
[28] *Id*. at P 6.
[29] A "responsible entity" is a Registered Entity subject to the CIP mandatory standards. Not all Registered Entities are responsible entities as not all Registered Entities are subject to the CIP mandatory standards.

the perimeter is to encompass the critical cyber assets identified by the methodology required in CIP-002-1.

- **CIP-006-1–Cyber Security–Physical Security of Critical Cyber Assets**, which requires a responsible entity to create and maintain a physical security plan that ensures that all cyber assets within an electronic security perimeter are kept in an identified physical security perimeter.

- **CIP-007-1–Cyber Security–Systems Security Management**, which requires a responsible entity to define methods, processes, and procedures for securing the systems identified as critical cyber assets, as well as the non-critical cyber assets within an electronic security perimeter.

- **CIP-008-1–Cyber Security–Incident Reporting and Response Planning**, which requires a responsible entity to identify, classify, respond to, and report cyber security incidents related to critical cyber assets.

- **CIP-009-1– Cyber Security–Recovery Plans for Critical Cyber Assets**, which requires the establishment of recovery plans for critical cyber assets using established business continuity and disaster recovery techniques and practices.

NERC described these standards as providing,

> A comprehensive set of requirements to protect the Bulk-Power System from malicious cyber-attacks. They require Bulk-Power users, owners, and operators to establish a risk-based vulnerability assessment methodology to identify and prioritize critical asset and critical cyber assets. Once the critical cyber assets are identified, the CIP Reliability Standards, require, among other things, that the responsible parties establish plans, protocols, and controls to safeguard physical and electronic access, to train personnel on security matters, to report security incidents, and to be prepared for recovery actions.[30]

FERC also approved NERC's implementation plan that provided for a three-year phase-in to achieve full compliance with all of the requirements in order to give responsible entities enough time to purchase and install new cyber software and equipment and develop new programs and procedures to achieve compliance.[31] Furthermore, recognizing the challenges presented by the new CIP standards, the Commission allowed responsible entities to seek exceptions from coverage of those standards, especially with respect to long-life equipment in place that is not readily compatible with a modern environment where cyber security issues are a concern.[32]

---

[30] Order No. 706, at P 7.

[31] *Id.* P at 86.

[32] *Id.* P at 180. *See also North Am. Elec. Reliability Corp.*, Order Approving Technical Feasibility Exception Procedures and Ordering Compliance Filing, 130 F.E.R.C. ¶ 61,050 (2010); *North Am. Elec. Reliability Corp.,* Order Approving Revisions to Electric Reliability Organization's Rules of Procedure and Directing Compliance Filing, 144 F.E.R.C. ¶ 61,180 (2013).

As noted, the next version of the mandatory CIP Reliability Standards—CIP V5—is on the horizon.[33] On November 22, 2013, the Commission approved a final rule—Order No. 791—that modified CIP-002-3 through CIP-009-3 and added two new standards, CIP-010-1 and CIP-011-1. Generally, the Commission agreed with NERC's proposal, finding that it represented an improvement over the currently effective standards because it includes new cyber security controls and extends the scope of the systems that are protected by the standards.[34]

Briefly, the CIP V5 standards to be effective in April 2016 are:[35]

- **CIP-002-5–Cyber Security–BES Cyber System Categorization** redefines a BES Cyber Asset that "if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System," and defines a BES Cyber System as "one or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity." [36] This standard also requires a Registered Entity to classify its facilities into three categories of BES Cyber Systems. High Impact covers large Control Centers, Medium Impact covers generation and transmission facilities, and Low Impact covers all other BES Cyber Systems. Importantly, once a responsible entity identifies a BES Cyber System under CIP-002-5, it would be required to comply with the controls included in the remaining standards.

- **CIP-003-5–Cyber Security–Security Management Controls** requires approval by a CIP Senior Manager of the documented cyber security policies related to the remaining standards. It also requires implementation of policies related to cyber security awareness, physical security controls, electronic access controls, and incident response to a Cyber Security Incident for those assets that have Low Impact BES Cyber Systems under CIP-002-5 categorization process.

- **CIP-004-5–Cyber Security–Personnel and Training** requires documented processes or programs for security awareness, cyber security training, personnel risk assessment, and access management. Specific requirements include training for visitor control programs, electronic interconnectivity supporting the operation and control of BES Cyber Systems, storage media as part of the treatment of BES Cyber Systems Information, and a seven year criminal history check covering all locations where the individual has resided for six consecutive months.

- **CIP-005-5–Cyber Security–Electronic Security Perimeters** focuses on the discrete Electronic Access Points rather than the logical "perimeter," which is the focus of the currently effective standard.

[33] *See supra* note 25.
[34] Order No. 791 at P 1.
[35] *Id.* at PP 19-33.
[36] *Id.* at P 21.

- **CIP-006-5–Cyber Security–Physical Security of BES Cyber Systems** is intended to manage physical access to BES Cyber Systems by specifying a physical security plan to protect BES Cyber Systems against compromise that could lead to misoperation or instability.

- **CIP-007-5–Cyber Security–Systems Security Management** addresses system security by specifying technical operations, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability of the bulk electric system. For example, among other things, the responsible entity will be required to document how it addresses the malware risk for each BES Cyber System, but not be required to prescribe a particular technical method in order to account for potential technological advancement.

- **CIP-008-5–Cyber Security–Incident Reporting and Response Planning** mitigates the risk to the reliability operation of the bulk electric system resulting from a Cyber Security Incident by specifying incident response requirements. For example, responsible entities will be required to report Cyber Security Incidents within one hour of recognition, to verify response plan effectiveness and consistent application in responding to a Cyber Security Incident, and provide for an after-action review for tests or actual incidents, and an update to the Cyber Security Incident response plan based on those lessons learned.

- **CIP-009-5–Cyber Security–Recovery Plans for BES Cyber Systems** provides for the recovery of the reliability functions performed by BES Cyber Systems by specifying a recovery plan to support the continued stability, operability, and reliability of the bulk electric system. For example, a responsible entity must have controls to protect data that would be useful in the investigation of an event that results in the execution of a Cyber System recovery plan.

- **CIP-010-1–Cyber Security–Configuration Change Management and Vulnerability Assessments** specifies configuration change management requirements to detect unauthorized modifications to BES Cyber Systems and to ensure proper implementation of cyber security controls while promoting continuous improvement of a responsible entity's cyber security posture.

- **CIP-011-1–Cyber Security–Information Protection** specifies information protection controls to prevent unauthorized access to BES Cyber System Information and reuse and disposal provisions to prevent unauthorized dissemination of protected information.

While the Commission generally approved the CIP V5 standards as proposed by NERC, the Commission also directed NERC to provide more information on certain requirements to support their continued inclusion in the standards. For example, even though the Commission approved the revised definition of BES Cyber Asset in CIP-002-5, it directed NERC to conduct a survey of Cyber Assets that are included or excluded under the new BES Cyber Asset definition during the implementation periods, to gain a better understanding of the BES Cyber Asset definition.[37]

[37] *Id.* at P 124.

Based on that data, FERC told NERC to explain in an informational filing: (1) specific ways in which entities determine which Cyber Assets meet the 15 minute parameter; (2) types or functions of Cyber Assets that are excluded from being designated as BES Cyber Assets and the rationale as to why; (3) common problem areas with entities improperly designating BES Cyber Assets; and (4) feedback from each region participating in the implementation study on lessons learned with the application of BES Cyber Asset definition.[38]

Finally, with respect to the CIP V5, NERC, the Regional Entities, and the responsible entities have been engaged since early 2013 in efforts to transition to the new standards. Each group has dedicated staff to meet three objectives through outreach and training:

- To improve industry understanding of the technical security challenges that must be addressed in order to comply with CIP V5 standards, especially understanding the material differences between Version 3 and Version 5;

- To ensure that industry understands what will be expected of its members to comply with the new standards, including what evidence they must retain to demonstrate compliance; and

- To understand what technical and compliance related resources and efforts are needed to transition and manage compliance with CIP V5 standards.[39]

Enforcement of Mandatory CIP Reliability Standards

As mentioned earlier, the Regional Entities use the framework called the Compliance Monitoring and Enforcement Program, approved by the Commission in 2007, to ensure compliance by the Registered Entities with the mandatory Reliability Standards.[40] They use numerous tools to that end, including conducting audits and spot checks, reviewing self-certifications (of compliance) and self-reports, and pursuing complaints and investigations of alleged violations. Since the standards first became effective in June 2007, the ERO Enterprise has processed thousands of violations and collected millions of dollars in fines.[41] As relevant here, since they became effective, the CIP Reliability Standards have consistently accounted for the majority of the violations processed by the Regional Entities, and submitted to the Commission through NERC. For example, in the third quarter of 2013, the top ten violated standards, which closely followed

[38] *Id*.
[39] *See* Agenda Item 3 of Compliance Committee Meeting Agenda (Nov. 6, 2013), available at http://www.nerc.com/gov/bot/BOTCC/Compliance%20Committee%202013/BOTCC_11-13a_Complete.pdf.
[40] *See supra* note 16.
[41] See http://www.nerc.com/pa/comp/Pages/Enforcement-and-Mitigation.aspx (last accessed on October 30, 2013).

the trend for the previous four quarters, were CIP-007, CIP-006, CIP-005, PRC-005, CIP-004, CIP-002, CIP-003, VAR-002, CIP-009, and FAC-009.[42]

There are two reasons in particular for the high incidence of CIP violations. The CIP standards—indeed, even the concept of CIP standards—are relatively new. While many of the other standards were in place, albeit on a voluntary basis, for many years before the enactment of EPAct in 2005, the CIP standards were only developed in the past few years as the technology became more sophisticated and the need to secure cyber assets became more apparent. As a consequence, the responsible entities have less experience in complying with the CIP standards than they have with the other standards. Also, NERC and the Regional Entities have focused their compliance and enforcement resources and efforts on the CIP standards as they became more aware of the critical need for heightened cyber security. To this end, for example, the Regional Entities have increased their staffs and made a concerted effort to hire auditors and enforcement personnel with relevant technical experience.[43]

Once a Regional Entity has confirmed a violation of a standard, and, assuming the Registered Entity does not object to or settles with the Regional Entity on a remedy, the Regional Entity submits the case to NERC's Board of Trustees. If the Board agrees with the Region's resolution of the matter, the NERC staff submits the case to the FERC in a filing called a Notice of Penalty (NOP). FERC assigns the case a docket number, starting with the letters "NP." The notice becomes final after 30 days, unless the Commission "tolls" the time for acting on the matter. With few exceptions, the Commission has allowed NERC's NOPs, including those involving CIP violations, to become effective by operation of law, *i.e.*, by not taking further action on the submission, since the original 37 NOPs were filed in June 2008.[44] As a consequence, there is very little FERC action that would be considered "FERC case law," and there is no court decision on the enforcement of the Reliability Standards. For members of the electric utility industry and the public in general, the only insight into what constitutes a violation, at least in the

---

[42] *See* Agenda Item 4 of Compliance Committee Meeting Agenda (Nov. 6, 2013), at Slide 18, available at http://www.nerc.com/gov/bot/BOTCC/Compliance%20Committee%202013/BOTCC_11-13a_Complete.pdf.

[43] Most of the Regional Entities also participated in the NERC Grid Security Exercises ("GridEx"), on November 16-17, 2011, and November 13-14, 2013. GridEx is a biennial international grid security exercise that uses best practices from the Department of Homeland Security, the Federal Emergency Management Agency, and the National Institute of Standards and Technology. The 2011 GridEx exercise, for example, was designed to validate the readiness of the Electricity Sub-sector to respond to a cyber-security incident, strengthen Registered Entities' crisis response functions, and provide input for internal security program improvements. Overall, the exercise was widely regarded across industry and government as a critical imperative in preparing the bulk-power system for a disruptive cyber event. See generally *2011 NERC Grid Security Exercise*, After Action Report (March 2012), at http://www.nerc.com/pa/CI/CIPOutreach/Documents/NERC%20GridEx%20AAR%2016Mar2012%20Final.pdf.

[44] *See Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards,* Statement of Administrative Policy on Processing Reliability Notices of Penalty and Order Revising Statement in Order No 672, 123 F.E.R.C. ¶ 61,046 (2008). Through the end of 2013, the Regional Entities submitted approximately 5,000 NOPs regarding confirmed violations of the mandatory reliability standards.

view of the Regional Entities, is found in the records that NERC submits to the FERC in the NOP filings.

Illustratively, on October 31, 2012, NERC filed an NOP, in Docket No. NP13-1-000, which included a settlement between the Western Electric Coordinating Council (WECC) and an Unidentified Registered Entity (URE) resolving WECC's determination and findings of the violations of CIP-002-1, CIP-003-1, CIP-004-1, CIP-005-1, CIP-006, and CIP-007.[45] The URE agreed to the assessed penalty of $200,000. With respect to CIP-002-1, WECC pointed out that the URE had self-reported that during an internal review of compliance with the CIP Standards, and in connection with the commencement of its annual review of Critical Cyber Assets (CCA), the URE discovered that it failed to identify 13 CAAs essential to the operation of its Critical Assets (CAs). The URE had two managers who were responsible for identifying CCA, and also relied on electronic records to identify CCAs and develop lists. However, during its annual review process, the URE discovered its lists of CCAs were insufficient. With respect to the violation of CIP-003-1, the URE self-certified that it was not in compliance. Even though the URE had established and documented a process for change control, the process failed to effectively control changes made to its CCA hardware or software, and the URE lacked a process that explicitly governed managing configuration changes.

On February 28, 2013, NERC filed an NOP, in Docket No. NP13-24-000, which included a settlement between WECC and three URE's arising out of WECC's determination and findings of violations of CIP-006-1, CIP-004-3, CIP-006-1, and CIP-007-2. The URE's agreed to an assessed penalty of $151,500. With respect to CIP-006-1, WECC explained that the URE self-reported that it had failed to provide alarming for five card readers that controlled access to three Physical Security Perimeters (PSPs). Four of the card readers controlled access to the blackstart human machine interface (HIMI) PSP at two of the URE's facilities. The card readers involved were incorrectly configured and failed to send alarms to the central alarm station. In addition, one card reader's air compressor PSP card reader was unplugged from its power source which caused the reader to fail to send an alarm to the central alarm station. With respect to CIP-004, a second URE self-reported that it had failed to update the personnel risk assessment (PRA) for one of its employees. The URE stated that the employee's PRA was valid until it expired in the fall. The URE discovered the expired PRA during a quarterly PRA review, resubmitted the PRA, and approximately a month later completed the PRA for the employee. WECC determined the duration of the violation to be from when the URE should have performed the PRA through when it performed the PRA.

For its part, the Commission has issued seven orders approving settlements with Registered Entities, which FERC enforcement staff alleged had violated the mandatory Reliability Standards.[46] Only one of those cases involved alleged violations of a CIP standard. In 2013,

[45] The Regional Entities routinely do not identify the Registered Entity that has violated the CIP standards, to avoid putting the Registered Entity's facilities in harm's way.

[46] *See Southwest Power Pool, Inc.,* 144 F.E.R.C. ¶ 61,019 (2013), *Entergy Services, Inc.*, 142 F.E.R.C. ¶ 61,241 (2013), *California Independent System Operator Corporation*, 141 F.E.R.C. ¶ 61,209 (2012), *Western Electric Coordination Council*, 136 F.E.R.C. ¶ 61,020 (2011), *PacifiCorp*, 137 FERC ¶ 61,176 (2011*), Florida Blackout (FPCC*), 130 F.E.R.C. ¶ 61,163 (2010), and *Florida Blackout (Florida Power)*, 129 F.E.R.C. ¶ 61,016 (2009). FERC imposed a total of $29,850,000 in penalties on the settling entities.

FERC's enforcement staff entered into a settlement with Entergy Services, Inc., which the staff accused of violating CIP-007-1, because the utility allegedly failed to adequately protect critical infrastructure by neglecting to test a firmware upgrade before applying the upgrade in production mode.[47] FERC fined Entergy $975,000, which covered alleged violations of a total of 27 requirements in 15 standards, not just the violation of the CIP standard, and required Entergy to make semi-annual compliance filings for two years.[48]

Finally, with respect to the enforcement of the mandatory CIP Reliability Standards, the Commission affirmed a penalty of $19,500 against the Southwestern Power Administration (SWPA), one of four power administrations within the U.S. Department of Energy, for violating CIP-004-1 and CIP-007-1 in 2008-2010.[49] The specific violations, which SWPA did not deny, involved the following activities:

- Two of SWPA's employees on its authorized unescorted access list had not received 2008 physical security training within 90 days of being placed on the list.

- Two other employees were placed on its access list and given unescorted physical access to a CAA area without a criminal background check being performed within the past seven years.

- Two SWPA contractors were improperly included in the list of personnel with authorized, unescorted physical access to the CA area.

- SWPA's test program for significant changes to Cyber Assets only verified application functionality and did not verify that existing security controls were not adversely affected. SWPA did not test the proper configuration and operation of the security controls.

Dismissing SWPA and DOE's arguments that the doctrine of sovereign immunity precluded FERC's imposing a penalty on another Federal agency, the Commission found that the plain language of FPA section 215 explicitly conveys authority to FERC to assess a monetary penalty against a federal entity that is a user, owner, or operator of the Bulk-Power System for a violation of a mandatory Reliability Standard.[50] Among other things, the Commission explained that "any exemption of a large class of customers from the imposition of penalties for violations of a mandatory Reliability Standard would undermine NERC's enforcement regime, which is an integral part of ensuring the reliable operation of the Bulk-Power System."[51]

---

[47] *See* 142 F.E.R.C. ¶ 61,241, at P 18.
[48] *Id.* at P 1.
[49] *See North Am. Elec. Reliability Corp.*, 140 F.E.R.C. ¶ 61,048, *order on reh'g*, 141 F.E.R.C. ¶ 61,242 (2012), *appeal pending sub nom. Southwestern Power Administration, et al. v. F.E.R.C.*, No. 13-1033 (D.C. Cir. Mar. 23, 2013).
[50] *Id.* at P 37.
[51] *Id.* at P 55 (footnote omitted).

Possible Cyber Legislation and Executive Order 13636

For several years, Congress has considered various cyber-security bills, some of which would have expanded FERC's authority. Partly, these pieces of legislation have been informed by the U.S. Department of Energy Inspector General's January 2011 audit report on FERC's "Monitoring of Power Grid Cyber Security."[52] This report raised concerns about the adequacy of, and the implementation and schedule for, the CIP standards, and concluded that these problems exist in part because FERC's authority to ensure adequate BES reliability is limited. The audit report then recommended that additional authority be granted to FERC to ensure adequate BES cyber security. FERC staff subsequently testified before Congress, pointing out, among other things, that the standards development process, which takes years and is transparent, is inadequate for the agency to respond timely to a cyber matter, and further is inconsistent with the need to keep security-sensitive information out of the hands of potential adversaries.[53] Accordingly, FERC staff suggested that (1) the Federal government should be able to require mitigation even before or while NERC and its stakeholders develop a standard, when circumstances require urgent action, (2) any legislation should ensure appropriate confidentiality of sensitive information submitted, developed or issued under this authority, (3) Congress should consider extending FERC's reliability authority beyond the current statutory definition which does not authorize Federal action to mitigate cyber or other national security threats to reliability that involve certain critical facilities and major population areas, and (4) it is important that entities be able to recover costs they incur to mitigate vulnerabilities and threats.[54]

With the prospect of legislation remote in the 113th Congress, in February 2013, President Obama issued Executive Order 13636 (Improving Critical Infrastructure Cybersecurity) (EO). The EO's stated aim is to strengthen the cyber security of critical infrastructure by increasing information sharing and by jointly developing and implementing a framework of cyber security practices with the government's industry partners.[55] The EO established new information sharing between the private and public sectors, providing classified and unclassified threat information to U.S. companies. It required federal agencies to produce unclassified reports of threats to U.S. companies and to share the reports in a timely manner. It also opened up a real-time information sharing program, currently open to the defense industry, to other sectors. In addition, the order directed the National Institute of Standards and Technology (NIST), a federal agency, to develop a new cyber security framework to reduce cyber risks to critical infrastructure, and required NIST to publish a preliminary version of the framework within 240 days of the Executive Order and a final version one year after the Executive Order. Finally, it called on agencies to incorporate privacy and civil liberties safeguards, based in part on the Fair

[52] *See* http://www.wired.com/images_blogs/threatlevel/2011/02/DoE-IG-Report-on-Grid-Security.pdf.
[53] See Testimony of Joseph McClelland, Director, FERC Office of Electric Reliability, before the U.S. Senate Committee on Energy and Natural Resources, July 17, 2012, at pp. 4-5, available at http://ferc.gov/EventCalendar/Files/20120717100957-7-17-12-FERC-Testimony.pdf
[54] *Id.* at 7-8.
[55] http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0.

Information Practice Principles, into their cyber security efforts and required agencies to conduct regular, public assessments of their privacy and civil liberties standards.[56]

In response to the EO, the U.S. Department of Homeland Security created the Integrated Task Force, which consists of eight working groups, each focused on specific implementation deliverables. As relevant here, NERC and the electric industry experts represent the Electricity Sub-sector on all active implementation working groups. These groups are:

- Cybersecurity Framework Development Working Group, which works with NIST to develop a voluntary, repeatable cybersecurity framework to promote the protection of critical infrastructure;
- Cyber Dependent Infrastructur4e Identification Work Group, which collaborates with industry and the Department of Energy to identify entities with critical infrastructure that, if faced with a cyber incident, could have catastrophic effects;
- Planning and Evaluation Work Group, which is tasked with updating the National Infrastructure Protection Plan (NIPP) to coordinate public-private efforts to improve infrastructure security and resiliency; and
- Incentives Work Group, which directs the study of incentives for participating in the voluntary critical infrastructure cybersecuirty program.[57]

As an independent agency, FERC is not specifically assigned any responsibilities under the Executive Order. However, shortly before the President issued the Order, on September 20, 2012, the Commission created a new office to focus exclusively on cyber security—the Office of Energy Infrastructure Security (OEIS). As described by the FERC Chairman at that time, "[c]reating this office allows FERC to leverage its existing resources with those of other government agencies and private industry in a coordinated, focused manner. Effective mitigation of cyber and other physical attacks requires rapid interactions among regulators, industry and federal and state agencies."[58] The office has four primary objectives: (1) to develop recommendations for identifying, communicating and mitigating potential cyber and physical security threats and vulnerabilities to FERC-jurisdictional energy facilities using the Commission's existing statutory authority; (2) to provide assistance, expertise and advice to other federal and state agencies, jurisdictional utilities and Congress in identifying, communicating and mitigating potential cyber and physical threats and vulnerabilities to FERC-jurisdictional energy facilities; (3) to participate in interagency and intelligence-related coordination and collaboration efforts with appropriate federal and state agencies and industry representatives on cyber and physical security matters related to FERC-jurisdictional energy facilities; and (4) to conduct outreach with private sector owners, users and operators of energy

[56] See http://www.nerc.com/gov/bot/Board%20of%20Trustees%20Quarterly%20Meetings/BOT_1113a_Complete%20(v2).pdf

[57] See Agenda Item 11c of the Board of Trustees Meeting (Nov. 7, 2013), available at http://www.nerc.com/gov/bot/Board%20of%20Trustees%20Quarterly%20Meetings/11c-EO%20and%20PPD%20Brief.pdf.

[58] http://ferc.gov/media/news-releases/2012/2012-3/09-20-12.asp.

delivery systems regarding identification, communication and mitigation of cyber and physical threats to FERC-jurisdictional energy facilities.[59]

Conclusion

As is true for other areas, protection of the nation's electric grid cyber assets is still in the early stages of development. Unlike other areas, however, this protection is being undertaken within a unique Federally-mandated structure. Congress has charged FERC, an independent regulatory agency, with the responsibility to oversee both the development and the enforcement of standards, which are applicable to over 1,800 entities registered as users, owners, and operators of the Bulk-Power System. FERC fulfills this responsibility by reviewing the actions of NERC and eight Regional Entities, which are required to develop those standards and ensure that the Registered Entities comply with them. NERC is mainly responsible for developing the standards, subject to FERC approval, which it accomplishes through an iterative process in which the electric utility industry is actively involved. The Regional Entities are mainly responsible for enforcing the standards, and may impose hefty penalties, subject to FERC approval, on entities which violate the standards.

To date, FERC has approved over 100 mandatory Reliability Standards. While only about ten percent of those standards pertain to cyber security, the vast majority of the violations discovered and processed since the implementation of the Federal program have involved violations of the cyber infrastructure protection (CIP) standards. This fact reflects both the newness of the CIP standards, compared to the other standards, and the concomitant lack of experience of Registered Entities to comply with them. This fact also reflects the high priority that FERC, NERC, and the Regional Entities place on compliance with the CIP standards. There is no reason to believe that their emphasis will change in the future; indeed, more likely they will increase their oversight of protecting critical electric grid cyber assets consistent with the focus of other Federal departments and agencies. Colloquially speaking, "only time will tell" whether the current and relatively new Federal paradigm of developing and enforcing standards is effective, and, if so, whether it is the most effective way to ensure a secure electric grid.

[59] *See* http://ferc.gov/about/offices/oeis.asp (last accessed on October 28, 2013).