

**UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION**

**Revised Critical Infrastructure Protection)
Reliability Standards)**

Docket No. RM15-14-000

**PETITION FOR REHEARING OF FERC ORDER NO. 822, REVISED CRITICAL INFRASTRUCTURE
RELIABILITY STANDARDS, 154 FERC ¶ 61,037, JANUARY 21, 2016
AND MOTION FOR REMAND**

Submitted to FERC on February 22, 2016¹

Pursuant to section 313(a) of the Federal Power Act (“FPA”), 16 U.S.C. § 825 (a), and Rule 713 of the Federal Energy Regulatory Commission’s (“FERC” or “Commission”) Rules of Practice and Procedure, 18 C.F.R. § 385.713, the Foundation for Resilient Societies hereby respectfully submits this Petition for Rehearing of the Final Rule issued in Order No. 822 in FERC Docket RM15-14-000, relating to unfulfilled mandates of the Energy Policy Act of 2005.

The Foundation for Resilient Societies (or “Resilient Societies”) is incorporated in the State of New Hampshire as a non-profit organization engaged in scientific research and education with the goal of protecting technologically-advanced societies from infrequently occurring natural and man-made disasters. Information about Resilient Societies, its mission and research, may be found at www.resilientsocieties.org.

Background

In July 2015 the Commission issued a Notice of Proposed Rulemaking on Revised Critical Infrastructure Protection Reliability Standards.² Pursuant to Section 215 of the Federal Power

¹ The Petition for Rehearing is timely filed, because the 30-day filing deadline falls on Saturday February 20, 2016; hence, the first date on which the FERC Office of the Secretary is open for filing is Monday, February 22, 2016. See *Cities of Batavia, et al. v. FERC*, 672 F.2d 64 at 72 (D.C. Circuit, 1982) (FERC regulations extend filing deadlines for weekend due dates and for legal holidays in the District of Columbia).

² 152 FERC ¶ 61,054, July 16, 2015, FERC Docket RM15-14-000.

Act (“Section 215”)³, the Commission on January 21, 2016 approved seven critical infrastructure protection (CIP) Reliability Standards: CIP-003-6 (Security Management Controls), CIP-004-6 (Personnel and Training), CIP-006-6 (Physical Security of BES Cyber Systems), CIP-007-6 (Systems Security Management), CIP-009-6 (Recovery Plans for BES Cyber Systems), CIP-010-2 (Configuration Change Management and Vulnerability Assessments), and CIP-011-2 (Information Protection) (proposed CIP Reliability Standards).⁴

The North American Electric Reliability Corporation (hereafter “NERC”), the Commission-certified Electric Reliability Organization (ERO), submitted the seven proposed CIP Reliability Standards in response to Order No. 791.⁵ The Commission also approves NERC’s implementation plan and violation risk factor and violation severity level assignments. In addition, the Commission approves NERC’s new or revised definitions for inclusion in the NERC Glossary of Terms Used in Reliability Standards (NERC Glossary), subject to modification.

Notably, via Order No. 822 the Commission acquiesced in and rationalized NERC’s defiance of the Commission-ordered definition of “communication networks” earlier required in FERC Order No. 791.⁶

Commission appointees to the Federal Energy Regulatory Commission and the Commission staff have often rationalized weak electric reliability standards promulgated by the Commission as the byproduct of a reliability standard-setting process that places exclusive powers to propose reliability standards in an industry-dominated Electric Reliability Organization.

However, the legislative history of the Energy Policy Act of 2005, which enables mandatory

³³ 16 U.S.C. 824o.

⁴ FERC Order No. 822, Revised Critical Infrastructure Protection Reliability Standards, 81 Fed. Reg. 4177 (Jan. 26, 2016), 154 FERC ¶ 61,037, issued January 21, 2016 in FERC Docket RM15-14-000

⁵ *Version 5 Critical Infrastructure Protection Reliability Standards*, FERC Order No. 791, 78 Fed. Reg. 72,755 (Dec. 3, 2013), 145 FERC ¶ 61,160 (2013), *order on clarification and reh’g*, Order No. 791-A, 146 FERC ¶ 61,188 (2014).

⁶ In FERC Order No. 822, the Commission claimed that, despite NERC’s refusal to define “communication networks” that NERC was “addressing in an equally effective and efficient manner the need for a NERC Glossary definition for the term “communication networks”. See FERC Order 822 at Para. 2, pp. 2-3. NERC concedes that “any proposed definition [of the term “communication networks”] would need to be sufficiently broad to encompass all components in a communication network as they exist now and in the future.” NERC Petition of February 13, 2015, at pp. 51-52.

electric reliability standards and authorizes fines for industry entities, demonstrates through the Federal Power Act amendments of August 2005 a mandate **“to provide for reliable operation of the bulk power system.”**⁷ Among the specific means of implementing that Congressional policy was the authorization of the Commission to protect against “cybersecurity incidents” whether a malicious act or suspicious event” that “disrupts, or was an attempt to disrupt, the operation of those programmable electronic devices and communication networks, including hardware, software and data that are essential to the reliable operation of the bulk power system.”

As the former Chief Scientist of the National Security Agency, George R. Cotter, notes in a concurrent filing:⁸ “ [T]his passage [from Section 215 of the Federal Power Act] refers both to programmable electronic devices” **and** “communications networks including hardware, software and data.’ It does not define communications networks in terms of devices. . . There can be no misunderstanding the intent of Congress in the FPA, the security of communications networks is paramount.”

The divergence between the unequivocal authority that Congress provided the Commission to protect both “programmable electronic devices” and “communications networks” and what the Commission has enabled NERC to do, or to postpone, or to limit, or to exempt from a system for cyber-protected operation of the bulk power system is at the heart of this Petition for Rehearing.

Statement of Issues and Specifications of Error

- 1. The Commission unlawfully failed to implement the unambiguous intent of the Congress to protect reliably against “cybersecurity incidents”: by failing to require broad-scope operational cybersecurity protection, and by reversing the Commission’s requirement for NERC to make a full-scope definition of “communication networks.”**

⁷ Section 215(a), para (3).

⁸ Filing of Isologic LLC, in Docket RM15-14-000, February 22, 2016.

In justification of the refusal of the NERC Standard Drafting Team to define “communication networks” as mandated by para. 150 in FERC Order 791, NERC has admitted that –

“[A]ny proposed definition [of the term “communication networks”] would need to be sufficiently broad to encompass all components in a communication network as they exist now and in the future.” NERC Petition of February 13, 2015, in Docket RM15-14-000, at pp. 51-52.

Conversely, by enabling NERC to *exclude* from cyber protection key components in communication networks, including devices and networks that operate outside of designated physical perimeters, FERC enables continuing use of Internet-connected “communication networks” and cyber-unprotected electric grid substations, and cyber-unprotected industrial control systems that are encompassed by communications networks as they exist now and in the future.

Is the Commission’s action, through adoption of truncated protections from cyber incidents, lawful or unlawful?

What do we learn from the legislative history of the adoption of electric reliability standards via Section 1211 (now Section 215) of the Energy Policy Act of 2005? First, we learn that FERC was signaling to the North American Electric Reliability Council back in year 2002 that cyber penetrations of the bulk power system were an unacceptable hazard, and that the industry had best take the lead in cyber protection before the Commission mandated protections.⁹

Then, the Joint U.S. – Canada Task Force that investigated the causes of the cascading outages in the Northeastern United States and Canada starting on August 14, 2003, determined that unintended loss of Control Center visibility resulted from a “Trojan” malware intrusion, not a purposeful act, but an intrusion of malware that reduced control room visibility and that delayed prompt action by regional Transmission Operators and other utilities. The result was a

⁹ Consult remarks of the Special Assistant to the Chairman of FERC, Alison Silverstein, on the need for cyber protection of the electric grid at a year 2002 conference in Salt Lake City attended by Joseph M. Weiss, then an employee at the Electric Power Research Institute. Personal communication from Mr. Weiss, Jan. 2016.

cascading collapse and wide-area blackout that affected at least 50 million people for up to four days in the United States and seven days in Canada. Cyber protections were among the proposed mandatory reforms resulting from the Joint U.S.-Canada Power System Outage Task Force Report of 2004.¹⁰

A mandate for cyber protection of the U.S. bulk power system was a key component of the proposed reliability standards authority of FERC as presented to the Congress on April 20, 2005 and as enacted on August 8, 2005. The unambiguous Congressional intent to protect “communication networks” from “cybersecurity incidents” and indirectly to protect against cyber-flaw enabled cascading outages is indicated by the careful definition of “cybersecurity incident” in Section 215. The Congress expected protection of the “communication networks” that increasingly would impact control center visibility and the reliable operation of the bulk power system.

Why is it unlawful for the FERC Commissioners to delay consideration of the protection of “communication networks” for a full decade after enactment of Section 215 in year 2005? Why is it unlawful for the FERC Commissioners to condone piecemeal, partial protection from cyber vulnerabilities, whether malicious or unintentional, but nonetheless an unacceptable hazard to consumers who depend upon FERC to assure reliable electric service?

The answer is found in Chevron, U.S.A. v. Natural Res. Def. Council, 467 U.S. 837, 843 (1984), and subsequent cases. In the first of a two-step process, the Commission must give effect to the unambiguous intent of the Congress, where the Congress has expressed its intent, as by specific definition of “cybersecurity incident” for which reliable operation of the bulk power system is mandated. It is the duty of FERC to provide for “reliable operations” of the electric grid, despite cyber hazards known in year 2005 and anticipated for the future. The Commission’s connivance with NERC to exclude an inclusive definition of “communication networks” may be attractive to

¹⁰ See 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, ch. 9, “Physical and Cyber Security Aspects of the Blackout,” p. 131 ff.

utilities seeking financial shields from blackout liability. But it contravenes clear Congressional intent and is unlawful.

The unambiguous duty of the Commission to provide full-scope cyber protection is not merely an obligation under Section 215, but is supportive of the broader obligations of the Commission to provide for reliable operations of the bulk power system.¹¹ Order No. 822 leaves loopholes, access channels for malware, arbitrary labeling of access channels as of “Low Risk” when these channels can nevertheless enable sustained takedown of the North American electric grid. The Commission must implement the cyber protections of the full-scope “communication networks” as intended and as defined by the Congress.

Moreover, FERC Order 672, which sets forth criteria for future ERO reliability standard setting, holds the ERO to a higher standard than “limited impact” on Reliable Operation, requiring design for operations so reliability failures will not occur, not merely a lower likelihood:

Reliable Operation 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 Cybersecurity Incident**, or unanticipated failure of system elements.¹² (Emphasis added).

2. The Commission is Arbitrary and Capricious if the Commission excludes Electric Grid Substations and Industrial Control Systems from cybersecurity protections.

FERC Order No. 822 excludes electric grid substations from mandatory cyber protections in the CIP Version 5/6 standards. The Commission fails to cite the factual explanation of Power Company of New Mexico *(PNM) and Texas New Mexico Power (TNNM) filed in this Docket:

“The NOPR indicates that physical protections may be required for only communication links between Control Center and not Control Centers to non-

¹¹ For the overall duties under the Federal Power Act to provide for reliable wholesale operations of the U.S. electric grid, see the 6 - 2 decision of the U.S. Supreme Court in FERC v. Electric Power Supply Ass’n, Case 14-840, 577 U.S. ____ (Jan 25, 2016).

¹² In February 2006 the Commission adopted as its definition of “Reliable Operation” the phrase quoted above, derived from section 215(a)(4) of the Federal Power Act. See FERC Order No. 672, ¶ 64, issued February 3, 2006 in FERC Docket RM05-30-000. FERC Stats. & Regs. ¶ 31,204, *order on reh’g*, Order No. 672-A, FERC Stats. & Regs. ¶ 31,212 (2006).

Control Centers. FERC may not be aware that some of these communications links actually traverse switch packet systems on a meshed network that includes substations... The backup link may be extended over the Entity's own communication systems. These systems can be full mesh switched packet networks that traverse substations."¹³

It is common, and may be the dominant modality of network control systems, for electric utility Control Center networks to include substation communications in their control networks.¹⁴ The entire network needs cybersecurity protection; otherwise access to or through an electric substation can compromise control centers. Moreover, physical entry to unmanned electric substations can provide "cover" for cyber reconnaissance or implantation of cyber malware into Industrial Control Systems, and into connected Control Centers, especially if electric grid substations are exempted from mandatory cyber protection.¹⁵

Moreover, on January 28 and 29, 2016, a national expert on cyber protection of the electric grid, George R. Cotter, and a national expert on protection of industrial control systems, Joseph M. Weiss of Applied Control Solutions, briefed the FERC Commissioners. The briefing slides prepared by Resilient Societies have been filed in this Docket, following the issuance of FERC Order No. 822 on January 21, 2016.¹⁶

FERC Commissioners need to recognize that, if they insist upon leaving electric grid substations outside the bounds of mandatory cybersecurity protection, these substations provide power to critical facilities operated by large electricity customers. These customers operate aqueducts, oil refineries, telecommunications networks, water & sewer systems, etc.

¹³ See filing of PNM Resources, Inc. in FERC Docket RM15-14-000, filed August 24, 2015.

¹⁴ See the section on "ICS Architecture" in Lewis Folkerth, Forensic Analysis of Industrial Control Systems, Sans Institute, September 24, 2015; and Richard J. Campbell, Cybersecurity Issues for the Bulk Power System, Congressional Research Service, June 10, 2015, section on "Electric Utility Industrial Control System," pp. 3-6. .

¹⁵ See Scott D. Swartz and Michael J. Assante, Industrial Control System (ICS) Cybersecurity Response to Physical Breaches of Unmanned Critical Infrastructure Sites, SANS Institute, Jan. 2014.

¹⁶ See Resilient Societies filing on February 12, 2016. See in particular the PowerPoint viewgraphs provided by Joseph Weiss that illustrate how cybersecurity unprotected electric grid substations can allow harm to other critical infrastructures via the electric substation to customer ICS infrastructure.

Do the FERC Commissions view these hazards, however acute, as beyond their official jurisdiction, because these other critical infrastructures are outside the bulk power system and the wholesale electric markets that the Commissioners regulate? The Commissioners need to broaden their horizons concerning the direct damage they may inadvertently perpetuate. If these other critical infrastructures fail, because FERC left electric grid substation cybersecurity unprotected, it is foreseeable that other operations of the bulk power system will fail, and perhaps in modalities that cause cascading collapse and long-term electric grid blackout.

If communications systems are inoperable for lack of electric power, or if water is not delivered to electric utilities that require water for electric generation, or worse, make-up water essential for spent fuel protection at nuclear power plants, the indirect effects of failing to protect electric grid substations, and associated industrial control systems, will ultimately risk inoperability of the bulk electric system.¹⁷

Order No. 822 fails to provide a reasoned explanation of why the exclusion from cybersecurity protection of electric grid substations is consistent with Congressional intent under the Energy Policy Act of 2005, and consistent with the FERC mandate to protect reliable operations of the bulk power system. For FERC to remain silent on these issues would be arbitrary and capricious.

Moreover, Order No. 822 is conspicuously silent with respect to “lessons learned” from the cyber attacks upon two, and probably as many as eight electric distribution entities in the Ukraine on December 23, 2015.¹⁸ The targets of attack were electric grid substations and their connected control centers, and their service call centers.

Unprotected communications links enabled spearfishing; seizure of Human Machine

¹⁷ In a Keynote Address before the National Academy of Engineering, scheduled for Washington, D.C. on February 23, 2016, Mr. Weiss estimates that there are at least two million industrial control systems presently connected to the Internet, with significant increases pending. If electric grid substations are exempt from mandatory cybersecurity protection, and these substations are connected to networks of unprotected ICS devices, how can the U.S. electric grid operate reliably in the future?

¹⁸ See George R. Cotter PowerPoint presented to FERC Commissioners, and filed by Resilient Societies in Docket RM15-14-000 in February 2016, especially Slide 15 entitled, “Russian Cyber Attack on the Ukrainian National Grid”.

Interfaces (HMIs); blindsiding of system dispatchers; and damage to SCADA system hosts and workstations.¹⁹

How can FERC Order No. 822 be squared with the recent experience in the Ukraine in December 2015? Why was FERC Order 822 silent and nonresponsive to a dramatic cyberattack that occurred just 29 days earlier?

What can FERC do to re-assess and better analyze its dubious claim in Order 822 that the record in Docket RM15-14-000 does not as yet support mandatory cyber protections for Electric Substations? Does FERC expect state regulators to enforce cyber protections for their intrastate load serving entities while FERC adopts an “ostrich” strategy regarding FERC-jurisdictional blackout risks that link Control Centers and electric grid substations, and industrial control systems²⁰ – whether in the Ukraine or in North America?

By retreating from FERC’s prior order to define “communication networks”, intended to broaden the network scope for cybersecurity protections, FERC Order No. 822 places at risk almost all electric grid substations, industrial control systems outside electronic and physical security perimeters, and customer critical infrastructures. FERC has a duty to rationally explain and legally justify its pullback from congressionally mandated protections.²¹

¹⁹ On February 9, 2016 NERC issued a cyber security alert to registered entities but did not release the text of the alert publicly. Two days later, the U.S. Department of Homeland Security’s ICS CERT revised an alert connecting Russian malware utilized since year 2011, with revisions in year 2014, to target electric distribution entities and their electric substations in the Ukraine. ICS CERT noted that “Recent open-source reports have circulated alleging that a December 23, 2015 power outage in Ukraine was caused by BlackEnergy Malware.” ICS CERT Alert 14-281-01E, revised February 11, 2016.

²¹ The Commission must explain a departure from precedent and Order 822 fails to adequately address the Commission’s departure from Order 791, requiring (broad scope) definition of “communication networks” to scope necessary cyber protections. See e.g., Greater Boston Television Corp. v. FCC, 444 F.2d 841, 852 (D.C. Cir. 1970) (“an agency changing its course must supply a reasoned analysis indicating that prior policies and standards are being deliberately changed, not casually ignored, and if an agency glosses over or swerves from prior precedents without discussion it may cross the line from the tolerably terse to the intolerably mute”); La. Pub. Serv. Comm’n v. FERC, 184 F.3d 892, 897 (D.C. Cir. 1999).

3. The Commission’s failure to Order the removal of embedded cyber malware from the U.S. bulk power system is contrary to the Congressional purpose of enabling the reliable operation of the bulk power system.

Nowhere in the series of CIP standards, and nowhere in FERC Order No. 822 is there a mandate for NERC registered entities to remove cyber malware from the U.S. bulk power system. Why is a mandate to remove embedded malware missing from FERC Order No. 822?

Resilient Societies understands that some hardware now installed within the bulk power system contains firmware that cannot be modified to exclude foreign adversaries from prospective cyber exploitations, without removal of the associated hardware. We understand that enhancing the integrity of the cyber supply chain will be further considered by the FERC Commissioners and staff.

These installed hardware and firmware vulnerabilities do not justify the failure of the Commission to order the removal of malware embedded in critical equipment, control centers, and electric grid substations of the U.S. bulk power system.²² FERC has plenary powers for reliable operation of the bulk power system and for enforcement actions.

We respectfully request that the Commission modify Order No. 822 to include the duty to assess, to monitor, *and to remove* cyber malware from the system components of NERC-registered entities subject to FERC jurisdiction.²³ To do otherwise is to defeat the Congressional intent of the Federal Power Act as amended in year 2005.

²² Once again, we cite Chevron, U.S.A. v. Natural Resources Def. Council, 467 U.S. 837 (1984) for the duty of a rulemaking agency to fulfill the unambiguous legislative intent of the Congress. Absolutely nothing in the Energy Policy Act of 2005 implies merely an initial duty to protect against “cyber incidents” but Commission discretion to withhold a duty to remove adversary malware that is feasible to remove from the bulk power system before the results are grid instability, cascading outages, and permanent damage to grid equipment.

²³ The Commission should take notice of a voluntary international cybersecurity industry initiative known as the “Coordinated Malware Eradication Program” (known as CMEP). With tools now available for malware removal and more broadly, with tools now available for malware family eradication, the time has come for the Commission to require more than malware prevention, detection, and identification.

4. The Commission should amend Order No. 822 to clarify that it is not the intent of the Commission to preclude more uniform broad-scope cyber operational program mandates that may in the future be promulgated by the President of the United States or by the U.S. Secretary of Energy.

The Commission in its Order No. 822 on January 21, 2016 makes no mention of extensive cybersecurity protection initiatives that the Congress and the President addressed in year 2015.

One initiative in particular, the Consolidated Appropriation Act for FY2016, H.R. 2029, was signed by the President and became Public Law 114-113 on December 18, 2015. This includes in Division N the Cybersecurity Act of 2015, and the Cybersecurity Information Sharing Act of 2015.

A substantial increase in federal funding for cyber security initiatives is contained in the President's Budget for FY2017.

Also in year 2015, the House of Representatives passed a Proposed Section 215A as an addition to the Federal Power Act which *inter alia* would provide emergency powers vested in the U.S. Secretary of Energy. These powers provide for 15-day limit emergency authorities, including emergency authorities in event of a cyberattack on the U.S. electric grid. This legislation has not been approved but is under consideration in the U.S. Senate in the year 2016 session of the 114th Congress.

Resilient Societies is concerned that, despite newly enacted legislative authority under various titles of the Consolidated Appropriations Act, and potential cyber authority for the U.S. Secretary of Energy governing the Energy Sector, that FERC Order No. 822 will become an inadvertent "ceiling" upon cybersecurity protection mandates for the U.S. electric grid. Congress can pass remedial legislation, but if FERC refuses to implement the clear intent of Congress through the Administrative Procedure Act and Section 215, the public will remain unprotected from the grave risk of cyberattack on the bulk power system.

Will electric utilities claim that FERC Order No. 822 effectively bars the President, or bars the Secretary of Energy from promulgating a broad-scope cybersecurity operational protection

program for the energy sector of the economy? The procedures underlying Section 215 of the Federal Power Act provide opportunities to stall, to weaken, and to undermine the reliability goals of the Commission. FERC and its Commissioners should not fall into this trap.

FERC as a federal regulatory Commission is now joined by the President and various federal departments, and the U.S. intelligence community is seeking to better protect our society from cybersecurity vulnerabilities of our critical infrastructures. We respectfully ask that the Commission modify its Order No. 822 to clarify that it is not the intent of the Commission to preclude complementary operational cybersecurity programs; and that the requirements of FERC Order No. 822 are not intended as a barrier to essential cybersecurity protections otherwise duly authorized.

Additional Reference Material for the Docket

In Order 822, FERC set aside the request of Resilient Societies for cybersecurity protection of communications with electric grid substations, claiming that there was insufficient material in the docket to support this action.

It is entirely within the authority and ability of FERC to research cybersecurity risks and place material in the docket. In fact, this diligent research should be an obligation of FERC and its staff under Section 215. Expecting the electric utility industry to provide all the elements of a balanced docket record is unreasonable at the very least and also could be evidence of intent to be arbitrary and capricious against the interests of the public.

To fill the gap in the docket record, Resilient Societies has provided “Reference Documents to Illustrate Cybersecurity Risks in the Docket” in Appendix 1 to this Petition for Rehearing and Motion for Remand.

Request for Rehearing


For each of the issues presented and for the reasons provided, Resilient Societies respectfully requests that FERC schedule a rehearing on the inadequacies and opportunities to improve FERC Order No. 822; and that, whether or not FERC grants a rehearing, that the Commission order the removal of malware where feasible from the bulk power system; and that the Commission clarify the scope of Order 822 so that, if other duly authorized authorities promulgate cybersecurity operational protection programs for the energy sector, that this Order shall not be used as a bar to further protections of the U.S. bulk power system.

Requests for Remand

Resilient Societies requests that FERC remand to NERC portions of Order No. 822

1. To extend cyber security protections beyond the physical security of designated entities;
and
2. To include electric grid substations in cybersecurity protection standards; and
3. To include cybersecurity protections of communications between electric grid control centers and electric grid substations with industrial control systems; and
4. To include in a revised CIP5/CIP6 cybersecurity standard the duty of registered entities to remove, where feasible, malware embedded in facilities, networks and equipment of the bulk power system; and
5. To include, at a future time, criteria for improved cyber supply chain integrity and
6. To include Red Team exercises testing cybersecurity protections, so cybersecurity standards are not a paper exercise without adequate field assessments; and
7. To consider other recommendations provided separately to the Commission in filings of Isologic, LLC (George R. Cotter) and Applied Control Solutions (Joseph M Weiss).

Respectfully submitted by:



Thomas S. Popik, Chairman,



William R. Harris, Secretary,

For the

Foundation for Resilient Societies

52 Technology Way

Nashua, NH 03060-3245

www.resilientsocieties.org

Appendix 1: Reference Documents to Illustrate Cybersecurity Risks in the Docket

It is intended that each of these below reference documents be incorporated into the record of Docket RM15-14-000 in their entirety, for use in this legal proceeding and/ or future legal proceedings.

ABB, (12/2010), "Cyber security for substation automation systems by ABB," Product Brochure, available at [http://www02.abb.com/global/gad/gad02181.nsf/0/83d0626f0d5bdb56c1257a62004602c9/\\$file/Cyber+security+for+substation+automation+systems+by+ABB.pdf](http://www02.abb.com/global/gad/gad02181.nsf/0/83d0626f0d5bdb56c1257a62004602c9/$file/Cyber+security+for+substation+automation+systems+by+ABB.pdf)

Adhikari , Richard (Dec 16, 2011), "Power Grid Cybersecurity: Who's In Charge?," TechNewsWorld, available at <http://www.technewsworld.com/story/73991.html>

Ali, Ikkal (05/2015), "IEC 61850 Substation Communication Network Architecture for Efficient Energy System Automation," Energy Technology & Policy, available at <http://www.tandfonline.com/doi/pdf/10.1080/23317000.2015.1043475>

Anderson, Dwight (April 7–9, 2009), "Securing Modern Substations With an Open Standard Network Security Solution," 11th Annual Western Power Delivery Automation Conference, available at https://cdn.selinc.com/assets/Literature/Publications/Technical%20Papers/6365_SecuringModern_DA_20090216_Web.pdf

Bucci, Steven (01/2014), "Plotting a More Confident Course: Rethinking Oversight of the Electric Sector and Critical Infrastructure Cybersecurity," Heritage Foundation, available at http://thf_media.s3.amazonaws.com/2014/pdf/SR150.pdf

Burke, Garance (12/2015), "AP Investigation: US power grid vulnerable to foreign hacks," Article, available at <http://bigstory.ap.org/article/c8d531ec05e0403a90e9d3ec0b8f83c2/ap-investigation-us-power-grid-vulnerable-foreign-hacks>

Fox-Brewster, Thomas (10/2015), "Want Some Nuclear Power Plant 'Zero-Day' Vulnerabilities? Yours For Just \$8,000," Forbes, available at <http://www.forbes.com/sites/thomasbrewster/2015/10/21/scada-zero-day-exploit-sales/#db921f7d96c9>

Gung, V. Cagri (05/2006), "A Survey on Communication Networks for Electric System Automation," Computer Networks; Volume 50, Issue 7, 15 May 2006, Pages 877–897, available at <http://www.neetrac.gatech.edu/publications/Electric%20System%20Automation.pdf>

Jackson Higgins, Kelly (01/2014), "Power Utility Substations At Risk," InformationWeek, available at <http://www.darkreading.com/vulnerabilities---threats/power-utility-substations-at-risk/d/d-id/1141197>

Jackson Higgins, Kelly (01/2016), "Project 'Gridstrike' Finds Substations To Hit For A US Power Grid Blackout," InformationWeek, available at <http://www.darkreading.com/threat-intelligence/project-gridstrike-finds-substations-to-hit-for-a-us-power-grid-blackout/d/d-id/1323788>

James, Clapper (09/2015), "Statement for the Record; Worldwide Cyber Threats; House Permanent Select Committee on Intelligence," Office of the Director of National Intelligence, available at <http://www.dni.gov/index.php/newsroom/testimonies/209-congressional-testimonies-2015/1251-dni-clapper-statement-for-the-record,-worldwide-cyber-threats-before-the-house-permanent-select-committee-on-intelligence>

Kassakian, John (12/2011), "The Future of the Electric Grid An Interdisciplinary MIT study," MIT Energy Initiative, available at <http://mitei.mit.edu/publications/reports-studies/future-electric-grid>

McDonald, John (05/2012), Electric Power Substations Engineering, Third Edition, CRCPress, Available for purchase only

Mills, Elinor (05/2010), "Joe Weiss, crusader for critical infrastructure security (Q&A)," Cnet, available at <http://www.cnet.com/news/joe-weiss-crusader-for-critical-infrastructure-security-q-a/>

National Cybersecurity And Communications Integration Center, (12/2012), "ICS-CERT Monitor," Newsletter, available at https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2012.pdf

National Cybersecurity And Communications Integration Center, (04/2014), "ICS-CERT Monitor," Newsletter, available at https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_%20Jan-April2014.pdf

Nordell, Daniel (01/1900), "Communication Systems for Distribution Automation," , available at <http://cialab.ee.washington.edu/nwess/2008/presentations/daniel.pdf>

Pagliery, Jose (12/2014), "U.S. power grid hit by hackers 79 times so far this year," CNN, available at <http://www.smartgridnews.com/story/us-power-grid-hit-hackers-79-times-so-far-year/2014-11-19>

Rashid, Fahmida (10/2014), "Project SHINE Reveals Magnitude of Internet-connected Critical Control Systems," SecurityWeek, available at <http://www.securityweek.com/project-shine-reveals-magnitude-internet-connected-critical-control-systems>

Rogers, Michael (11/2014), "National Security Agency; Hearing of the House (Select) Intelligence Committee; Subject: Cybersecurity Threats: The Way Forward," National Security Agency, available at https://www.nsa.gov/public_info/files/speeches_testimonies/ADM.ROGERS.Hill.20.Nov.pdf

St. John , Jeff (08/2012), "Cisco and Alstom Plot the Internet of the Grid Substation," Article, available at <http://www.greentechmedia.com/articles/read/cisco-and-alstom-plot-ip-for-the-grid-substation>

Udren, Eric (04/2000), "Significant Substation Communication Standardization Developments," 2nd Annual Western Power Delivery Automation Conference, April 2000, available at https://cdn.selinc.com/assets/Literature/Publications/Technical%20Papers/6105_SignificantSubstation_20000417_Web.pdf

Weiss, Joseph (July 30 2014), "Real Hacks of Critical Infrastructure are Occurring – Information Sharing is Not Working," InfoSec Island, available at <http://www.infosecisland.com/blogview/23893-Real-Hacks-of-Critical-Infrastructure-are-Occurring--Information-Sharing-is-Not-Working.html>

WGBH, (10/2015), "Cyberwar Threat," PBS, available at <http://www.pbs.org/wgbh/nova/military/cyberwar-threat.html>