193 Southdown Road
Edgewater, MD 21037
grcotter@comcast.net

April 11, 2020

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, NE
Washington, D.C. 20426

Dear Ms. Bose,

Attached, please find my Motion to Intervene filing on Docket No. EL20-46-000 Related to Critical Infrastructure Supply Chain Reliability Standards.

Respectfully,

George R. Cotter

Enclosure: a/s

UNITED STATES OF AMERICA

BEFORE THE

FEDERAL ENERGY REGULATORY COMMISSION

Motion to Intervene in Docket)
Related to Critical Infrastructure) **Docket No. EL20-46-000**
Supply Chain Reliability Standards)

Submitted to FERC on June 11, 2020

Introduction

I, George R. Cotter, a private citizenl, am filing this Motion to Intervene in Docket No. El20-46-000 in accordance with 16 U.S. Code § 824o(d)(5) and 16 U.S. Code § 824o(e) in support of Mr. Mike Mabee's Complaint on this docket dated May 11, 2020. Mr. Mabee's Complaint focuses on the lack of transparency in Regulatory actions on Critical Infrastructure Protection violations by utilities, and the conflict of FERC Order No. 850 with Executive Order 13920. My Intervention adds significant background and additional challenges to Federal Energy Regulatory Commissions actions on Supply Chain vulnerabilities, and more importantly, the deliberate Commission policy of dissembling on security standards, the distortion and suppression of vulnerabilities in the North American Grid, and a conspiracy of cover-up actions in regulatory management of ERA Section 215 responsibilities to protect critical electric infrastructure.

Of note:

1. Eight years of delay, and counting, on Supply Chain risks after major penetrations of vendors by Russia in 2012, a full decade since, with major Supply Chain regulatory actions that will still be open past 2022.
2. Suppression of the FBI report on the follow-on 2014 lengthy Federation reconnaissance of the U.S. Electric Grid enabled by Supply Chain vulnerabilities.
3. Failing to secure electric power service to critical National Security facilities nearly totally dependent on commercial power; specifically, facilities known to be critical to response to such attacks.
4. Total failure to effectuate a 24/7 nation-wide utility BPS situational awareness, warning network.
5. Violating a public trust by facilitating a decade-long cover-up of electric system vulnerabilities and intrusions by foreign nation/state adversaries.
6. Despite the clear language of EPA Section 215, approving the exclusion of Grid communications and networks from CIP Standards, CIP-002.5.1a; the major pathway for adversary exploitation of Supply Chain, and other vulnerabilities.
7. Deliberate denial of Congress, the GAO, oversight Departments, Federal Agencies and State governments on security of BPS power feeds to Distribution systems through misuse of FAST Act provisions for protection of critical assets, i.e.,. CEII actions on CIP Violations
8. Ensuring that CIP Standards, all subject to approval by FERC, do not reveal and therefore compromise, the massive and insecure interconnection of BES and Distribution systems; i.e., less that 10% of BPS substations subject to CIP Standards, (see NASPI synchrophasor map Page 13.)

9. Prohibiting utility actions for vendors' culpability in Supply Chain attacks, including US vendors that supply major IT underpinnings for electric instrumentation (i.e., IT firms).

Comment: ***Most prior filings and White Papers have described CIP Standards as a veritable "House of Cards", superficially protecting management, organizational, internal systems; hardly a deterrence to the nation's adversaries targeting the electric power system. For this filing, the entire stack of "Reliability Standards" was shredded into CIP and non-CIP elements, and "Operational" cyber systems standards stood out in stark contrast to non-power cybersecurity standards, revealing the NERC/FERC cybersecurity protocol as the charade it is. Examine the table on P7, 476 pages of critical "operational" protection systems standards, whose cyber assets are absolutely devoid of cybersecurity wrappings.***

Background

The Bulk Power System is a cybersecurity nightmare, almost totally susceptible to Supply Chain attacks, when, as and if a nation/state adversary chooses. FERC, NERC and industry efforts have conspired to create a regime that almost totally isolated Operational activities from federal cybersecurity regulation; substituting an almost meaningless structure limited to individual facilities, ensuring the continued protection of utilities from federal security oversight.

For many years, this filer, and others have documented vulnerabilities and threats directly linked to current Critical Infrastructure Protection (CIP) standards.[1] These filings have intervened in NOPRs and Final Orders in public comment periods, with mixed but usually poor results. Filings have also been made on issues arising from questionable NERC and industry reports of CIP and other violations of Reliability Standards. And more recently, challenges including FOIAs objecting to the industry, NERC and FERC practice of redacting violation reports including inappropriate use of CEII to obscure utility identifications and critical details of infractions.

It would be a gross understatement to say that filers have seen steady deterioration of protection of the electric system from nation/state adversaries, largely due to weak standards, major delays on implementation, and negative effects on vendors from "Security through Obscurity". FERC has consistently used "divide and conquer" techniques in its policies of denial. The effect has been to add grave risk to unprotected Distribution systems, electrical supply to Critical Infrastructures, and place the Grid-dependent national security facilities responsible for protection of the nation, in dire jeopardy.

Additionally, for many years, FERC chairmen have also received this filer's White Papers on "***Security in the North American Grid***" with cover letters to key Congressional and Administration leadership. Themes included CIP Standards, utility vulnerabilities including Supply Chain issues, significant threats including malware development, U.S. incursions, testing abroad, and direct connectivity to 2016 and 2018 U.S. elections. FERC Commissioners have generally ignored these warning papers.

[1] See for example Isologic LLC, filing NOPR Supply Chain Risk Management Reliability, Docket No. RM17-13-000 Jan 18, 2018

In early days, these White Paper distributions were followed up with constructive meetings with Chairmen or Commissioners but this has ended. Chairman Chatterjee was sent the most recent White Paper[2] along with cover letters to Secretary of Defense and Co-Chairs of the Congressional Cyberspace Solarium Commission. That report was mainly to document the dire condition in the overall national Grid arising out of the growing divide between the reality of threats and contributions to that debacle by the FERC/NERC cover-up conspiracy.

Details

This filing centers on the frailties of Order No. 850 as well as the systemic weaknesses of what passes for BES security. The public, critical infrastructures, the national security community, and Congress is asked to believe that Order No. 850 will provide adequate Supply Chain protection of electric supply to their facilities. This filing will prove otherwise.

Those interested might fairly ask "***What overall cybersecurity structure is in place to accommodate these changes to protect the end user?"***

So, Commissioners, let us examine your cybersecurity infrastructure ***and the stack of cyber assets, industry systems needing cybersecurity protection from adversaries, top down and end-to-end:***

1. Two national authorities, FERC and NRC, and 50 state authorities independently regulate cybersecurity protection for electric services but ***with no operational security coordination mechanism across the Grid as a whole.*** Supply Chain standards (Order No. 850) are applicable only to FERC-regulated Bulk Energy Systems ***(but by no means, all such vulnerable systems, as will be documented in this filing.)***
2. NRC-controlled, nuclear generation sites transfer their power to Transmission (BES) substations and Distribution facilities to users but must import power for safety-critical systems. This import of power is generally considered contractually regulated, not federally regulated***, i.e., outside the scope of Order No. 850.***
3. There is ***no Grid-wide operational "situational awareness" or alerting structure functioning across this three way digital divide*** to warn of Supply Chain attacks, incursions, incidents, campaigns, etc.
4. Coincidentally, therefore, there is ***no operational data exchange between these three separate domains,*** no nation-wide data base on operational data, no concentrated examination of operational data for Supply Chain threat determination or actual adversary penetrations.
5. Further, ***a major source of Supply Chain vulnerabilities of domestic IT firms and which are endemic to BES/Transmission and Distribution facilities*** is exploited by nation/state adversaries; example: the 2014 U.S. Grid attack facilitated by a zero-day Microsoft system vulnerability.

[2] "Security in the North American Grid-Cybersecurity, CEII and the Digital Divide", A White Paper, April 25, 2020

6. Bulk power is transmitted to/through state-regulated "Distribution" systems within and across 48/50 states to end users. ~1400 independent/semi-independent "registered" Generation and/or Transmission entities (i.e., utilities) ***independently categorize BES cyber systems*** (consisting of ***BES cyber assets***). That is what is subject, in theory, to Order No.850.
7. But many operational technology **(OT)** systems remain uncharacterized as ***BES*** cyber systems, although clearly have substantial ***cyber assets***. NERC's extensive compendium of Reliability Standards[3] differentiates, i.e., separately lists **CIP** standards from a plethora of Operational (OT) standards, labeled **BAL, COM,** etc. These **non-CIP** standards' characterizations differing them from **CIP** standards, and are BES operational functions. ***There is no EPA 2005 Section 215 authorization for this policy and NERC is silent with no logical justification for such practice. This gives the nation's adversaries engaged in Supply Chain attacks freedom of choice on industry targets.***

> **Comment:** As cited above, a significant element of Supply Chain attacks is the exploitation of extensive security vulnerabilities in commercial Information technologies (IT). Most utility operational capabilities use commercial systems for data management, communications interfaces, enterprise management systems. Many such commercial IT systems host security vendor software for gateway protection. Importantly, these IT systems underpin energy-unique systems supplied for control systems and other energy-unique functions. If vulnerable to cyberattack, they represent a major complication in defense of Supply Chain attacks although not explicitly identified as such in Order No. 850. In 2014, a Microsoft system vulnerability was, in fact, the major portal for the Russian Federation attack using previously (in 2012) hacked control systems of three major industry control system vendors. An FBI investigation report was never made public. Federation tools were accordingly updated and tested the following year in the Ukraine. That relationship to the 2014 U.S. attack was signicantly underplayed by FERC.

8. **BAL non-CIP** standards are where Balancing Authorities these days make extensive use of **DDR** and **Synchrophasor** systems as well as Data Processing Centers to manage operational power flows. These tools are now the principal source of quality data supplementing SCADA flows with higher precision results. NERC and the industry assiduously avoid characterizing these operational cyber assets under ***CIP*** standards, but the Russian Federation is targeting them you can be sure; see **Synchrophasor** map on Page 13.
9. Several other ***non-CIP*** Reliability Standards (e.g., **COM, EOP**) show clearly they are thinly -disguised efforts to keep Operational activities out of ***CIP*** categorization. Modern communications systems are heavily digital, highly automated, and therefore susceptible

[3] NERC publication titled: "***Reliability Standards for the Bulk Electric Systems of North America,*** Updated January 2, 2020" . This publication hosts all Reliability Standards; both CIP and non-CIP.

to Supply Chain attacks. Many of the ***EOP***, non-CIP standards involve digital systems whose loss would jeopardize the operation of the BES, incident identification and reporting, also available vectors for Supply Chain attacks ***but not covered by Order No. 850.***

10. ***FAC*** standards, notably Facility Interconnection requirements, Transmission Vegetation Management, System Operating Limits, Maintenance, Transfer Limits, etc., involve complex data aggregations, interoperability capabilities, real time monitoring functions and a host of planning and data exchange capabilities. These **non-CIP** cyber asset activities are natural targets for sophisticated information operations and therefore Supply Chain attacks by the nation's adversaries. The ***PG&E*** massive data base compromise and the abject vegetation management failure of this major utility had deadly consequences. All these ***FAC*** functions ***are excluded from Order No. 850.***
11. The functions and capabilities required of Reliability Coordinators (RCs) are major utilities) reflected in the ***IRO*** Reliability standard are replete with descriptions of data compilations, logging information and similar tools that are heavily automated both in data processing but also data exchange. ***Such activities are massive operational cybersecurity targets in the heart of the Bulk Electric System***, but as with other ***non-CIP*** standards, ***not covered by Order No. 850.***
12. Transmission operations, **TOP**, is a catch-all Reliability Standard that ensures that ***each utility*** involved in operations understands its unique (i.e., individual utility) responsibilities to the overall **BES.** As such, every cyber asset and cyber system within a utility is, ***in principle,*** subject to all of the NERC Reliability Standards. **TOP non-CIP** standards requirements are totally oriented to "Operations" and include 24 separate requirements each dealing with real-time actions and protection function. There are separate requirements addressing planning, data collection and retention, and monitoring and analysis activities. **TOP** activities therefore require each utility to employ cyber assets/systems applicable to any Reliability-Standards requirement across its entire footprint, from Enterprise Management Systems to each substation's interface with Distribution Systems. ***There are no requirements citing Cybersecurity Standards, thus no obligatory utility linkages to Order No. 850.***
13. **TPL, non-CIP** Transmission System Planning Performance Requirements***,*** is the Reliability Standards category describing all regulated functions involved in planning performance for the **BES**. Note that planning is collectively viewed as being so critical to the BES that utility's "***performance"*** of the planning function is included in these standards. **TPL** therefore deals with cyber assets used in the performance of control systems, operations, data management, communications, monitoring and analysis. Although such **TPL** cyber systems are certain to be targeted by the nation's adversaries for Supply Chain vulnerabilities, they are ***excluded from Order No. 850 controls***.
14. **TPL non-CIP** standards are even more concerning on emerging national cyber threat issues coupled to modernization (e.g., Synchrophasors, GPS, and "natural" events; weather, climate-change solar/wind systems, and solar storms (Global Magnetic

Disturbances, GMD.) The GMD threat to the BES is well established through largely Canadian experiences, **despite concerted efforts by the industry to avoid requirements for GIC devices** and critical protection for ***step-up transformers*** in major areas of the Northeast, the Canadian Maritime Provinces, the Pacific Northwest. ***Note over 200 Chinese high voltage transformers have been installed in the US, including Northwestern GMD-susceptible federal generation facilities.*** Significant **TPL** actions on cyber systems critical to **GMD**, forced on NERC and FERC by relentless pressure from technical and scientific sources, carefully avoid cybersecurity requirements in the extensive **TPL GMD** documentation. A reasonable assumption is that the Russian Federation might target those transformers in a "false flag" operation coupled to election intrusions. ***However, there are no hooks to Supply Chain controls, i.e., Order No. 850, in the extensive NERC Reliability Standards GMD documentation.***

15. **VAR** is a category of Reliability Standards that covers measurement, monitoring and control of real time voltages and reactive systems critical to the exchange of power from one utility to another. Power system stability is critical to functioning of the BES and **VAR** standards apply to systems important in the handoff of power from one utility to another. Cyber assets/cyber systems vulnerable through "Supply Chain" firmware or malware ***should be covered by Order No. 850***, but VAR requirements are devoid of this factor.

16. **PRC** Reliability standards include a massive set of over 30 BES Protection requirements covering Transmission, Generation and "connected" Distribution functions. Note this is the largest set of Reliability rules for protection of the Bulk Power System, what should be at the heart of Supply Chain protection needs, but they are **non-CIP**, not covered by Order No. 850.
17. A revealing example of this **non-CIP/CIP** "digital divide" comes to light from a SERC RE Compliance audit[4] that aggressively cited TVA for "serious" violations of **PRC-001-1**, maintenance failures of less than 1% of over 45000 TVA protection devices. TVA protested to no avail and since the SERC RE penalty assessment of $852,000 was null and void (TVA is a Federal Corporation), SERC RE sanctioned TVA for three years for quarterly reports on all 45000 protection devices. Part of the SERC RE charge incredibly claimed that TVA failed to consider **CIP** Communications risks in its violation of **non-CIP** Standards.

18. **PRC non-CIP** requirements cover the entire gamut of BES cyber assets/cyber systems that involve BES Protection Systems. Requirements bear dates as early as 2005 to the present day. The Eastern Blackout of 2003 and the technical reviews that followed are the genesis of many of these requirements. More recent requirements arise from the trend to solar and wind generation and of course the complexity of absorbing such power into the grid. There are 476 pages devoted to PRC non-CIP Protection issues. Writeups are often lengthy and highly technical on complex engineering matters, a testimonial to hard working utility engineers and utility operators and executives who have engineered one of the marvels of modern American and Canadian technology. The simple table that

[4] NERC Full Notice of Penalty Re: Tennessee Valley Authority, Docket No. NP18-000, July 31, 2018

follows is included here to try to illustrate the comprehensive nature of Protection measures inherent in the BPS[5]. Page counts are a good indicator of complexity. The PRC topics undoubtedly also reflect similar Distribution system functions***. Note however that in scanning and assembling the foregoing summay, not a single cybersecurity mention was encountered. This was understandable in 2003; in 2019 it is incomprehensible.*** There were, however, frequent admonitions about the importance of communications systems to coordination, data exchange, real time calculations, measurements, and operations.

RQMT	Description	Page Count	Comment
PRC-001-1	Protection Coordination System	6	Across Entities
PRC-002-2	Disturbance Monitoring & Reporting	38	Data needs, precision
PRC-004-5	Mis-operation, Identification, Correction	32	
PRC-004-6	WECC Remedial Action Scheme	7	Occasional Regional Variation
PRC-005-1b	Transmission& Generator Maint & Testing	40	Voltage/Current Sensing Device
PRC-008-0	Under Frequency Load Shedding	2	Auto Switching
PRC-010-2	Under Voltage Load Shedding	29	Transmission lines, Reactors
PRC-011-0	Maintenance and Testing	2	Relays, Transformers, Batteries
PRC-012-2	Remedial Action Scheme, RAS	49	Ditto
PRC-013-1	RAS Database, Disturbance Monitoring Equip	2	Installation, Data Recording
PRC-014-1	RAS Assessment	2	
PRC-015-1	RAS Data & Documentation-Capabilities	2	Coord Generator Unit & Plant Controls
PRC-016-1	RAS Mis-operations	2	
PRC-017-1	RAS Maintenance and Testing	2	
PRC-018-1	Disturbance Monitoring Equipment	4	Data Reporting
PRC-019-2	Coord Gen Unit and Plant capabilities	11	Voltage Regulation
PRC-023-4	Coord Transmission Relay Loadability	15	Transformers !!!
PRC-024-2	Generator Freq & Voltage Protection	12	Relay Settings
PRC-025-2	Generator Relay Loadability	114	Step-up Transformers
	Application Guidelines	1	
PRC-026-1	Relay Performance	84	During Stable Power Swings
PRC-027-1	Coordination	17	Across Entities/Functions
	Total	476	

[5] The 476 pages of text, data and diagrams show no coverage of cybersecurity standards or sensitivity of the cyber assets or cyber systems to vulnerabilities, even Supply Chain vulnerabilities. These are fundamental protection devices but reflect no cybersecurity protection.

There are 3X the number of pages in NERC's Reliability Standards publication devoted to **non-CIP** Standards compared to **CIP** standards. How, then, do the **CIP** Standards provide adequate security to BES cyber systems? Let's add the following **CIP BES** Transmission and Generator data to the above "Stack"to complete this summary of the focus of NERC Reliability Requirements.

1. **CIP-002** cyber system categorization excludes Nuclear sites and Distribution facilities, and of course Alaska and Hawaii, non-sensible but blame the EPA. But this **CIP** standard also excludes categorization of all **BES** Communications and Network cyber systems, despite contrary language in EPA Section 215. ***Why?*** Any examination of **non-CIP** standards shows that to have included this in **CIP** standards would compromise the separation of OT Operational standards from cybersecurity (**CIP**) envelopment. The previous chart shows why.
2. NERC and FERC assert that **CIP** standards are conditioned on risk to the **BES**, not risks to the Grid writ large. This is absurd on the face of it; **BES** protection does not ensure protection of Distribution or Nuclear facilities. The nation's cyber adversaries have demonstrated ability to penetrate the overall Grid through multiple portals and move laterally. GAO has tasked FERC to show how the Grid would respond to simultaneous attacks.[6] Nevertheless, **CIP-002** excludes from **CIP** standards any facility that does not pose a risk to the **BES** within 15 minutes of assault. Further, CIP also excludes from its standards, any facility/substation that is below a graduated set of MW limits for the BES, ignoring plausible attack vectors. Cyber systems also are graded into Low, Medium and High categories, dependent on impact of loss to the BES.
3. Furthermore, it is left to individual utilities to define a cyber system subject to **CIP** standards; be it a single cyber asset, a collection of cyber assets, even an entire substation. This produced a weird set of disparate candidates for **CIP v4**, approximately only 5% of Transmission substations covered by **CIP** Standards. Even FERC could not stomach these numbers, **CIP v4** gave way to **CIP v5**. Nevertheless, the candidate numbers did not change and FERC has steadfastly refused to divulge what is covered by **CIP** standards and what facilities are not. Thus, the very base for **CIP** coverage is unspecified and thus ***the actual cyber systems subject to Supply Chain Standards, Order No. 850 remains unknown***, presumably even to NERC and FERC.

[6] GAO Report 19-332 Critical Infrastructure Protection, August 2019

Comment: NERC and FERC may try to assert that BPS Operations are exempt from cybersecurity controls or assert that **CIP** Standards are effective for all cyber systems in Reliability Standards labeled **non-CIP** in this filing. ***Either would be utter nonsense.*** The mass of documentation in NERC's **non-CIP** Reliability Standards compendium are totally devoid of **CIP** linkages. Further, Compliance audits avoid any cross connection. And given these major **CIP-002** uncertainties, it is impossible to judge the efficacy of standards subordinate to **CIP-002**. Given what has preceded, in the foregoing stack, it is reasonable to assume this obscurity was by design. With the large number of variables on categorization of cyber assets and cyber systems, registered entities (utilities) could easily confuse compliance authorities (RCs) on periodic assessments. Very large utilities would incur increased costs if the conflict of **CIP** and **non-CIP** systems was exposed and use categorization vagueness to minimize such conflicts, for example in hundreds if substations housing both Transmission and Distribution assets. CIP-002 exceptions and vagueness make a nonsense of the term "standard" for the Bulk Power System.

4. **CIP-003** Security Management Controls assert separate protection requirements for medium/high impact and low impact cyber systems. A fundamental condition is that all electronic aspects involve a concept of a Secure Electronic Perimeter***, given the total exclusion of communications and network cyber systems from CIP Standards***. This is a theoretical but thoroughly impractical condition that ignores security of data flows and interactive electronic functions critical to operations, all of which would have to be ignored in compliance assessments. Even controls on vendors are impractical considering extensive direct maintenance contracted out. And those are ideal venues for Supply Chain attacks. Most other security management functions in this standard affect subsequent CIP standards (e.g., CIP 004 Personnel and Training). ***It is important to note that CIP-003 and subsequent standards detail management, planning and other, often idealistic, security hygienic functions and rigorously avoid direct relevance to Operations.***
5. **CIP-*004*** Personnel and Training Standard exists as part of a suite of CIP Standards "***related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES."*** There are, in fact, no linkages of this standard to actual "Operations". Operational here can only mean the functions of personnel security. Here again, the process involves the bureaucratic (documentation, planning, hygienic) stages of security management of BES Cyber Systems, ***not security management of utility's power operations (covered by non-CIP standards.)***
6. **CIP-*005*** Electronic Security Perimeter standard, previously mentioned, is an artifice to account for ***exclusion*** of communications and networks from categorization of Cyber Systems. It is maddening to try to understand the standard, ***applicable only to BES Cyber Systems***, when it cites registered entities such as Balancing Authorities controlling

systems such as load shedding, cranking paths, systems carried under non-CIP Reliability Standards. Is this the "carny" game of "which shell is the peanut under?" And ***"Each Responsible Entity shall implement one or more documented [processes, plan, etc]"*** is the end game, not "Operations". ***But let's take the 10,000 foot view and ask "How do tens of thousands Transmission, Generator and Distribution Provider ESPs in a connected Grid, lacking cybersecurity controls on their ESP communications and network connectivity,*** protect even the Bulk Electric System from penetration, and more importantly, Supply Chain attacks? More utter nonsense.

7. **CIP-006** Physical Security of BES Cyber Systems, **CIP-007** Systems Security Management, **CIP-008** Incident Reporting and Response Planning and **CIP-009** Recovery Plans for BES Cyber Systems is more of the same. Applicability to BES Cyber Systems is asserted but applicability to Cyber Systems organic to Operational functions, i.e., cyber assets of **non-CIP** cyber systems with different Reliability Standards. ***This conundrum is not addressed in Order No. 850, Supply Chain Standards.***
8. ***CIP-010*** *Configuration Change Management and Vulnerability Assessments* purpose is *to* prevent and detect unauthorized changes to BES Cyber Systems. In respect to systems not categorized as such, i.e., Operational Cyber Systems under **non-CIP** Reliability Standards, it has no applicability. The use of cyber security controls refers specifically to controls referenced and applied according to **CIP-005** and **CIP-007**. Therefore, if those standards only apply to cyber assets categorized under CIP-002 as BES Cyber Systems, **CIP-010** is further excluded from applying to **non-CIP** Reliability Standards. **CIP-011** Cyber Security Information Protection is to prevent unauthorized access to BES Cyber System Information and therefore is linked only to foregoing **CIP** standards.
9. ***CIP*-012** Cyber Security – Communications between Control Centers is to protect the confidentiality and integrity of Real-time Assessment and Real-time monitoring data transmitted between Control Centers. It is not an exception to **CIP** 002 since it deals with data exchange, not the communications media itself. Also, although it is a **CIP** standard, its only requirement is for a "plan" on how protection is applied, and stops short of any reference to Cyber Assets or Cyber Systems. FERC had originally directed NERC to ***"develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers.".*** However, the requirement to protect, at a minimum, communication links was dropped in the final Order No. 822 rule. Thus, the **CIP-002** exception was essentially retained.
10. ***CIP-013*** Cyber Security - Supply Chain Risk Management addresses Order No. 829 directives for entities to implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts. The plan(s) would apply to BES medium and high impact but not low impact Cyber Systems. And while the ***plan(s)*** must address…….

(1) Software integrity and authenticity
(2) Vendor remote access
(3) Information system planning; and
(4) Vendor risk management and procurement controls,

……but there are no meaningful guidelines for plan(s) to ensure effective mitigation of risks and no "standardization" of measures to ensure effectiveness, across 1400 Registered Entities separate Order No. 850 plans.

Comment: The Order No. 850 Supply Chain standard hardly exceeds good hygienic security procedures for ordinary procurements and implementations. It totally fails to recognize the sophistication of adversaries' cyber capabilities and the realities of flaws and vulnerabilities of commercial IT systems linked to energy industry vendor offerings. And inclusion of access control systems, e.g., EACMS, is delayed several years. Further, a single, recent CISCO vulnerability assessment, **for example,** listed over 3600 CVEs that are totally beyond a utility's ability to understand, let alone relate to unique energy industry products. Supply Chain threats are at a stage where the only sensible activity in a proposed Supply Chain Standard is **Whitelisting** and **Blacklisting**, and, in the interest of costs, a funded, industry-wide vulnerability evaluation program for critical procurements. FERC Order no. 850 is dead on arrival.

"Exposure" Summary

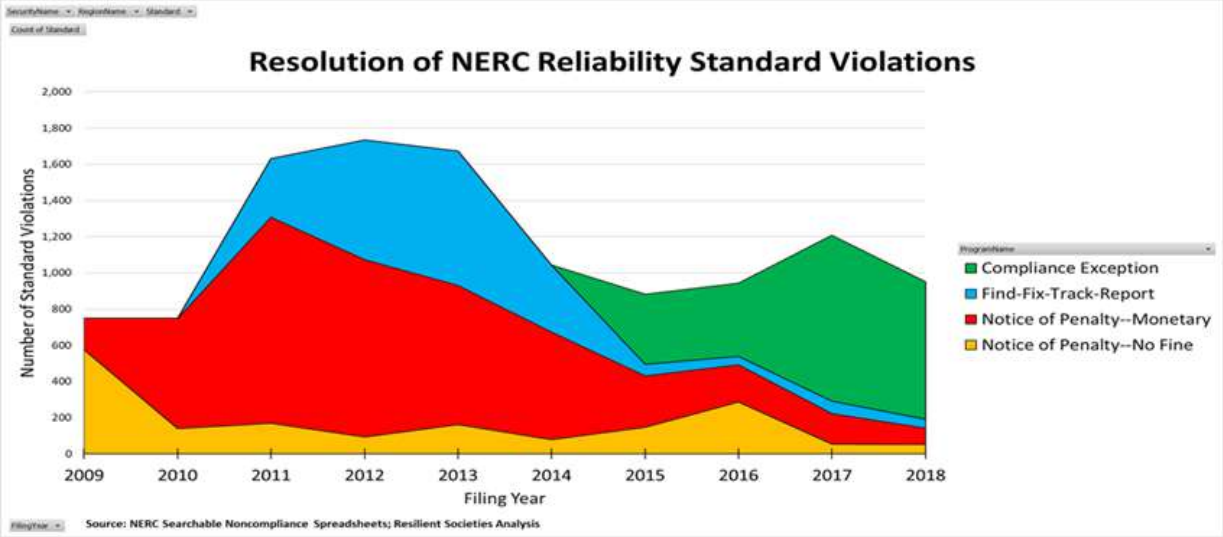
It is admittedly difficult for anyone caught up in the cyber risks to this nation to understand the actual effects of the foregoing summary of flaws in what is defended as protection for the Bulk Electric System. It is probably more complex than predicting the economic aftereffects of the current pandemic. But experts in the five or six critical infrastructures, including the Conus national security functions, have grave concerns and some actual experiences (i.e., malware-related election intrusions), in the capabilities of the Russian Federation to seriously disrupt the Grid. The current Congress in bi-partisan frustration created the Congressional Cyberspace Solarium Commission to address cyber threats to the nation and is strongly recommending a National Deterrence Policy. That key finding is driven by a prior Defense Science Board Deterrence recommendation directly coupled to national security risks of a Grid takedown. FERC has had this filer's interventions on precisely this evolution, yet continues abetting these risks from the Federation out of deference other industry priorities.

Comment: At this point, what should be obvious to any reader of this filing is that Regulators are excluding most if not all operational functions of the BES from cybersecurity controls, This was clearly not the intention of Congress in its EPA legislation of 2005. Nevertheless, Standards authorities (e.g., NERC and FERC) have created a CIP and non-CIP separation of operational systems and non-operational systems and have been careful to maintain this separation in regulatory matters since implementation of Section 215 of the EPA. This has required cooperation between utilities, NERC, and FERC taking conspiracy to defeat EPA Section 215 to new heights. Reliability Coordinators have been careful to avoid compliance monitoring of very large utilities for fear of exposing the seams of this digital divide. Conflation of CIP and non-CIP standards has been rigorously avoided. Minimization of compliance reporting, redactions and CEII are used to further obscure the near-universal avoidance of cybersecurity controls on most operational cyber assets.

Compliance (?)

There is little point to repeat in this filing the many issues raised by this, and other filers over the last eight years expressing fears of Supply Chain vulnerabilities, actual subversion of vendors' systems used in the Grid, related malware challenges, and systemic weaknesses in CIP Standards. A few highlights are in order, however.

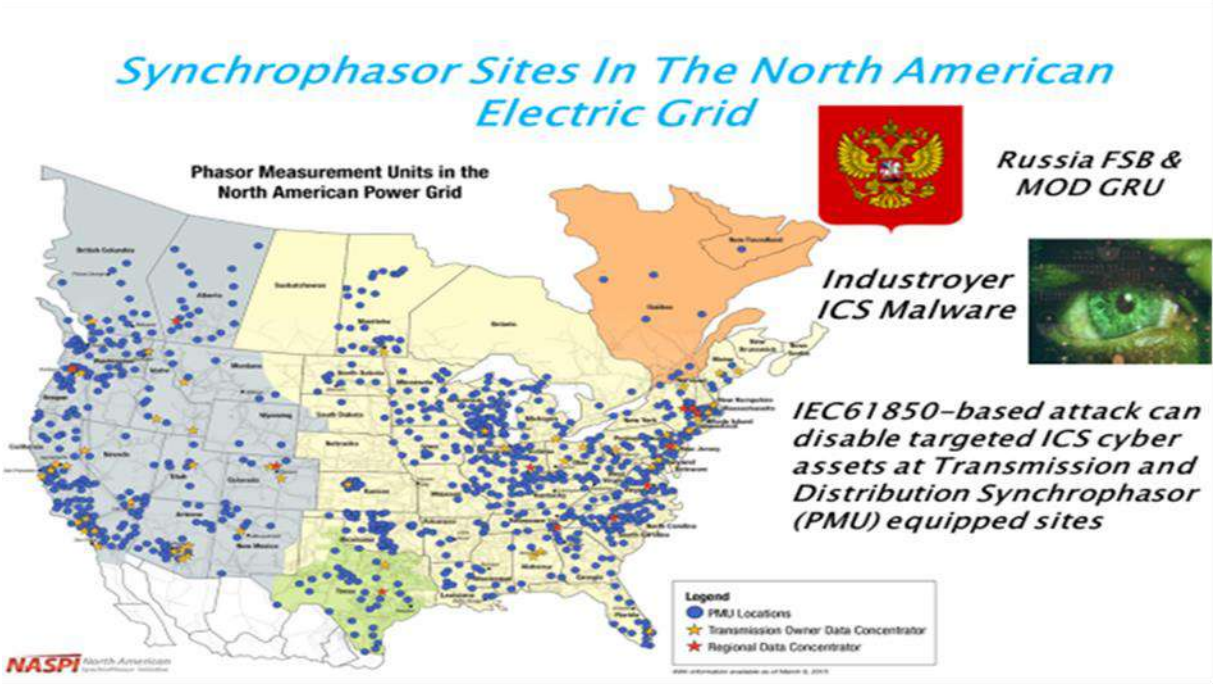
1. Redactions of RC compliance assessments including utility identifications[7] is being challenged, in FOIA cases, but what has remained obscure is NERC's steady attack on any public awareness. While not quite successful in convincing FERC of the need, it has steadily whittled down the process with FERC until it is practically meaningless. Witness what the following chart reveals in the trend to zero compliance:



Courtesy of the Foundation for Resilient Societies

2. Modernization activities often complicate the NERC/FERC cybersecurity regime. Nowhere is this more evident than in the Synchrophasor evolution from utilities' digital data recorder (DDR) systems to capture in real time, power fluctuations for stability maintenance or post-event analysis. In due course, these systems wired together in networks with centers for data processing totally compromises the separation of Transmission systems and Distribution systems, as can be seen on the map that follows. NERC's CIP Standards, or even the other, cybersecurity-unprotected NERC Reliability Standards cannot admit even the existence of these technologies and networks.

[7] Protest and Comments of Michael Mabee, Dockets RM15-4-000, RM16-22-000, RM17-1-000, RD18-4-000, April 10, 2020



Modernization of the electric grid is relentless, examples are in solar and wind power generation and energy storage. And chasing Synchrophasors is a major upgrade in precision measurement, which in combination with machine learning will lead to extensive automation of the overall system.[8] NERC and FERC must realize they are fighting a loosing battle in minimizing cybersecurity protection for the Grid. Indeed, the separation of State authorities from Federal authorities is now being challenged by modernization.

3. Several audits of very large, multi-state utilities have exposed seams in the NERC/FERC regime.

   The Duke Energy audit redacted in a 700+ page NoP[9] reported on 127 separate infractions of CIP Standards. None of these violations applied directly to Duke Energy operations; operations of cyber assets critical to the protection of generation, transmission and distribution of electric power. Further, no unredacted audit of the non-CIP Reliability Standards of Duke Energy linked to these 127 violations could be identified in the NERC audit database. Thus we are asked to believe that all the linkages between **CIP** Standards and **non-CIP** standards, i.e., the cyber assets and cyber systems audited in 127 instances had no critical effect on the cyber assets and

[8] NASPI "Synchronized Measurements and their Application to Distribution Systems, DRAFT, An Update", May 12, 2020

[9] Full Notice of Penalty NP19-4-000 Docket January 25, 2019

cyber systems otherwise described in the **non-CIP** NERC Reliability Standards publication including any cyber assets/cyber systems reflected in the 467 page PRC chart on page 7. The NERC/FERC scheme is simply mind boggllng.

Conversely, the SERC RE **non-CIP** audit of the Tennessee Valley Authority, a Federal Corporation, from 2015-2018[10] revealed a direct connection between a **PRC-001** violation of maintenance and testing of 45000 operational protection devices and **CIP** standards. This was mistakenly cited in the Settlement Agreement. Conveniently, for the auditors, **CIP-002-5(1a)** lists communications and networks as being exempt from **CIP** standards.

Summary and Conclusion

This filing's depiction of the cybersecurity regime that the industry, its ERO (NERC), and FERC created under Federal Power Act, Section 215 tasking, reveals the Act's intention was quite deliberately distorted to insulate, repeat insulate BPS Operations from effective federal cybersecurity controls. A set of Operational Reliability Standards, largely in existence before 2005, was maintained apart from **CIP** standards in the extended 2010-2012 period leading to **CIP v3,** the first FERC-approved cybersecurity standards. Today, they continue to exist separately from **CIP v5/6** cybersecurity standards**.** And an organized coverup of the resultant gaps in overall cybersecurity for the entire North American Grid continues, everything from systematic avoidance of meaningful compliance with the weak **CIP** standards, to enormous payoffs to key Congressional energy committees, a war chest funded by excess profits conveniently provided by padded FERC-approved tariffs.[11]

To extend this conspiracy throughout intervening years, a policy and practice of obscuring the implementation of this regime took several additional forms -- minimization of public knowledge of vulnerabilities, suppression of incident reporting of actual incursions by adversaries, denial of relevant adversary testing of malware abroad, misleading testimony before Congress, and misuse of CEII (Critical Enterprise Infrastructure Information) in sanitization of utility compliance audits. And now underway is promotion of Senate Bill S.3688 to codify misused CEII procedures.

These practices have aided and abetted the threat to hazard the Grid, national elections, and invade social media. The seams in this NERC/FERC regime have widened, an Executive Order complicates procurements and a Congressional Commission is forcing a national deterrence

[10] See Footnote 4.

[11] "***Operator of Power Grid Accused of Overcharging Utility Customers Billions of Dollars***" Tom Johnson | March 17, 2020 | Energy & Environment. Study faults **PJM** Interconnection for inaccurately forecasting energy requirements and sticking utility customers with the costs. **PJM** is the largest U.S. Transmission Operator, 14 States

policy that must defeat S.3688 to be effective. FOIAs and lawsuits are forcing the industry and FERC to greater coverup lengths. As a 60-year veteran of cyber wars, there is not a chance those practices contribute to Security in the National Grid, rather they are efforts to keep federal cybersecurity regulation at arm's length. In fact, and to this experienced cryptologist, the technical and procedural content of the NERC publication ***"Reliability Standards for the Bulk Electric Systems of North America"*** has undoubtedly proven far more valuable to Russia and China than ***all*** of the CEII-protected violation reports, together.

Further, the Commission should really recognize that their practice of "Security Through Obscurity" is causing grave risks to Distribution facilities and local gas, electric firms, and also to the national security facilities, dependent on commercial power. Hopefully, this filing should help the Congress, the federal government, state PUCs, and the public to understand what has been in play. The commission may wish to deny the conclusions of this filing but they would be better advised to actively support the Congressional cyberspace Solarium Commission's efforts to authorize a deterrence policy that would buffer the Grid from attacks and permit a far less costly industry protection regime.

Respectfully Submitted

_____

George R. Cotter

CC:

Director Federal Bureau of Investigation
Chairman, SEC
50 State PUCs
Congressional Cyberspace Solarium Commission
Secretary Department of Energy
Secretary, Department of Defense
Commander, Cyber Command/Director National Security Agency

Document Content(s)