.

193 Southdown Road
Edgewater, MD 21037

grcotter@comcast.net

August 7, 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 3rd Motion to Intervene on Dockets Nos. EL20-46-000, RM20-12-000 and AD20-19-000, all Related to Critical Infrastructure Reliability Standards.

Respectfully,

/s/

George R. Cotter

Enclosure: a/s

UNITED STATES OF AMERICA

BEFORE THE

FEDERAL ENERGY REGULATORY COMMISSION

3rd Motion to Intervene in Dockets)	**(Docket No. EL20-46-000**
Related to Critical Infrastructure)	**(Docket No. AD20-19-000**
Reliability Standards)	**(Docket No. RM20-12-000**

Introduction

A recent joint Cybersecurity Advisory titled ***"NSA and CISA Recommend Immediate Actions to Reduce Exposure Across all Operational Technologies and Control Systems"***[1] described steps to be taken immediately to address risks to critical infrastructures from the nation's adversaries, risks focused on OT and Control Systems known to be vulnerable to malware attacks and held in high priority by the nation's cybersecurity adversaries. **Previous filings on these dockets built the case for the Bulk Electric Systems (BES) being a major example of OT and Control System vulnerabilities since BES cyber assets controlling real time operational power flows are devoid of cybersecurity protections.** Thus, this joint guidance issuance has the BES OT and Control Systems directly in its gunsights, unless of course FERC and NERC attempt to further cloud this reality from the organizations that issued the guidance, the Congress, and the public. This 3rd Motion to Intervene in related FERC dockets is intended to convince FERC and its overseers, the Congress, DOE and DHS, and the Administration to address this self-induced vulnerability, hopefully in parallel with the declaration of a National Deterrence Policy and Strategy that puts the North American Grid off-limits to the nation's adversaries.

Background

Few individuals and even fewer organizations can fathom the complexities of this engineering marvel --the nation's electric system, the complex of thousands of independent and semi-independent utilities that over the past hundred years or more have successfully connected and modernized their generation, transmission and distribution systems. However, it became increasingly difficult to create wide area power flows without developing and agreeing on conformance standards that would produce reliable power service to industry and the public. The reliability standards that work so well today grew out of a half century of collaboration, initially between a few utilities but ultimately through regional and national cooperation and regulation. This of course also required regulation of power markets and controlling tariffs,

[1] NSA and CISA Recommend Immediate Actions to Reduce Exposure Across all Operational Technologies and Control Systems, July 22, 2020

necessarily split between the federal and state levels (power flows arbitrarily labelled "Transmission" and "Distribution" systems, respectively.)

Growth and Grid integration had succeeded well until the major Northeast power outage of 2003, a cascading outage that exposed deep technical and operational flaws in the Grid. The joint US/Canadian study that followed for almost two years resulted in a major rewrite of the Energy Power Act of 2005. Cybersecurity had emerged over the previous decade that raised national concerns on the vulnerability of critical infrastructures including the electric Grid, and Congress added a new section 215 to the EPA that empowered an industry "not for profit" corporation , NERC, as the Electric Reliability Organization (ERO) responsible for developing cybersecurity standards for the Bulk Electric System and the Federal Regulatory Energy Commission for their oversight.

Critical Infrastructure Protection (CIP) Standards

CIP Standards have had a rocky evolution beginning with CIP v1 under FERC Order No. 706 in January 2008, with several iterations leading eventually to a version, CIP v3 formally approved in 2010 under FERC Order No.712. FERC's approval came with directions for further modifications leading to CIP v4 to be followed rapidly with CIP v5. The nearly continuous iteration between the industry, the NERC standards development teams, and FERC occurred throughout. One continuing disconnect was uncertainty over which Cyber systems would be covered by versions of standards. Statistics were publicly revealed for CIP v4; widely variant across eight Reliability Entities.[2] CIP v4 was approved by FERC but never really implemented by NERC. FERC approved CIP v5 in Order 791 on November 22, 2013, the first semi-stable version, but fully 8 years after passage of the EPA. Changes to CIP v5 trickled out but were eventually added to CIP v5 in an expanded CIP v5/v6.

The evolution of CIP Standards occurred out of the public and congressional consciousness but did extensively involve industry leadership, exercising control of the NERC Board of Trustees, a substantial NERC staff with oversight of a succession of standards bodies, and FERC which ultimately had to go through the formalities of public review of standards. Industry positions on contentious issues were strongly supported by active industry organizations, NEI, EPRI, etc.[3] However, cyber vulnerabilities were seldom discussed and threats, almost never. As the Russian Federation began incursions in 2012 (supply chain penetrations) and active attacks in 2014 (with extensive malware testing in the Ukraine in 2015 and 2016),

[2] Characterization of CIP facilities averaged less than 10% for Generator, Transmission and Distribution satisfying the "BES impact within 15 minutes" guidance in CiIP v4, substantially unchanged in transition to CIP v5.

[3] See Tom Aldrich Blog dated Monday, January 1, 2018 "An (Impressionistic) History of NERC CIP". This "history" of CIP evolution provides a capsule (but biased) review of this evolution, a near continuous exercise in futility, a back and forth contest between an industry that viewed cybersecurity regulations as a reversal of federal deregulation, and a Regulatory Commission obviously sensitive to the increasing threat from Russia but lacking the depth and continuity to hold NERC in check.

NERC and FERC showed little inclination to link cyber standards to BES vulnerabilities and Federation threats. An FBI report on the 2014 incursions was never publicly released.

CIP Compliance

CIP standards compliance audits largely by Reliability Entities (RE's) essentially mandated by the EPA but under control of NERC, were slow to emerge. Depending on severity of the infraction, these could range from self-reported by utilities with little or no penalty to lengthy assessments by RE's with financial fines and/or sanctions. NERC's annual, generalized Compliance report to FERC has consistently requested that all compliance reporting be made non-public. FERC has never agreed although succumbing to pressures to substantial weakening of compliance programs and, more critically, substantial redactions in published assessments to hide violations, utility identifications and almost anything that would trace to the violator. The practice is ostensibly to protect information that could be used by an attacker but without documentation of cause and effect, but is more likely intended to protect utilities from liability charges by the SEC, insurance firms, and the public. These practices have been contested by public-spirited individuals and organizations. The industry succeeded in getting some protection written into the FAST Act and has recently succeeded in getting comprehensive support in a proposed Senate Bill (s.3688) dedicated to outlawing FOIA's, regulatory filings, and actions by State PUCs.

Cybersecurity-Related Developments

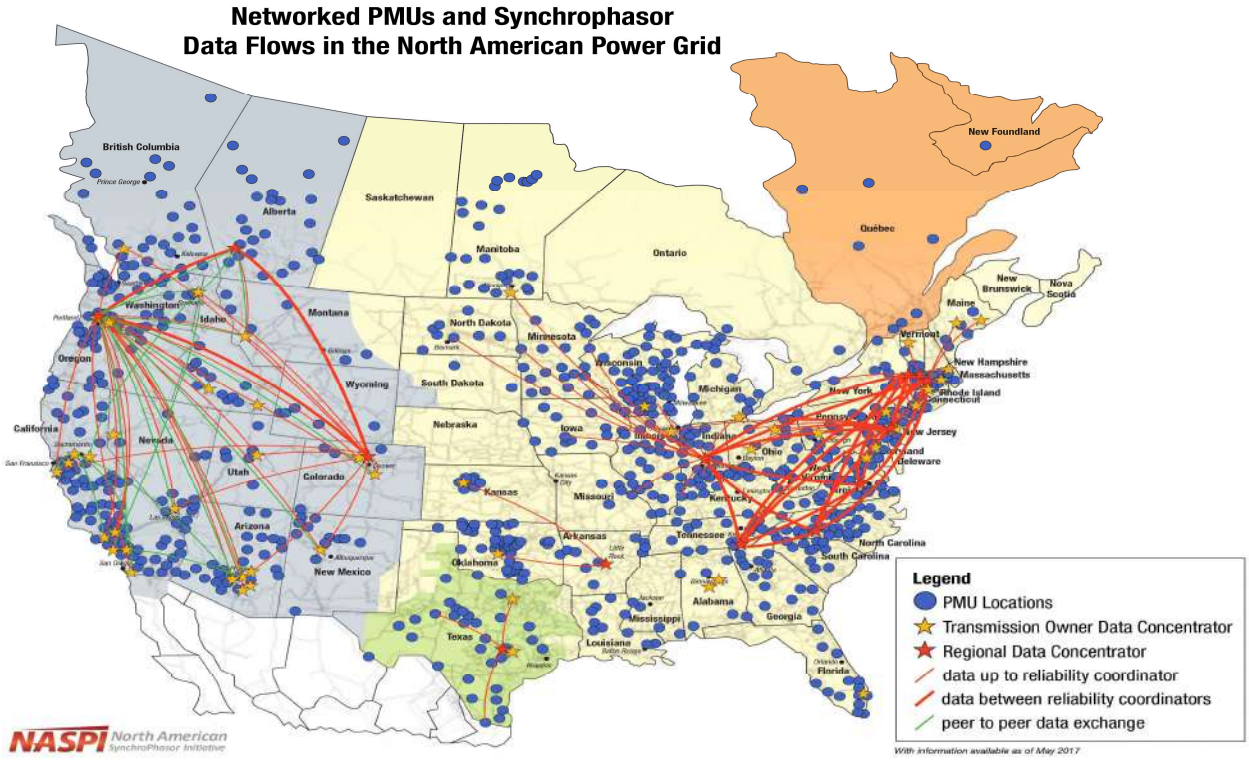
That a disaggregated electric industry has faced many apparently adverse developments over the past two decades[4] that affect implementation of cybersecurity controls will not be debated. These include cybersecurity issues associated with groundbreaking changes in energy sources (solar, wind), nation-wide environmental concerns with pollution from coal and other thermal energy sources, fracking for oil and gas, energy industry economic competition, climate change contentions, threats to the industry from nation/states and criminal groups, and modernization pressures, induced by all of the foregoing.

Among all modernization activities has been the clash between utility independence and utility interdependencies; critical engineering issues arising from the peculiarities of "electricity", its stability, integration pressures that result in lengthening of power flows, and growth and complexity of power demands. Automation of inter-utility systems is a constant concern. Sensors are essential, the trends from analogue to digital controls, data exchanges and the like have increased in complexity. Over several decades the use of digital data recorders (DDRs) to record and manage current, voltage, frequency and phase conditions in power exchanges

[4] This exposition will only address major cybersecurity related developments since the implementation of PD 63 in 1998l

between utilities. They have largely been replaced by "Synchrophasor Systems feeding SCADA systems supporting energy management

There has been an explosion of "Synchrophasor Systems" higher precision instrumentation replacing DDRs. With precise timing system accuracies, these permit wide area coordination of power flows and, in fact, have been useful in resolving wide area "flaws" in generation systems and interconnections. Data collections and their aggregations at processing centers amount to a Synchrophasor explosion, easily seen on the following map, produced by NASPI, an informal association of utility users. These systems are now the principal input to management of Distribution systems across the lower 48.



Synchrophasors and CIP Standards

A reasonable question, therefore, is how does this modernization initiative interface with CIP Standards, since these systems are not only extensively used in the BES but also must be the principal means for controlling operational power flows from Transmission networks to and through, Distribution networks. Strangely, Synchrophasor technologies appear to be totally missing from any description or categorization of BES Cyber Systems. Not a mention, Nil. Well, how are they reflected in the massive NERC Reliability Standards document[5] that contains, in enormous detail, the engineering standards that essentially control the technical interfaces for

[5] NERC Reliability Standards for the North American Bulk Power System, Updated June 23, 2020

all networks, and digital (cyber) devices used to manage operational power flows? A once-over examination of thousands of pages of such standards fails to turn up any references to Synchrophasor systems, although their earlier characterization, DDRs, are prominently featured. Furthermore, the term is also missing from CIP sections of the NERC Reliability Standards document.

There could be only one reason for this anomaly, deliberate suppression of this modernization program. Why? One possible answer is that the industry and NERC did not want any questions raised on how, repeat how, power flows from the CIP-protected BES Cyber Systems into unprotected Distribution networks could be managed? But of course, CIP-002 ***exclusions*** of communications and networks (from the inception of CIP, a profound exclusion mystery) meant that these power flows were not, technically, in conflict with CIP cybersecurity regulations. ***Did this mean that all Grid operational power flows have been deliberately left unprotected by CIP cyber regulations since the passage of the EPA? Regrettably, the answer is yes.***[6]

Further Indications of Deliberate Exclusion from CIP

Did this revelation imply that other CIP Standards or their requirements bypassed (i.e., had no effect) on operational power flows? ***Regrettably, the answer is also yes.*** Engineering (non-CIP) Reliability Standards show no linkages between (1)systems and technologies controlling operational power flows, and (2) CIP Standards. This is extensively documented for both non-CIP Reliability Standards and CIP Standards in my initial Motion to Intervene filing on Docket No. EL20-46-000 dated April 11, 2020. For example, in over 470 pages of technical data on Protection Systems (PRC) summarized in a table on page 8, in that Motion to Intervene. Digital (i.e., cyber) systems show no cybersecurity requirements or CIP references in this extensive tutorial on Protection Systems. And further, while CIP Standard 002 has occasional references to Reliability Standards (such as **PRC**), these references discribe boundary conditions for categorization decisions, not requirements for CIP protection.

One of the major issues complicating application of CIP Standards to operational power flows are important differences between Reliability Entities (example: Balancing Authorities) on some Reliability Standards. As integration of utilities occurred in the early Grid, connectivity needs required agreement on power metrics, e.g, frequency and phase variations in power flows. This of course led to the creation of NERC and Reliability Regions and standardization. Differences between Reliability Entities persist to this day, Balancing Authorities (BAs) must oversee agreed boundary metrics for operational power flows between Reliability Regions. The current issue of NERC's Reliability Standards on **BAL** standards, their calculation, boundary conditions, development history, persistent differences across major interconnections, variances for several

[6] It is important to note that this analysis addresses only regulatory cybersecurity provisions. An individual utility may voluntarily adopt security features such as encryption of data flows, internal access controls over operational data flow cyber assets, etc. Indeed, in 50/50 funding of Synchrophasor implementations, DoE left it to utilities to include or exclude encryption from their grant proposals.

BAs. The current publication exhaustively describes engineering standards in many other categories though also without linkages to cybersecurity requirements. With the multilevel standards approval process – industry, Reliability Entity, SDT, NERC Board of Trustees, FERC NOPR and Final Rule, there are myriad opportunities to consider cybersecurity protection requirements for cyber assets critical to BES operational power flows. For a single albeit major function, what does the record reveal?

Selecting **PRC-006** ***Underfrequency and Undervoltage Load Shedding Performance Standards***, what is documented is the complete history, agreements, uncertainties, discontinuities with other requirements, open issues and FAQs covering the complexities of intentional and unintentional load shedding at generator, transmission, and distribution facilities of the BES. We observe at best, only partial standards for the BES, thus continuing efforts within the WECC, SERC, the NPCC and/or Quebec (interconnections and REs) to achieve standardization on these critical functions. The set of associated Remedial Action Schemes (RAS) are a long way from integration for the BES.

Hence, application of CIP Standards to cyber assets essential to UFLS and UVLS, and by extension to BAL, FAC and other Reliability functions, is clearly unattainable.

Comment: Back in April 2005 with FERC initial approval of many Reliability Standards, the emphasis was on fixing interoperability flaws exposed by the Joint US/Canadian study of the 2003 NE power outage. In that context, cybersecurity requirements understandably took a back seat to other reliability issues. It is now clear that in the interval to 2008 and formalization of CIP v1, the industry, NERC and FERC had only two choices on a CIP structure, (1) sets of Cybersecurity Standards largely developed within Interconnections and perhaps Reliability Regions to permit variances across the BES, a process that continues to this day. Alternatively (2), careful development of BES-wide CIP Standards, deliberately avoiding adding complexity to the unresolved interoperability issues extant, and of course BES operational power flows. Option 2 was chosen, without public exposure or debate. Over the past 15 years, it has therefore been essential that implementation and extension of CIP Standards would not compromise BES real time operational power flows. Over time, this has presented NERC and FERC with additional CIP complications, examples such as communications and network data flows, supply chain vulnerabilities, Internet vendor access, incident reporting. And of course, we see the explosion of Synchrophasor PMUs and related Data Concentrator Centers and networks whose precision technologies addressed the very technical issues inherent in non-CIP engineering standards. CIP compliance audits had to be sanitized as this process continued, foreign adversary threats had to be similarly buried, i.e***., Security through Obscurity***. And today, BES as well as Distribution level operational power flows are largely open and available to these foreign adversaries for malware development and attack planning.

Exclusion of Real Time Power Flow Operations from Non-CIP Compliance Audits

The question naturally arises "How and to what extent are real time power flows addressed in non-CIP Reliability Standards, and therefore in non=CIP Reliability Standards Compliance Audits? For purposes of this Motion to Intervene, an NPCC audit[7] of a reasonable size utility, the Long Island Power Authority conducted on November 28/29, 2017 was examined. No violations of these standards were identified in the audit. At the time of this audit, LIPA was a TOP, TO, DP and TP; responsibilities to be audited. LIPAs area covered most of Long Island. The NYISO was the RC, BA, PA, and lead TOP for LIPA. NPCC identified the non-CIP Reliability Standards in the following Table[8] for this audit:

Table 1: Compliance Audit Scope

Registered Function	Standards	Requirement(s)
TOP	COM-002-4	R1, R5
TOP	EOP-005-2	R1, R6, R9, R12, R13
TOP	EOP-008-1	R2, R4, R5, R6, R7, R8
TOP	EOP-010-1	R3
TOP	EOP-011-1	R1
TOP, TP	FAC-014-2	R2, R4, R5
TOP	PER-005-2	R1, R3, R4
TOP	PRC-001-1.1(ii)	R3, R4, R5
TOP	TOP-001-3	R1, R5, R6, R7, R8, R9, R15, R16, R18, R19
TOP	TOP-002-4	R1, R2, R3, R6
TP	TPL-001-4	R1, R2, R3, R4

The team did not expand the scope of the Compliance Audit beyond what was stated in the notification package.

A comparison of the included standards and requirements against those documented in NERC Reliability Standards was conducted to determine if the audited functions included any cybersecurity-related cyber assets or control functions exclusive to real-time power flows. Observations:

1. All Distribution Provider (i.e., power flow) functions were excluded from the audit.
2. Any applicable standard flagged ***"real-time operations"*** was also omitted from the audit.
3. Requirements labeled as "event reporting", "emergency functions", "system restoration", related training, and similar operational activities were excluded from the audit.

[7] NCR07133 Long Island Power Authority Compliance Audit November 28/29 2017 dated 12/8/2017

[8] A direct comparison was not always possible with time lapses between FERC standard approval and the audit date, also the migration of requirements from one category to another in the NERC Standards process; e.g., COM-001 "no longer enforceable", included in other ways evidently but not trackable.

4. Explicit requirements for actions related in any way to real-time power flow operations, such as authorities to notify in the event of outages, were excluded from the audit.
5. Most importantly, LIPA's responsibilities to other BES authorities critical to real time operations, e.g, Balance Authorities, generator operators for Black Start operations, etc. were excluded from the Audit implying the former were non-operative.
6. Synchrophasor Technologies and related Data Concentrator facilities, real-time operational activities, are totally missing from this audit as well.

The conclusion is therefore inescapable, this audit and assessment not only lacked linkages to Critical Infrastructure Protection (CIP) standards but rigorously avoided any non-CIP Reliability Standard related to "Real-Time Operational Power Flows".

Thus, all BES digital (cyber) systems for any non-CIP Reliability Standards and control center functions have no cybersecurity protections. Further, all Reliability Standards and control center functions critical to real-time operational power flows including Synchrophasor Systems, their Data Processing and Data Flow technologies are also excluded, repeat excluded from compliance audits of utilities.

It therefore appears that cybersecurity protections afforded BES cyber assets apply only to a very thin set of utilities non-operational functions, characterized under CIP-002.

Summary and Conclusion

Except for what an individual utility might voluntarily do for security, most BES digital (cyber) systems have been deliberately excluded from BES cybersecurity protection, including all systems controlling real-time operational power flows. This is not problematical, the massive NERC Reliability (engineering) Standards compilation contains extensive details of cyber (digital) systems utterly devoid of cybersecurity protection. Modernization, such as Synchrophasor Technologies have made it increasingly difficult for NERC and FERC to hide this violation of the intent, and indeed actual wording, of EPA 2005 Section 215.

Had NERC and FERC developed CIP Standards in parallel with non-CIP (engineering) standards, modernizations of Operational Technologies would have included appropriate cyber protections. Systems such as Synchrophasor PMUs, solar and wind generators, Internet and vendor connectivity, Supply Chain Standards etc., would have had to include cybersecurity protection. Incidentally, there is little doubt that insertion of Synchrophasor technologies, particularly software, is delayed in some utilities over fear of conflict with CIP Standards.

Critical Infrastructure Protection standards are simply inconsequential for protection of cyber systems critical to BES operations. In 2008 the objective might have been otherwise, but CIP has become a façade for utility insular management functions, access controls and physical and electronic isolation of facilities. NERC and FERC claims that the CIP Program reduces the risk to the BES are hollow, for in this decade and a half of CIP evolution, we witnessed:

- BES and Distribution systems in open access to the nation's adversaries,
- suppressed reporting of adversary incursions, including critical malware development
- Further efforts spawned by NERC and FERC to obscure vulnerabilities and threats through the Senate Bill s.3688
- unchallenged follow-on adversary malware testing in the Ukraine
- freedom for adversary's cyber forces to employ that same malware in the 2016 election
- increasing risks to Grid-dependent national security facilities and other critical infrastructures.
- Inordinate costs of ineffective cybersecurity protections for the North American Grid.[9]

The joint NSA and DHS/CSIA Advisory cited in the introduction to this Motion to Intervene provides detailed guidance for the protection of Operational Technologies and related Control Centers, in their continuing campaign focused on access to Industrial Control Systems. It emphasizes the immediacy of necessary actions, the widespread internet access to OT systems, endangerment to DoD and National Security Systems, and recently observed adversary actions.

The North American Grid's operational power complexes and networks could be the poster child for this Advisory. Many of its recommendations should certainly be taken seriously by electric utilities. However, the existential threat to US national interests and to Critical Infrastructures requires much, much more, a threat engineered by the industry, NERC and FERC but hidden from public and Congressional consciousness.

Congress and the Administration must implement the Congressional Cyberspace Solarium's 2020 report recommendation with a law invoking a Declaration of National Deterrence Policy with Measured Retaliation, as originally proposed in 2017 by the Defense Science Board.[10]

[9] N.Y. utility, Siemens Energy plan first-of-a-kind cyber hub, Christian Vasquez, E&E News reporter Published: Wednesday, July 29, 2020. The complete IBM report can be downloaded from this reference. Costs per incursion and magnitude are reportedly higher than any other industry.

[10] Department of Defense, Defense Science Board, Task Force on Cyber Deterrence, February, 2017

Document Content(s)