193 Southdown Road
Edgewater, MD 21037

November 18, 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 5th Motion to Intervene on Dockets Nos. EL20-46-000, RM20-12-000, AD20-19-000, and RM18-20-000, 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

5th 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**
	(Docket No. RM18-20-000

November 18, 2020

Introduction

Four prior Motions to Intervene in the above dockets made the solid case that Critical Infrastructure Protection Standards were essentially null and void for Bulk Power Systems Operations, particularly "Real-time Operational Data Flows". Those filings have been ignored by FERC without comment except for taking this filer's threat information completely out of context to support a total block on public access to cybersecurity incidents.[1] This Fifth Motion to Intervene in FERC Orders and White Papers, supplements data and conclusions in earlier Motions and while it may also be ignored by FERC, it most certainly will have to be considered in this filer's complaint to the DoE (and FERC's) Inspector General that FERC and its NERC surrogate have been, and are, in direct violation of Section 215 of the FPAct 2005.

Background

This filer's 4th Motion to Intervene in the cited Dockets was built around a NERC Reliability Standards Compliance filing[2] which clearly revealed the total absence of cybersecurity linkages to CIP Standards, one of a number of similar audits that collectively prove that CIP Standards do not protect BPS Operations, as called for in Section 215, FPAct 2005. CIP Standards from their inception in 2008 provide hygienic defenses only to BPS utilities' administrative and management physical structures that leaves a cybersecurity gap used by utilities to avoid CIP complications in actual operational venues and in major BPS modernization projects. Information from actual cases provided in this, 5th Motion to Intervene, reveal direct couplings between Transmission and Distribution systems in Interconnection Regions that are essential for Grid operations, modernization and reliability, but impossible to justify on CIP Standards grounds. ***The industry has witnessed a substantial growth in Sychrophasor technologies, spurned by***

[1] Section IV A, Footnotes 17 and 20, ENERGY REGULATORY COMMISSION and NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION, SECOND JOINT STAFF WHITE PAPER ON NOTICES OF PENALTY PERTAINING TO VIOLATIONS OF INFRASTRUCTURE PROTECTION RELIABILITY STANDARDS, DOCKET NO. AD19-18-000 September 23, 2020

[2] 4th Motion to Intervene in Dockets Related to Critical Infrastructure Reliability Standards; Dockets Nos. EL20-46-000, AD20-19-000, RM20-12-000, RM18-20-000, September 19, 2020

FERC and NERC, but these trends now show that despite the FPAct 2005's separation of BPS Transmission authorities from State Distribution responsibilities, the delegation of BPS cybersecurity responsibilities to NERC and FERC is now completely muddled by Grid Synchrophasors, (and other modernization efforts.)

Synchrophasors are rapidly increasing in large BPS utilities. They are critical to resolution of forced oscillation events, incidents where oscillations travel hundreds of miles with expanding magnitudes, dangerous to grid operations. Synchrophasors are also increasingly used to control real time Transmission and Distribution power flows where lower grade oscillations must be dealt with rapidly, on-line. What is clear is that modernization imperatives are now dominant with a cosmetic CIP program providing cover for utilities largely able to ignore cybersecurity threats in integration of Transmission and Distribution power flows. ***In this Motion to Intervene, the thrust is heavily on where it is unrealistic to expect utilities to invoke separate CIP controls for the BPS in the handoff of power to Distribution facilities.***

Sample Cases

Dominion Energy

This utility was a 2009 stakeholder in the DoE initial 50/50 funding of Synchrophasor technologies in the Grid, installing its first batch of PMUs in 2012. By 2013 they were committed to install 80 PMUs on their 500kv transmission lines and 12 PMUs on their 230kv lines. This involved 28 transformers and 110 circuit breakers; this illustrates the scope of cyber-related systems in modernized power flows. Dominion added DFRs to the mix to buffer streaming operations and support off-line analytic applications development, a total of 10 "open source" applications for users of these technologies. Note that these facilities are streaming operational data from PMUs and PDCs as a member of PJM transmission operations, a not-for-profit organization consisting of 19 major utilities over 14 eastern interconnection states.

It is difficult to read these developments other than as good news. Case after case reported by Dominion engineers describe successes in resolving fault detections, averaging 87 per year. Importantly, many of these trace to other generators or to non-grid industrial disturbances, high voltage frequency disturbances that are intermodulation products from local non-grid sources. Much is being learned in the process, very much dependent on "real-time operations" across Dominion's Transmission and Distribution systems. Dominion's successes come in large part from outsourcing synchrophasor data processing, storage and retrieval through a vendor to the Amazon Cloud. The cloud trend presents the latest security issues adding to BPS vulnerabilities. CIP ignores vulnerabilities of vendors and Big Data "cloud" systems, of course but Dominion Energy cloud initiatives are continuing. Note that Dominion states that all Synchrophasor data is transmitted on fiber optic cables.

It is perfectly reasonable for Dominion to not fret the failure of FERC in 2008 to integrate CIP and Regional non-CIP Standards, perhaps putting Dominion in technical violation of CIP Standards. Regrettably, these good Dominion Energy experiences are slow to adoption across the nation by FERC/NERC sending Synchrophasors to "Coventry", (a British expression for ridding oneself of unpleasantness). ***Of course, it is a major national security issue that operations of the nation's electricity system remain open to incursions by foreign states' cyber warfare forces.***

California Independent System Operator (CAISO)

Required reading is this filer's 4th Motion to Intervene; the description of a truncated non-CIP compliance audit on this utility that obscures its cybersecurity vulnerabilities. CAISO operates across much of the State of California. The referenced audit lists over 100 CAISO utilities that are Registered Entities in the BPS. As with Dominion Energy, CAISO was an early stakeholder in the Synchrophasor program in the WECC, with hundreds of PMUs and PDCs installed over the past decade. The topology of their systems supports both local Distribution and overall WECC Grid Transmission architectures.

CAISO comprises:

Largest of 37 Balancing Authorities in the West
38 intertie points with neighboring systems
Managing 80% of California load
Representing 30% of the Western Interconnection load.

As an early adopter, by 2015, CAISO had installed over 100 PMU/PDC systems and they contributed to the WECC's efforts in balancing power exchanges across the enormous Western Interconnection. The WECC was also instrumental in early development of PMU applications. CIP Standards were no complication since CIP compliance assessments neatly avoided BPS Operations and Real Time Power Flows. Within CAISO, synchrophasors became a critical, real-time operational asset for several reasons, wind and solar additions to the mix, climate and wildfire tragedies. Sudden outages demanded automatic adjustments driven by metrics which could only be available from advanced technologies, like PMUs/PDCs. Human-originated SCADA data was insufficient for utility control center actions. Control center-to-control center communications systems and their data flows are a major issue in FERC-NERC disputes on CIP Standards.[3]

In this filer's 4th Motion to Intervene[4], a CA ISO non-CIP Reliability Standards Compliance Audit was reviewed. An audit of a major ISO is almost unprecedented and CA ISO had over 100 component utilities so most of its activities would involve real-time power flow management linking BPS assets to Distribution assets across most of the State. Synchrophasor systems are therefore a significant technology in CA ISO's operations. The audit had all the appearances of a "proforma" exercise with no publicly-available results, leading to the conclusion that exposure of the exclusion of its major real-time power flows from Cybersecurity Standards would be revealed.

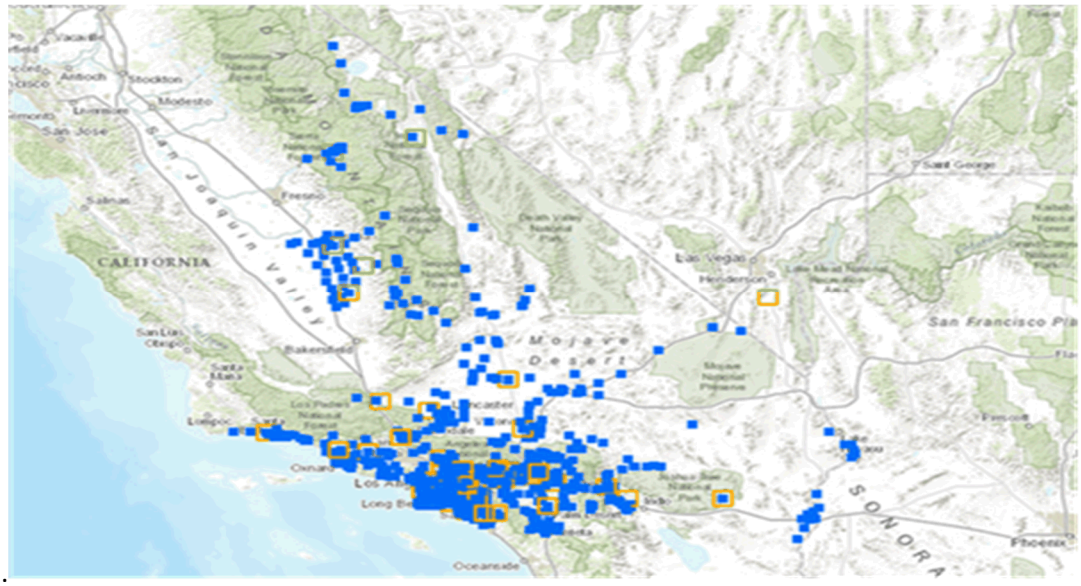
Southern California Edison (SCE)

Examine the following map, can you conceive of 24/7 operations being managed across these substations that can occur without synchrophasors and distributed phasor data centers? Can you

[3] FERC Critical Infrastructure Protection Reliability Standard CIP-012-1 – Cyber Security – Communications between Control Centers, Docket No. RM18-20-000; ORDER NO. 866 (Issued January 23, 2020)
[4] See Footnote 2

conceive of CIP Standards providing effective cybersecurity protections to BPS operations separately from local power distribution, in the Los Angeles Basin? SCE has prioritized the automation of power operations in its region, operating over 100 PMUs and PDCs. It has described this evolution in a paper delivered at a 2017 workshop[5] --"***Phasor measurement units (PMUs) are an important tool for monitoring electrical transmission networks. They provide time-synchronized measurements continuously streamed at configurable rates through use of the IEEE C37.118 protocol. These measurements are aggregated at control centers and allow for convenient real-time analysis and visualization of systems…… These data are used for real-time trending and historical analysis. This system generates more than three million data points per minute and more than six terabytes of data per year. With so many data points, manual analysis is impractical.***"

Substations, Southern California Edison (SCE) Service Area, California



.

ISO-New England

ISO-NE was one of the first adopters of synchrophasor technologies. They are in use, operationally, in ISO-NE's management of Generation and Transmission efforts across NE and cooperatively with Canadian provinces. The ISO recently reported all 345Kv facilities were PMU equipped and it would upgrade from 227 PMUs currently to over 300 by 2024. Using GE's Phasor Point Wide Area Management System, the ISO provides PMU-based protection including automatic relay protection for short circuit faults and locating faults, all for situational awareness across the ISO's footprint.[6] The data is inserted in SCADA streams to EMS and broadcast to ISO operational utilities via Email, soon to be replaced by EMS "Alarms".

[5] Presented at the 20th Annual Georgia Tech Fault and Disturbance Analysis Conference, Atlanta, Georgia May 1–2, 2017

[6] See 3rd Motion to Intervene, Related to Critical Infrastructure Reliability Standards - Docket Nos. EL20-46-000, No. AD20-19-000, RM20-12-000, August 7, 2020

The ISO also developed, at an early point, its Oscillation Source Location applications, aimed at the grid-wide forced oscillation problem. It is fully automated and uses all PMUs in ISO-NE footprint to identify the phenomena inside or outside it's control area. PMU data from the NYISO and PJM is also available at the ISO. It has identified and located dangerous forced oscillations hundreds of miles outside its footprint.

Thus, ISO-NE, despite its serious energy deficiencies, functions as a well-modernized operator including operational use of synchrophasors in real-time support to its utility members. As long as "Real-Time Power Flows" fall in the crack between non-CIP Reliability Standards and CIP Standards, ISO-NE has no mandatory cybersecurity protections to worry about.

Bonneville Power Administration (BPA)

As a key member of the WECC, BPA was an charter member of the NASPI effort, using DoE grants to acquire synchrophasor technologies. It has maintained a two-vector program, real-time controls and R&D, with careful attention to encryption of data streams and access controls. It is currently reportedly operating 77 PMU "pairs" at 54 sites for real-time power operations and 32 "pairs" of PMUs at 23 sites for post-event off-line analysis. BPA admits that the latter get a lower grade of security protection (otherwise undefined).

Since it is a federal corporation, BPA has been careful to meet the cybersecurity standards of multiple oversight organizations but it undoubtedly aware of the digital divide built into the CIP Program. Conforming to CIP Standards quite readily permits BPA to operate its real-time power flow systems with its own, more comprehensive cybersecurity program; protecting the interconnections between Generation, Transmission and Distribution networks while taking maximum advantage of sychrophasor systems, efficiency and reliability.

Note, BPA is considering joining the Western Energy Imbalance Market (EIM), operated by the California Independent System Operator (CAISO). It is important to note that the Western EIM is not a regional transmission operator. BPA is not joining an RTO. BPA would preserve its autonomy and retain authority over transmission planning, day-ahead marketing, and transmission system and balancing authority operations if it were to join the EIM. The EIM aims to create a market for power based on a goal of 5 minute adjustment in supply and demand. PMU's would be critical to BPA's role in managing such a market.

Tennessee Valley Authority

TVA's entry into Synchrophasor technologies occurred as early as 2004, prior to introduction of CIP Standards. Up until 2013, TVA was a supported NERC functionary in development of PMU and PDC applications, serving the linkage role for technology transfer to vendors. Among those initiatives was the creation of the Grid Protection Alliance, an industry/utility not-for-profit organization responsible ultimately for a raft of PMU and PDC applications. TVA also was the NASPIl host for PMU data as the

"SuperPDC" through at least 2013 when NERC contracted with Electric Power Group to assume that function.

TVA has kept a low profile on implementation of synchrophasor systems into its generation, transmission and distribution facilities. It is undoubtedly aware of the cybersecurity gap on real-time operations which involve handoff of power to six other states. As a federal corporation, TVA believes it must satisfy oversight by its own IG, the NRC, FERC/NERC, OMB/NIST, GAO and increasingly, the Security Exchange Commission. TVA created a 24/7 Cybersecurity Center to monitor all of its networks to keep itself secure, and undoubtedly gives high attention to cybersecurity compliance in the Generation-Transmission-Distribution digital divide.

Forced Oscillation Event, January 11, 2019

No single event characterizes the importance of synchrophasor installations in the electric industry better than a forced oscillation occurrence on January 11, 2019 in the Eastern Interconnection of the BPS. ***No single event*** characterizes the importance of resolution of critical differences between the six remaining interconnections in non-CIP Reliability (engineering) Standards than this multi-interconnection event. No ***single event*** characterizes the importance of integrating Transmission and Distribution operational networks controlling real-time power flows than the NERC report[7] on this incident.

An 18-minute duration Forced Oscillation Event on January 11, 2019 affected the entire Eastern Interconnection before it was cut off at the source, a steam turbine in a Georgia utility. Because of a parallel failure of the Reliability Coordination network in play, the RCs were blindsided on the source. Fortunately, PMUs across the region were instantly affected and utilities with advanced PMU applications were able to recognize its effect on their systems. What started out as a .25Hz perturbation was magnified to a 200Mw peak, 50Mw as far away as NYISO and ISO-NE. SCADA data in various EMS reflected the event but could not resolve the system or location.

Forced oscillation events are most often traced to malfunctioning or poorly maintained generators. This was a signature event since, for 18 minutes across the entire eastern US, the unexplained risk to the overall Grid was significant. The NERC report does not address this issue, nor does it call attention to the overall importance of PMUs in controlling power flows, and therefore their criticality to ***Security of the North American Grid.***

[7] NERC Report, "Eastern Interconnection Oscillation Disturbance, January 11, 2019 Forced Oscillation Event," December 2019

Summary

With the passage of FPAct2005 and designation of NERC as the ERO, FERC was faced with a dilemma; creation of nationwide cybersecurity standards for the Bulk Power System while the industry was still technically unconnected with 8 Reliability Regions operating semi-autonomously, regulated independently on separate engineering standards. ***Cybersecurity Standards should parallel and intersect with existing Reliability Standards*** but that would require delegation of cybersecurity responsibility to 8 regions and their independent certification boards. FERC chose to honor the regional control in existence and construct a CIP strategy that would not conflict with individual utility operations in the BPS.

The slippery slope that resulted was the certainty that major engineering modernization developments by utilities had to be avoided in the CIP Standards evolution. Synchrophasors, Point on Wave, Solar, Wind Turbine, Cloud/IoT, inevitably 5G developments must be accommodated to some extent in NERC non-CIP Reliability Standards but collectively slow down the resolution of regional engineering variances. Note the extreme difficulty in creation of CIP Standards for Supply Chain vulnerabilities and also of note, the decades-long NERC/FERC disagreement on Control Center-to-Control Center networking and data exchange.

The previous four Motions to Intervene[8] in recent CIP-related Dockets conclusively documented the decade-long violations of Section 215 FPAct 2005 by NERC (as the ERO) and FERC. This Motion-to-Intervene addresses major utilities' adjustment to modernization and CIP Standards dynamics, focused mainly on Synchrophasor systems contributions to real-time operations and overall health of the Grid with evidence from filings, reports, workshops and conferences. Citation of CIP Standards is extremely rare.[9] However, utilities' security posture on communications and networks, firewalls, access controls will be observed. What stands out in most of these cases is the willingness of utilities to directly couple generation, transmission and distribution power systems controlled and managed with PMUs and attached and distributed PDCs.

That merger is irreversible. *Reconciliation of the security and operational conflicts reflected in these sample cases, and unaddressed of course in the NERC December 2019 Oscillation event report, presents an apparently insurmountable challenge across the 50 states. However, the violation of Section 215 of the FPAct 2005 falls on FERC and NERC. utilities are operating in conformance of NERC's* ***non-CIP*** *Reliability Standards and FERC's* **CIP** *Orders as they exist.* Most major utilities realize that unprotected BPS power flows to critical infrastructures, including nuclear generation sites and national security facilities in 48 states are at risk and *most* take standard security precautions. Regrettably, cyber defense against the Russian Federation is not the sum of separate utility security practices.

[8] FERC Supply Chain Risk Management Reliability Standards, Docket No. RM17-13-000; Order No. 850, (Issued October 18, 2018) prompted this filer's initial Motion to Intervene in Docket No. EL20-46-000 Related to Critical Infrastructure Supply Chain Reliability Standards Submitted to FERC on June 11, 2020

[9] A few large utilities obliquely citing CIP Standards play the FERC/NERC game of "Let's Pretend".

Conclusion

FERC's silence on this fundamental risk to Grid survivability may simply indicate it sees no way out of the jam it created, except to press for legislative ***"Security through Obscurity"*** (i.e., s3688). A National Deterrence policy is essential to simplify protection for the electric grid. The Congressional Cyberspace Solarium Commission study recommended this but its efforts to get agreement through the outgoing Congress bogged down. ***With over 1500 Registered Entities just in the BPS, years away from a fully-connected national generation, transmission and distribution system (actually delaying modernization), and too large and disaggregated to effectively manage cybersecurity on behalf of the entire industry, a new Administration needs to put up effective barriers to its nation/state adversaries.***

DoD and the National Security Community have demonstrated competency in thwarting the nation's adversaries in cyberwarfare against our infrastructures. The Power Industry behind a deterrence ***red-line*** can substantially cut costs. Rate payers must inevitably defray cybersecurity costs but the unfettered practice by FERC of hiding those costs in tariffs must end. The FERC efforts to permit utilities to recover voluntary cybersecurity-related expenses in FERC Docket Nr. AD20-19-000 should be blocked until a National Deterrence Policy is declared. Hopefully a new Administration will understand that a stated deterrence policy will permit this nation to negotiate international support for collective efforts against international criminal cyberattacks.

/s/

George R. Cotter
grcotter@comcast.net

CC:
DoE Inspector General
President-Elect Transition Team
Cyberspace Solarium Commission
Secretary of Defense
Secretary of Energy

Document Content(s)