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

June 25, 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 2nd Motion to Intervene on Dockets Nos. EL20-46-000, RM20-12-000 and AD20-19-000, all Related to Critical Infrastructure Reliability Standards.

Respectfully,

George R. Cotter

Enclosure: a/s

UNITED STATES OF AMERICA

BEFORE THE

FEDERAL ENERGY REGULATORY COMMISSION

2nd 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

The FERC Staff White Paper[1], Docket No. AD20-19-000 asserts ***"In general, NERC recognizes the BES to include all Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher."*** And it further states ***"The electric transmission grid has many components that are vulnerable to cyber-attacks, and a cyber-attack against high voltage transformers or other large equipment used to support transformer functions can have a large impact on the transmission system."*** Warnings such as these are standard fare when linked to proposed increases in tariffs but actually are hollow when examined in parallel with current BES cybersecurity practices as documented in this filer's first Motion to Intervene[2] in Docket No. EL-46-000.

Discussion

The CIP Standard 002-5.1a may require the ***cataloging*** of cyber assets as BES cyber systems if satisfying certain time and metric BES risk requirements, but the wealth of evidence in my prior ***Motion to Intervene*** on Docket EL20-46-000 shows that grid ***Operations*** do not enjoy cybersecurity controls for the type assets cited above. Is this a scheme to reward utilities with higher user-funded tariffs without any significant improvement in BES cybersecurity? If not, they kindly explain how masses of **BAL, IRO, PRC** etc. reliability requirements in NERC's January 2020 update can be safely used, **Operationally**, without a semblance of cybersecurity controls that would also be required.

Please spare this filer and the public, any assertion that CIP standards do apply. Major, detailed linkages to and among the Cyber Assets listed in the NERC Reliability Standards[3] document would be critical to such a claim. Furthermore, CIP Standards subordinate to CIP-002-5 bear no relation to what would be needed for linkages to the excluded ***Operational*** Reliability Requirements. That NERC document does contain many examples of critical communications

[1] CYBERSECURITY INCENTIVES POLICY WHITE PAPER, June 18, 2020 Docket No. AD20-19-000

[2] George R. Cotter, Motion to Intervene, April 11, 2020 Docket No. EL-46-000

[3] NERC Reliability Standards for the Bulk Electric Systems of North America, Updated January 2020

and network linkages to facilitate ***Operational*** data exchange and coordination efforts which of course explains NERC's successful effort in early CIP days in ***excluding*** communications and networks from CIP Standards. Linkages such as these would have required substantial changes to the follow-on CIP Standards to address ***Operational*** factors, complications that NERC was anxious to avoid.

As an example, NERC must explain how CIP Standards ***fail to apply*** in the TVA Compliance Audit NP19-14-000 involving PRC-005-1b violations?

As another test, NERC must examine the attached summary of CIP standards violations extracted from the heavily-redacted Duke Energy compliance audit 2015-2018, Docket NP19-4-000[4] and address the question: ***Where is the comparable SERC RE audit of Duke Energy's performance on PRC-005-1b, similar to the TVA audit, occurring at the same time.*** There were 127 Duke Energy violations attributed to the listed CIP standards, violations that are management, security process, access, configuration management and other facility hygienic controls. Not one of these 127 violations had a semblance of linkage to Duke Energy ***Operational*** activities, i.e., the 24/7 control of power movement from Generation facilities through Duke Energy Transmission systems to Distribution systems to client-serving utilities.

These are just two of hundreds of cases of apparently unprotected BES ***Operational*** functions involving a myriad of BES cyber assets and cyber systems. Of course, FERC could claim that there was never any intention to apply CIP Standards to ***Operationally***-critical assets/systems; the functions embodied in CIP Standards were sufficient to cyber-protect such ***Operational*** functions. That would be virtually impossible given the extensive unprotected exposure of cyber assets reflected in the NERC compendium and direct vendor access to such cyber assets. Indeed, the BES is paying a real risk in its exclusion of communications and networks from CIP-002-5.1a.

Open Questions on Staff White Paper, Docket No. AD20-19-000

The bottom line here is that the Staff White Paper cannot be fully assessed unless and until FERC addresses the following issues:

1. What percentage of BES generation, transmission and associated Distribution ***facilities*** are covered and not covered by CIP Standards? (No CEII protestations, please.)
2. Can FERC or NERC Identify the actual cybersecurity controls applied to non-CIP Reliability Standard cyber assets in NERC's Reliability Standards document update, January 2020? (No CEII protestations, please.)
3. How does the Staff White Paper propose to apply voluntary cybersecurity measures to utilities involved in the hybrid Transmission/Distribution Synchrophasor networks? See Appendix 2.

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

4. Are the NIST options limited to the NIST ***Framework*** or do they extend to NIST ***Standards***, (SP800-53v5)? Note BES Federal Corporations employ a mixture of NIST Standards, NERC (non-CIP) Regulatory Standards, and CIP Standards.
5. Are the proposed tariff options actually meant to cover ***Operationa***l cybersecurity costs incurred voluntarily by utilities but not approved by the 50 states since such costs lack coverage by CIP Standards?

Open Questions on the FERC Notice of Inquiry, Docket No. RM20-12-000

1. Although stated as a product of a FERC Staff study of CIP gaps compared with the NIST Framework, do the inquiries reflect a NERC effort to extend CIP Standards to justify in part, tariff options to cover cybersecurity costs voluntarily adopted by BES utilities? An example would be the impressive TVA Chattanooga 24/7 cybersecurity center, and other TVA costs of voluntary cybersecurity initiatives.
2. What jurisdictional conflicts exist between FERC, the NRC and individual states on the cybersecurity responsibility for protection of the hybrid Synchrophasor complex depicted in the map in Appendix 2? Note that the NERC/NRC agreement on off-site power supply to nuclear sites is seriously in need of replacement, in view of reported Russian Federation reconnaissance of such facilities.
3. Given the hint of potential use of NIST Standards,[5] not merely the Framework, should FERC "inquire" whether voluntary adoption of NIST Standards should be a BES utility option after formal declaration of a National Deterrence Policy?

Summary and Conclusions

CIP Standards have been described by this filer for years as a "House of Cards". They have served only to narrowly protect a utility's "House" and not its ***"Operations***". Although BES cyber assets are defined as affecting BES "***Operations***"[6], huge exceptions in NERC's Reliability Standards render the definition moot. It appears certain to this filer that there is no reasonable explanation for the deliberate exclusion of ***Operational*** systems cyber assets from cybersecurity standards; a profound obligation levied on NERC and FERC under EPA amendments in 2005. While this may appear to have been necessary in 2008 for an industry of approximately 1400 independent "Registered Entities", determination to maintain industry control of regulatory activities apparently predominates. This, in combination with industry and regulator combined efforts to obscure attacks and cover-up compliance failures e.g., CEII, has given our nation/state

[5] NIST SP800-53a Rev5. *"This publication provides a catalog of security and privacy controls for federal informationsystems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, natural disasters, structural failures, human errors, and privacy risks."*

[6] NERC defines BES CyberAsset as a "Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System."

adversaries over a decade's advantage in cyber warfare capabilities, with the nation's recovery being very uncertain.

It thus appears next to impossible at this late date to develop cybersecurity standards to envelop BES, Distribution and Nuclear ***Operational*** activities, sufficient to deter nation/state cyber offenders. This was the conclusion of the DoD Scientific Advisory Board[7] in their 2017 recommendation for a National Deterrence Policy; reaffirmed as the primary recommendation of the recent Congressional Cyberspace Solarium Commission report.[8]

Raising the ante for ratepayers as proposed in the FERC Staff White Paper is not something Congress should permit, with regulatory cybersecurity malfeasance slowly leaking out of the 2005 EPA. And tinkering with CIP Standards will continue to leave major Grid ***Operational*** systems unprotected. Rather, the Senate and House Energy Committees should rapidly endorse the CSC Deterrence recommendations and order a total industry reset to much simpler and less costly cybersecurity controls, safely ensconced behind a National Deterrence Policy announcement and U.S. Military retaliation for threats to America's critical civil infrastructures.

Attachments:

Appendix 1: Summary of Duke Energy Compliance Violations
Appendix 2: Synchrophasor Sites in the North American Electric Grid

Respectfully Submitted,

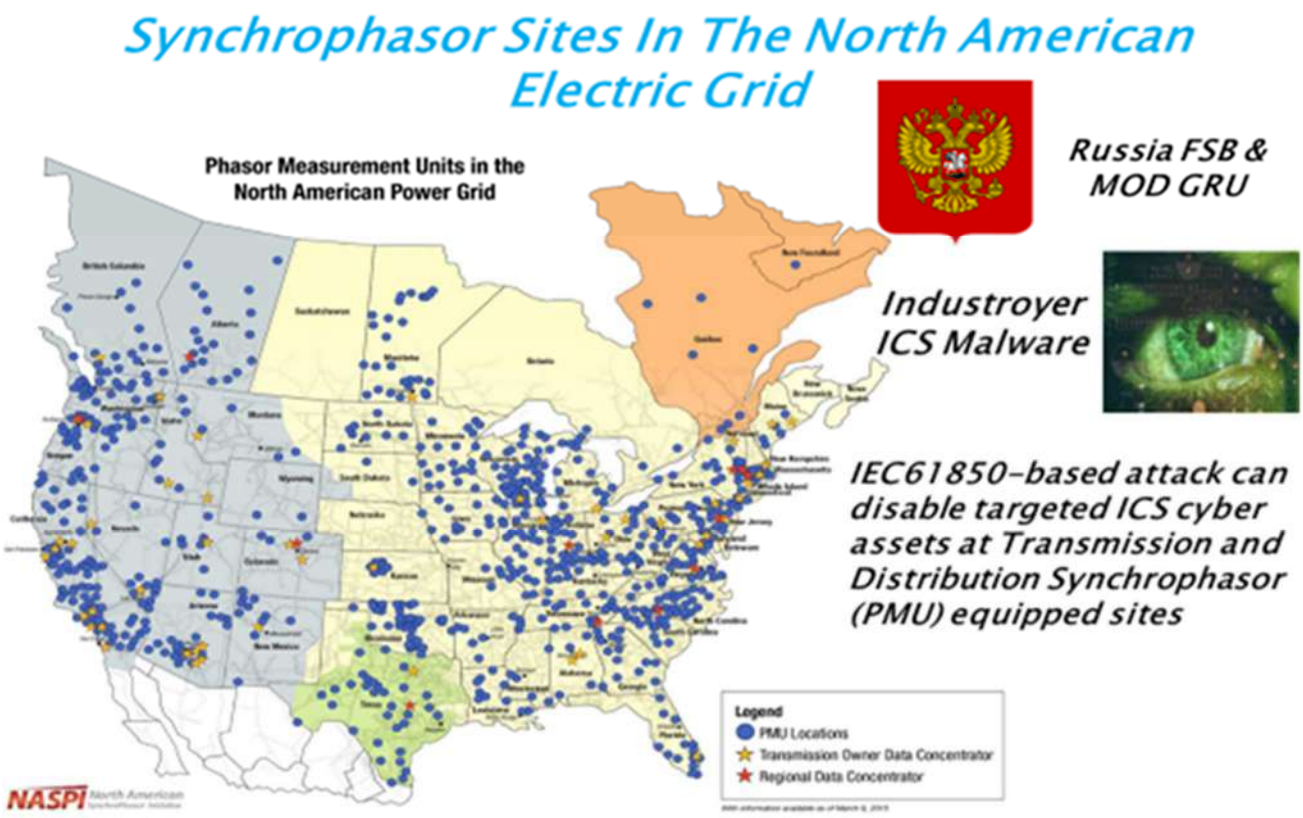
George R. Cotter

[7] DoD DSB Task Force on Cyber Deterrence, February 2017
[8] Congressional Cyberspace Symposium Report, March 2020

Summary of Duke Energy Compliance Violations Appendix 1.

002-5.1a R1 – Categorization of Cyber Assets
003-3 R4 – Protection of Critical Cyber Information
003-4 R6 – Configuration Management
004-3a R4 – Revocation of Access Rights
004-6 R4 – Unescorted Physical Access
004-6 R5 – Revocation of Unescorted Physical Access
004-3a R2 - Cybersecurity Training
004-6 R2 – Electronic Access before Training
005-1 (and 3a) R1 – Protection of non-critical Cyber Asset in ESP
005-5 R1 – Deny Access by Default Rules not Posted
005-3a R2 – Organizational Mechanisms for Electronic Access
005-5 R2 – Interactive Remote Access not thru Intermediate System
006-3c R1 – Maintenance of 6 wall PSP after Upgrade
006-6 R1 – Physical access controls for Unescorted access to PSP
006-3c R2 – PACS user accounts for access permissions
006-6 R2 – Continuous escorting within PSP
006-3c R4 – Controls to manage access to PSP
006-3c R5 – Immediate Review of Unauthorized Access to PSP
007-6 R1 – Enabling logical network accessible ports
007-3a R3 – Failure to access security patches within 30 days
007-6 R3 – Methods to deter, detect, prevent malicious code
007-6 R4 – Security event monitoring
007-3a R5 – Sharing user name, password to access devices
007-6 R5 – System access controls to Cas withing ESPs
007-3a R6 – Security monitoring controls for automated or manual alerts
007-3a R7 – Chain of custody process on device removal
007-3a R8 – Cyber vulnerability assessment action plan
007-3a R9 – Documentation of modifications to ESP systems and Controls within 30 days
009 6 R2 – Failure to include EACMSs in testing of Recovery Plan
009-6 R3 – Inclusion of EACMS in reviews and updates of Recovery Plan
010-2 R1 – Maintenance of accurate baseline configuration
010 2 R2 – Monitoring changes to Baseline configurations once every 35 days
010-2 R3 – Active vulnerability assessment of PCA before deployment
010-2 R4 – Implementation of documented plans for Transient Cyber Assets
011-2 R2 – Protection of BES Cyber System Information
011-2 R2 – Protection of BSCI iaw Information Protection Program
014-2 R1 – Removal Error in Risk Assessment

Appendix 2.



Notes:

1. Courtesy of NASPI web site, 2017 version.
2. Threat annotations are the authors.
3. A larger scale version of this map would show communications and network linkages and a clearer depiction of Transmission and Regional Data Center Concentrator Sites.
4. No effort is made to depict Transmission Facilities separately from Distribution Sites.

Document Content(s)