UNITED STATES OF AMERICA BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Complaint of Michael Mabee and Petition to Order Mandatory Reliability Standards. for Equipment and Monitoring Systems Marketed from the People's Republic of China	))))	Docket No. EL21-99-000

INITIAL COMMENTS OF DAVID JONAS BARDIN
September 6, 2021

These Initial Comments respond to the NOTICE OF COMPLAINT dated August 31, 2021, which sets a deadline of September 15 at 5:00 pm ET for Comments and Motions to Intervene.. [*Federal Register*, Vol. 86, No. 170 Page 50104; https://www.govinfo.gov/content/pkg/FR-2021-09-07/pdf/2021-19206.pdf]

Mr. Mabee (hereinafter COMPLAINANT) has posted his Complaint and Petition at https://michaelmabee.info/chinese-transformer-complaint-filed-with-u-s-government/ .

I hope these early Initial Comments will help and stimulate others to submit comments of importance to the Commission's unique statutory duties, to national safety and security, to the electric utility industry, and to people, businesses, institutions, and other industries which the electric utility industry serves.

My background

My professional background includes 11 years as a civil servant at the Federal Power Commission, FERC's predecessor (rising to Deputy General Counsel); State cabinet service as New Jersey's second Commissioner of Environmental Protection (including Governor's alternate on Delaware River Basin Commission); Presidential, Senate-confirmed appointments when FERC and the Department of Energy were created and got started (as Deputy Administrator of the Federal Energy Administration and Administrator of the Economic Regulatory Administration).

Opportunities

The Commission (as well as NERC [see **appended acronym list**]) has an opportunity to use this Complaint and Petition proceeding — Docket No. EL21-99-000 — to clarify, investigate, and resolve regulatory and supply chain cybersecurity issues.

The Commission also has an opportunity to try to win public confidence, by disclosing enough basic information to win public support (without compromising secrets which our adversaries don't know).

Does the People's Republic of China have the capability to shut down our power grid?

COMPLAINANT states that "On June 6, 2021 Secretary of Energy Jennifer Granholm confirmed in a CNN interview that U.S. adversaries have the capability to shut down our power grid." Footnoted link [[4] See https://www.cnn.com/2021/06/06/politics/us-power-grid-jennifer-granholm-cnntv/index.html] literally confirms that general statement, but does not mention China specifically. (This docket is about COMPLAINANT's concerns regarding Chinese-marketed electric power transformers, monitoring systems, and the like.) Yet Secretary Granholm disclosed a grievous problem to the public at large without giving away any secrets to our adversaries. Her careful words might help win public confidence and support. So far as I can tell, neither FERC nor NERC has done the equivalent. I believe they should. If they deem themselves incapable of carefully constructed, limited public disclosures, they should ask the Energy or Homeland Security Department, the FBI, or the ODNI to assume that task.

In any event, the four FERC Commissioners now in office need to be briefed confidentially in order to understand the context and urgency of carrying out the Commission's unique Section 215 responsibilities.

Related References

My list of **References**, below, includes two which I respectfully call to the FERC Commissioners' unfiltered attention:

A blog posted last week by Joseph Weiss, PE, CISM, CRISC, ISA Fellow, IEEE Senior Member (Managing Partner of Applied Control Solutions): "**Do the Chinese "own" our electric grids and other infrastructures?**" 8/27/2021 [posted at https://www.controlglobal.com/blogs/unfettered/do-the-chinese-own-our-electric-grids-and-other-infrastructures/] raises issues going to context and urgency of carrying out FERC's unique Section 215 responsibilities.

The Commission should also consider how FERC actions or inactions could strengthen or weaken the USA in "Information Warfare"; see Paul N. Stockton, August 2021, in **References**, below, at page vii:

> "US policymakers should also prepare for the risk that adversaries will carry out their threats to inflict suffering on the American population. If the president stands firm against coercive IOs, China and Russia may strike the power grid or other US targets to (1) magnify public fears and raise the perceived costs of defending US allies and (2) reinforce the cognitive impact of those attacks with warnings that more devastation will follow unless the president caves in."

Sources

On August 31 (thanks to NERC's Board of Trustees Chairman DeFontes Jr.), I conferred with
— Mark G. Lauby, NERC Senior VP & Chief Reliability Officer,
— Howard Gugel, NERC VP Engineering & Standards, and
— Fritz Hirst, NERC Director of Legislative and Regulatory Affairs. They shared relevant information, took my unresolved questions under advisement, and have since answered some of my questions.

Before and after August 31, I also conferred with George R. Cotter, Joseph Weiss, COMPLAINANT, and others, receiving some relevant information and raising some as yet unresolved questions

COMPLAINANT states [footnote omitted]:

"I am filing this complaint under 16 U.S. Code § 824o(d)(5)[1] because:

- Entities in the U.S. Bulk Power System (BPS) as well as the overall U.S. electric grid are buying critical equipment from the People's Republic of China to install into our critical electric infrastructure that the Communist regime's state sponsored and state supported hackers are already probing and attacking.
- There is no requirement that existing Chinese equipment or systems already installed in the electric grid be checked and tested for risks and vulnerabilities.
- There is no requirement that newly imported Chinese equipment or systems be checked and tested for risks and vulnerabilities before being installed on the electric grid

"**Request for Investigation**
I request [FERC to] issue a public notice ... pursuant to 18 CFR § 385.206(d), investigate this Complaint and issue an appropriate order to the [ERO] to strengthen the security of the bulk power system**.**
. . .
"**Relief Sought**

1. The ... Commission should direct the North American Electric Reliability Corporation (NERC) to conduct a comprehensive survey of all registered entities in the Bulk Power System to determine what Chinese equipment or systems are currently in use in the Bulk Power System.

2. The ... Commission should direct ... (NERC) to submit to the Commission a proposed reliability standard for testing and security of Chinese equipment or systems [which] are currently in use in the Bulk Power System or purchased for future use.
3. The ... Commission should work with all State Public Utility Commissions to encourage adoption of the reliability standard promulgated as a result of #2 above (or a state equivalent standard) for the protection of generation and distribution portions of the electric grid under state jurisdiction."

NERC's 2020 confidential Alert and survey

On August 31 I learned of a relevant 2020 NERC Alert and survey of responsible entities. See "NERC Issues Level 2 Supply Chain Alert | 2020-07-09 | RTO Insider" [see https://www.rtoinsider.com/articles/19115-nerc-issues-level-2-supply-chain-alert]. Mr. Lauby advises: "This Alert is confidential due to the nature of the threat and recommendations, as well as the rolled-up report that is provided to FERC." He amplifies: "This report is submitted only to FERC and other Applicable Governmental Authorities. Per section 810 of NERC's Rules of Procedure:

> NERC will advise the Commission and other Applicable Governmental Authorities of its intent to issue all Level 1 (Advisories), Level 2 (Recommendations), and Level 3 (Essential Actions) at least five (5) business days prior to issuance, unless extraordinary circumstances exist that warrant issuance less than five (5) business days after such advice. NERC will file a report with the Commission and other Applicable Governmental Authorities no later than thirty (30) days following the date by which NERC has requested the Bulk Power System owners, operators, and users to which a Level 2 (Recommendation) or Level 3 (Essential Action) issuance applies to provide reports of actions taken in response to the notification. NERC's report to the Commission and other Applicable Governmental Authorities will describe the actions taken by the relevant owners, operators, and users of the Bulk Power System and the success of such actions taken in correcting any vulnerability or deficiency that was the subject of the notification, with appropriate protection for Confidential Information or Critical Energy Infrastructure Information."

Mr. Lauby, in response to my question whether NERC shared its confidential Alert with Alaska and Hawaii (and referring to President Trump's Executive Order 13920 of May 1, 2020), further observes: "The Executive Order (EO) was a public document. The Alert asked industry how much of the EO identified equipment was on their system. The EO was available to everyone and highly publicized."

After September 15, the Commission should have its Staff access that Alert, evaluate it, and assess NERC's survey effort. How thorough was NERC's 2020 survey compared with COMPLAINANT's Bills of Lading (Exhibit A) and its underlying public data source? Mr. Weiss's blog states (of this docket):

> "Michael Mabee has amassed more than 150 bills of lading for Chinese-made electric equipment exported to the US electric grid from 2018-2020 ... . Utilities using this Chinese-made electric equipment range from the relatively small (e.g., the City of Anaheim, ...) to the large (e.g., PG&E, ...) and grid equipment suppliers (e.g., Alstom Grid). Some of this Chinese-made equipment has been installed in very sensitive locations."

Commission Staff should assess clarity and contents of NERC's confidential Alert — and its effectiveness — in light of all Comments and Motions to Intervene received. Did some (or many) electric utilities simply disregard NERC?

The Commission should also examine COMPLAINANT's analyses of Chinese government ownership and control of Doubletree Systems, Inc. of San Jose, CA and its roles in marketing Chinese-manufactured electric power transformers and other equipment, as well as monitoring systems and CIPS-compliance services (seemingly with EPRI endorsement). Those analyses have not been publicly presented before, as best I can determine (and may even not have been prepared confidentially in full before). COMPLAINANT concludes [footnote omitted]:

> **A Direct Line to the Government of the People's Republic of China**

> Behind many of the U.S. imports of Chinese-manufactured transformers, other equipment and components is a company called Doubletree Systems, Inc. Doubletree Systems, Inc. also represents several other Chinese companies that sell transformers and other equipment imported for use in the U.S. Critical Electric Infrastructure.[17] In addition, Doubletree sells grid security and monitoring systems and works with the Electric Power Research Institute (EPRI) on grid security issues.
>
> There is evidence that the government of the People's Republic of China has an ownership and/or control interest in Doubletree Systems, Inc. ...

COMPLAINANT also discusses obligations that Chinese laws impose on all entities [footnotes omitted]: "All Chinese companies have an obligation under the 2017 Chinese National Intelligence Law[27] to "support, assist and cooperate with the state intelligence work." Moreover, under China's 2014 Counter-Espionage Law[28] a company may not refuse the Chinese government when asked for information."

STG Coalition's February 2021 letter to Nominee Granholm

The Commission should be aware of February 4: 2021, letter (see **References**, below). STG quoted a George R. Cotter MTI addressed to the Commission, which summarizes:

> "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."

So far as I can determine, the Commission has not hitherto addressed the merits of detailed points submitted to it during 2020 by Mr. Cotter (who had a distinguished NSA career) in five MTIs.

Commission direction that NERC better protect Electronic Access Control and Monitoring Systems

The Commission's Order No. 850 (165 FERC ¶ 61,020), "Supply Chain Risk Management Reliabilty Standards" (October 18, 2018), observed (in Paragraphs 4 & 50) that the Critical Infrastructure Protection Standards (CIPS) presented to it for approval failed to "address Electronic Access Control and Monitoring Systems (EACMS)" and directed NERC to propose standards to remedy that gap. NERC submitted changes which FERC approved on March 18, 2021 (but are not yet effective). FERC observed:

> 8. Notice of NERC's December 14, 2020 filing was published in the *Federal Register*, 86 FR 2668 (2021), with interventions and protests due on or before January 28, 2021. No interventions or comments were received

NERC needed 3 membership ballotings and two revisions before making a filing with FERC.
— Here is the filing with FERC for the modified standards.
https://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Petition%20-%20Supply%20Chain%20Risk%20Management_final.pdf
— Here is the FERC order approving:
https://elibrary.ferc.gov/eLibrary/filelist?accession_num=20210318-3030

Unresolved synchrophasor (PMU) issues and some other issues:

Mr. Cotter advised that syncrophasors are used in North America to control electric utility operations as well as for forensic purposes. Mr. Gugel advised that in North America synchrophasors are used only for forensic purposes, with electric utilities relying on SCADA data for their operations, but Mr. Cotter asserts that examples of Bonneville Power Administration (BPA), Dominion Energy, ISO New England, and ISO New York support his conclusion. Commssion Staff should investigate the question after September 15, and advise NERC, Mr. Cotter, and the Commission of their findings.

If synchrophasor data (PMUs) — as well as SCADA data — are in fact used for real-time operational control of the electric power grid (including the Bulk Electric System as well as distribution systems),

then Mr. Cotter's arguments for strengthening the CIPS (and their implementation) to protect synchrophasors effectively are all the more important to evaluate on their merits.

Much will turn on meaning(s) of NERC terms, **BES Cyber Asset** and **Cyber Asset** — and on how loosely ERO audits let various entities interpret them. Mr. Gugel advises:

> As we stated on our [August 31] call, if any PMU meets the definition of BES Cyber Asset, which is "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. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems," it is subject to our CIP standards and must meet all the applicable requirements. Our auditors examine the use and scope of these systems during CIP audits.
>
> A Cyber Asset is defined as "Programmable electronic devices, including the hardware, software, and data in those devices."

After September 15, the Commission should have Staff closely review the "small print", exclusions, and exemptions of CIPS 13 [Supply Chain Risk Management] and 14 (as well as related NERC Glossary terms) to identify arguably unwarranted gaps.

On March 24, 2021, the ERO Enterprise declined to endorse Implementation Guidance for CIP-013-2 "Supply Chain Risk Management Plans (2019-03 SDT)". The Commission should have Staff determine policy implications of the proposed Implementation Guidance which the SDT presented and what potential "confusion" led to rejection. [See https://www.nerc.com/pa/comp/guidance/Documents/Non-Endorsed%20Implementation%20Guidance.pdf]

Follow-up to post-September 15 Commission Staff investigations

After September 15, I believe the Commission must have its Staff pursue unresolved questions because the Commission has *unique*, *independent* responsibilities under Section 215 of the Federal Power Act (which Congress added to FPA Part II in 2005). After Staff investigations are completed, the Commission would do well to schedule a carefully constructed public hearing or other public process that addresses the merits of issues raised in this docket.

References

Glossary of Terms Used in NERC Reliability Standards (updated June 28, 2021) [https://www.nerc.com/files/glossary_of_terms.pdf]. N.B., this website has four sections; each is alphabetical.

NERC website, "Regional Audit Reports of Registered Entities" [https://www.nerc.com/pa/comp/Pages/NERC%20Regional%20Audit%20Reports.aspx].

PNNL-26874, "Recommended Guidelines for NERC CIP Compliance for Synchrophasor Systems" (September 2017) [https://www.nerc.com/comm/PC/Synchronized%20Measurement%20Subcommittee/pnnl_26874_cip_recomm_synchrophasors_20170926.pd.pdf]

George R. Cotter, 3rd Motion to Intervene on Dockets Nos. EL20-46-000, RM20- 12-000 and AD20-19-000, all Related to Critical Infrastructure Reliability Standards (August 7, 2020) including critical analysis of NPCC's 2017 audit of LIPA. [https://securethegrid.com/wp-content/uploads/2021/02/GeorgeCotter-3rdMotion-FERC-7Aug20.pdf]

George R. Cotter, 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 (November 18, 2020) including discussions of Dominion Energy, CA-ISO, NE-ISO, So. California Edison, BPA, and TVA. [https://securethegrid.com/wp-content/uploads/2021/02/GeorgeCotter-5thMotion-FERC-18Nov20.pdf]

2020 FERC Staff Report, "Lessons Learned from Commission-Led CIP Reliability Audits" (October 2, 2020) [https://cms.ferc.gov/sites/default/files/2020-10/2020%20CIP%20Audits%20Report.pdf]

Paul N. Stockton, "Defeating Coercive Information Operations in Future Crises" (Laurel, MD: Johns Hopkins University Applied Physics Laboratory, August 2021) [https://www.jhuapl.edu/Content/documents/DefeatingCoerciveIOs.pdf]

Joseph Weiss, "Do Chinese "own" our electric grids and other infrastructures?" (August 27, 2021) [https://www.controlglobal.com/blogs/unfettered/do-the-chinese-own-our-electric-grids-and-other-infrastructures/]

Llewellyn King, "Your Utility Should Expect the Unexpected, It's on the Way" (SeptemSecure the Grid Coalition letter to Nominee Granholm Re: Improving Executive Branch Policies to Secure the United States Electric Grid (February 4, 2021) [https://michaelmabee.info/wp-content/uploads/2021/02/STG-Coalition-Letter-to-Honorable-Jennifer-Granholm-DOE-OMB.pdf]

Service

Once these Initial Comments are uploaded to eFile, I shall serve them by emailing to:

CivilDefenseBook@gmail.com;
NancyB@epsa.org;
jwilliams@thompsoncoburn.com;
aclair@thompsoncoburn.com;
Sonia.mendonca@nerc.net

Respectfully submitted, David Jonas Bardin

Appendix: Acronyms used herein (or in documents cited herein)

BES Bulk Electric System
BPA Bonneville Power Administration (in Department of Energy)
BPS Bulk Power System
CAISO California ISO
CIPS Critical Infrastructure Protection Standards
DFR digital fault recorder
EACMS Electronic Access Control and Monitoring Systems
EAP electronic access point
EPRI Electric Power Research Institute
ERO Electric Reliability Organization certified by FERC. It consists of NERC + Regional Entities.
ESP Electronic Security Perimeter
FERC Federal Energy Regulatory Commission (successor to Federal Power Commission)
FBI Federal Bureau of Investigation (in the Department of Justice)
FPA Federal Power Act
IOs Information Operations (in Information Warfare, see Paul N. Stockton, ...
ISO Independent system operator
ISO-NE New England ISO
JSHP JiangSu HuaPeng Transformer Co., Ltd.
LIPA Long Island Power Authority
MTI motion to intervene
NASPI North American Synchrophasor Initiative (see https://www.naspi.org)
NEISO New England ISO
NERC National Electric Reliability Corporation, a non-profit corporation (successor to National Electric Reliability Council)
NSA National Security Agency
ODNI Office of the Director of National Intelligence
PACS Physical Access Control Systems
PCA Protected Cyber Assets
PDC phasor data concentrators
PG&E Pacific Gas & Electric Company
PMU phasor measurement unit
PNNL Pacific Northwest National Laboratory (in Department of Energy)
REs Regional Entities (of the ERO)
SCE Southern California Edison
SNL Sandia National Laboratories (in Department of Energy)
SCADA Supervisory control and data systems
SDT Standard(s) drafting team
STG Secure the Grid [Coalition]
WAPA Western Area Power Administration (in Department of Energy)