UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

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

Motion to Intervene and Comments of John Organek

Purpose

I am submitting comments, as a private citizen, on Michael Mabee's complaint, EL21-99, with a focus on Emergency Presidential Executive Order (EO) 13920, issued May 1, 2020.[1] EO13920 was issued to address actions apparently undertaken by a nation-state that could lead to a catastrophic impact on our Nation's electric grid and on the critical infrastructures served by the electric grid, such as water and wastewater systems, vital to maintaining our society. At least two transformers supplied by the Chinese were found to have hardware-based backdoors that could be used to disrupt the reliability of power. The EO was designed to address the gaps and shortcomings of the NERC Supply Chain and CIP programs. Notwithstanding the fact that EO13920 addressed future purchases, there are over 300 Chinese-made transformers and other items of power control equipment already installed. **This is about the risks associated with hardware and grid monitoring products and services being incorporated into our electric grid by a potential adversary.**

I am seeking answers to the following questions and would like to propose several actions that the Federal Energy Regulatory Commission should take about these items of equipment.

- Do any of these transformers make the electric grid vulnerable to manipulation by China, a nation-state?
- Can manipulation of these transformers cause cascading effects on other critical infrastructures, particularly damage to electrical equipment?
- Can manipulation of these transformers prevent electric grid recovery—black start—in the event of an outage caused by a natural hazard?

My Background

I understand the risks posed to the electric grid and other critical infrastructures. I served in the US Army as an officer in the Corps of Engineers and at one point, I was the Chief of Engineering Plans for the defense of South Korea, which required me to plan for the protection and recovery of critical infrastructure in the event of a conflict. For the past 5 years, I have worked for a non-profit focused on building resilience to a catastrophic grid outage known as a Black Sky event, a prolonged and widespread power outage. Through my extensive research and

[1] Though it has been 'suspended' by Executive Order 13990, Executive Order 13920 reflects considerations pertinent to this filing. Furthermore, the action to suspend the order for a period of time until a study could be conducted is also relevant to this filing.

numerous meetings with critical infrastructure executives, planners, and operators, I am well aware of the operations of the electric grid and its relationships with the other critical infrastructures. For the past 2 years, I have participated in meetings, conferences, and working group sessions with the World Federation of Scientists, examining hazards, vulnerabilities, and consequences associated with the energy and water sectors. I have also served in key positions in Headquarters Department of Army, formulating policies across a variety of stakeholders on technical subjects involving our Nation's security. In short, I am a Civil Engineer with an extensive background in systems, architecture, and Information and Communications technology, as well as National Security.

The Problem

The Threat from China.

Since its admission to the World Trade Organization at the end of 2001, China has emerged as an industrial power, capable of delivering products and services used to provision and operate the electric grid. The economic and qualitative characteristics of its products have become very attractive and utility operators continue to purchase and embed and employ them into the makeup and operation of the grid. The problem is best framed by the questions: What can go wrong, and what are the consequences?

In parallel with its rise as an economic power, China has pursued a plan to gain global geopolitical dominance, as demonstrated by its belt and road initiative. Furthermore, it appears that even the products and services they produce and market globally, 'fit that purpose'. Witness, for instance, products that were manufactured by Huawei and insinuated in communications systems throughout the globe, and which were found to have critical vulnerabilities that could support certain acts that are able to monitor or even paralyze the critical infrastructures in which they are embedded.

And while China has every right to manufacture and sell their products anywhere, a couple of 'red flags' should be raised with regard to the risks we have already managed to accumulate, that is, an extensive dependence on external source of supply for critical equipment and the embed of undesirable capabilities as part of the critical equipment we use in our Nation's electric grid and other critical infrastructures.

Besides posing risk to the electric grid, transformers and other operational and control hardware can be used to negatively impact equipment in the other critical infrastructures that sustain our people and our society. Water and wastewater systems for example, require very large electric motors and these motors are quite sensitive to voltage and frequency variances. In some cases, as demonstrated by the Aurora tests conducted by the Idaho National Lab, and by the impact to Iranian equipment caused by Stuxnet, it is quite conceivable that an adversary can cause widespread and crippling damage to equipment, exercised through control of the voltage and frequency of the electric grid. It is relatively easy to envision an attack on our critical infrastructure being carried out 'quietly' by using and manipulating the key items of equipment cited in EO13920, and having an effectiveness that is greater than attacks conducted by bombers and missiles during combat operations, such as those carried out in Iraq.

The threat is real, it has been documented. Chinese attacks on electric grids have a history dating back at least 20 years—including an attack from within, on their own grid. And while covering only a communications-related threat, NERC and FERC issued in July 2019, a White Paper pointing out risks in the use of Huawei equipment and ZTE chips. Clearly, there has been US Government recognition of a potential threat posed specifically by China to the electric grid.

Advisories on Chinese Transformers.

NERC, jointly with, or with the concurrence of FERC has continued to issue alerts, advisories, white papers, etc., that have discussed the risks associated with hardware, software, firmware, controls, etc., embedded in the bulk power system.

In many cases, these were issued only ***after*** a component had already undergone the compliance checks required by the CIPs and using NERC Supply Chain criteria. Case in point is the joint whitepaper issued about SolarWinds. To the best of my knowledge, NERC has not publicly issued any alert, advisory, or white paper that addresses any potential vulnerability associated with the Chinese-made transformers cited in Mr. Mabee's complaint. It would seem appropriate to conduct such a risk assessment and report the results to the American people, who have grown an existential dependence on the electric grid.

EO13920 and CIPs

Were it still in force, EO13920 would have addressed many of the issues cited by the Complainant c and those I have expressed in this comment. While the Department of Energy continues to formulate policy based on comments received from their Request for Information that closed in June 2021, governance around reliability and security has 'defaulted' to the NERC CIPs and NERC Supply Chain criteria. Focus also has shifted from risks posed by the hardware to risks posed by networks and their components, as well as vulnerability of the software. Since the CIPs, the focus on network, and a 'defense in depth' strategy that looks at the risk from the outside in, rather than emanating from within, do not fully address the risks posed by a 'Trojan Transformer', it is incumbent on FERC, through NERC, to make the record clear about the Chinese-manufactured transformers.

Impact on Other Stakeholders.

FERC should keep in mind that this is not a matter solely affecting the bulk power system, but also has the potential to affect the distribution system and other critical infrastructures, which, though they do not fall under FERC's jurisdiction, are nevertheless affected by actions taken by FERC. Potentially vulnerable equipment must be kept out of our critical infrastructure, period!

FERC also should consider that despite providing an opportunity for public comment, a vast number of Americans do not have the knowledge or expertise to assess the technical aspects of the risks posed and therefore, they are reluctant to express their concerns. FERC should consider the larger populace when deciding how to act on the comments of Michael Mabee, and not simply reflect those of a narrower interest group. I am suggesting that FERC rise above

the 'constituencies' and assess and decide on the situation by addressing National Security, as well as economic, considerations.

A final point: having to maintain vigilance over potential vulnerabilities known to exist in the electric grid drives up the cost of providing electric service and it is borne by the American people. Beyond the 'priceless' cost of national security, it would seem that the cost of full monitoring and control of the risks associated with the equipment would erase any cost differentials. Of course, I am not advocating that the attendant cost of compliance should in any way soften the regulatory policy that FERC, through NERC, would impose!

Recommendations For Reducing the Vulnerability of Hardware in the Electric Grid

- Determine the degree of risk posed by the Chinese transformers.
- Develop standards for ***all*** grid **hardware** components such as transformers, sensors, etc. The current stipulation that standards apply to only 'critical' components unfortunately, does not cover those whose compromise could cause extensive damage, prolonged outages, and disruptions during periods of national emergency.
- Develop and promulgate standards for procurement of hardware critical to the operation of the electric grid. These standards should mirror those used by the Department of Defense when acquiring components for use in military equipment.
- Assess the adequacy of existing NERC CIPs and NERC Supply Chain criteria to prevent the use of vulnerable hardware in the electric grid.

Relief Sought

I concur with the position taken by Michael Mabee and am adding the following:

- Regarding Mabee's recommendation about conducting a comprehensive survey, but would modify it to include any foreign supplier.
- Regarding Mabee's recommendation on establishing a standard for testing and monitoring the security of Chinese-made equipment, I would expand the scope to include all foreign-sourced equipment ***critical*** to the electric grid. NOTE: the standard should include a definition of what is meant by 'critical'. FERC should direct NERC to develop standards for equipment, regardless of national origin, and to update current CIPs to reflect such equipment and supply chain issues cited.
- Regarding Mabee's recommendation for FERC to work with State Public Utility Commissions to encourage adoption of bulk power system standards, I would add more specific and directed guidance regarding Defense Critical Electric Infrastructure.
- Deliver to the American people the results of a complete and independent risk assessment of the Chinese transformers currently in the electric grid. This risk assessment should be as in-depth and comprehensive as the assessments performed for components used by the nuclear power industry. Add to this a certification that the assessment is "exhaustive, conducted by electrical and system engineers and cyber security experts, and there are no potential vulnerabilities."
- Disclose the added cost of monitoring needed to ensure that risks from embedded hardware having known vulnerabilities are mitigated.

Document Content(s)