

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 Joseph Weiss

Purpose

I am submitting comments on Michael Mabee’s complaint EL21-99 with a focus on Emergency Presidential Executive Order (EO) 13920 issued May 1, 2020.¹ The technical portion of the EO was developed by technical experts at the U.S. Department of Energy (DOE) and subsequently issued through emergency powers to address a **real** nation-state cyberattack against the U.S. bulk electric system (it is now known there were at least two Chinese-made transformers in the U.S. with hardware backdoors). The EO is necessary to provide the needed cyber security and safety that has been missing from the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) process, plug the holes in the NERC Supply Chain Program, and to address a real threat to our country. The NERC CIPs have missed the problems and effectively prevented the right people and expertise from being involved. These exclusions can preclude cyber events (malicious or unintentional) from being identified. A downside of the EO was that it was written for future purchases. As there are approximately 300 large Chinese-made transformers and many other pieces of critical Chinese-made grid equipment already installed in the U.S. electric grid, the questions are:

- What should be done about the potentially compromised equipment that could cause catastrophic damage to the U.S. grid?
- Why are U.S. utilities still buying this critical equipment from China?
- As the NERC CIP process does not protect the reliability of the electric grid, what other cyber security requirements should be used to protect the cyber security of the electric grid?

My background

I am considered an expert on control system cyber security of the electric grid. I spent almost 15 years at the Electric Power Research Institute (EPRI) managing various control system programs and in 2000 helped start the control system cyber security program for the electric utilities. After leaving EPRI in 2002, I went to KEMA. While there, I started the first control system cyber security conference in 2002. In the 2003-4 timeframe, I helped the Idaho National Laboratory establish the SCADA Test Bed. Through MITRE, I supported the National Institute on Standards and Technology (NIST) in extending SP800-53 for control systems. I supported the Pacific Northwest National Laboratory (PNNL) in supporting the Nuclear Regulatory Commission (NRC) on the development of the Regulatory Guide for nuclear plant cyber security – Reg Guide 5.71. I supported Navy Mission Assurance Division on the Aurora hardware vulnerability and the Federal Energy Regulatory Commission (FERC) on control system cyber issues including a review of the Aurora response. I also supported the International Atomic Energy Agency (IAEA) on nuclear plant cyber security. I have testified to both House and Senate hearings on control

¹ While Executive Order 13920 was “suspended” on January 20, 2021 by Executive Order 13990, the order remains very instructive given the continued supply chain cybersecurity vulnerabilities in the electric grid.

system cyber security. I have conducted numerous control system cyber security assessments and developed control system cyber security policies. I am the Managing Director of the international standards on control system cyber security – ISA99 (the ISA62443 series of standards) and a participant in various International ElectroTechnical Committee (IEC) standards committees. I also authored the book Protecting Industrial Control Systems from Electronic Threats².

Chinese cyberattacks against the U.S. electric systems

One of the first nation state cyberattacks against the U.S. grid was the Chinese cyberattack of the California Independent System Operator (CA ISO) in 2001. One of the first cases of cyberattacking control system vendor supply chains was in 2012 when China hacked Telvent (now part of Schneider Electric). The Chinese were providing counterfeit transmitters in Asia in the 2014 timeframe and the counterfeits made their way into North America in the 2018-19 timeframe. Supply chain attacks from China are not just aimed at the U.S. I participated in an international power engineering conference where the Chief Engineer from the Power Grid of China described how they were impacted by supply chain attacks from within China. July 12, 2019, NERC requested utilities to inventory reliance on Chinese technology.³ On July 31, 2020, NERC and FERC issued a joint white paper on Huawei and ZTE chips have been known to have backdoors resulting in a joint whitepaper in by FERC and NERC.⁴

Most Chinese cyberattacks have been to steal data. The transformer issues identified in EO 13920 were different – there was no data to steal, only access to the operation of the transformers enabling a Stuxnet-like attack.

EO 13920

The recognition of the need for spare transformers started almost 20 years ago as these very expensive, long-term procurement items could have a significant impact on grid reliability and availability. The scope of EO 13920 includes items used in bulk-power system substations, control rooms, or power generating stations, including reactors, capacitors, **substation transformers**, current coupling capacitors, large generators, backup generators, substation voltage regulators, **shunt capacitor equipment**, automatic circuit reclosers, instrument transformers, coupling capacity voltage transformers, **protective relaying**, metering equipment, high voltage circuit breakers, generation turbines, **industrial control systems**, distributed control systems, and safety instrumented systems. Items not included in the preceding list and that have broader application of use beyond the bulk-power system are outside the scope of this order.

The Chinese have provided almost 300 large electric transformers to the U.S. grid over the past 10-15 years. Recently, there were more than 50 Chinese-made transformers ordered in 2020 with more on order in 2021. Before 2005, there were no Chinese-made transformers in the US electric grid. It is not just transformers being bought from China. **DoubleTree Systems, Inc.**⁵ is associated with JSHP

² Weiss, Joseph, Protecting Industrial Control Systems from Electronic Threats, Momentum Press, May 2010, ISBN: 978-1-60650-197-9.

³ S&P Global. “NERC to ask utilities to inventory reliance on Chinese technology.” July 12, 2019. https://www.spglobal.com/marketintelligence/en/news-insights/trending/peha_2jR2jCRPAdm2DIX-w2

⁴ FERC & NERC Joint Staff Whitepaper. “Joint Staff White Paper on Supply Chain Vendor Identification - Noninvasive Network Interface Controller.” July 31, 2020. <https://www.nerc.com/pa/comp/CAOneStopShop/Joint%20Staff%20White%20Paper%20on%20Supply%20Chain%2007312020.pdf>

⁵ Doubletree Systems website: <http://www.dsius.com/>

transformers and other Chinese equipment manufacturers connected to the Chinese government including Beijing Power Equipment Group and the Xu Ji Group Co. **Doubletree Systems** continues to provide critical grid equipment and engineering services, including equipment explicitly addressed in EO 13920 (see items bolded above and identified below and included in the Complaint Appendix A), to large utilities (e.g., WAPA and the Bonneville Power Authority) and small utilities (e.g., City of Anaheim). **Doubletree Systems** not only imports and markets Chinese JSHP transformers in the U.S., including those specifically identified in EO 13920, but also sells a variety of critical grid monitoring products and services such as:

- POLARIS (substation monitoring system)
- SA200 (substation automation)
- Wide Area Measurement System (WAMS). According to **Doubletree System's** website: "WAMS solution provided is field-proven in Bonneville of Power Administration of WSCC (sic)".
- Generator Testing & Model Validation. According to **Doubletree System's** website: "The standard generator testing and model validation provided by **Doubletree Systems, Inc.** has extensive experience and has been certified by Western Systems Coordinating Council (WSCC)".
- Special Protection System (SPS).
- Transfer Limits Monitoring.
- SCADA/EMS/DMS/DA consulting.

The equipment and services provided by **Doubletree Systems** through POLARIS, WAMS and SA200 and the companies associated with the Xu Ji Group Co. and JSHP should raise major concerns about the integrity of the U.S. power grid. These grid monitoring and control systems can help China set up covert cyber infrastructure that can compromise the nation's electric grid. For example, these systems can impact the accuracy of the phasor measurements being counted on to provide grid monitoring and system restoration forensics.

The Electric Power Research Institute (EPRI) did a demonstration program of the Chinese-made grid equipment. EPRI's write up on the 2014 DISTRIBUTCH Conference and Exhibition noted: "Network Security: A kickoff meeting was held on the floor of DistribuTECH for a group of vendors currently interested in participating in the 'Protective Measures for Securing T&D Systems' project, which involves validating the mapping of IEC 62351-7 network security events. Vendors currently engaged in the project include SISCO, Ruggedcom, OSIsoft, **Doubletree Systems**, and Radiflow. Other vendors expressing interest include Cisco, Schneider Electric, and SEL. The project will be driven by use cases developed in early 2014 with proof-of concept implementations to be developed and demonstrated in the EPRI Cyber Security Research Lab throughout 2014." [Emphasis added.]

Not only does this project provide additional justification for U.S. utilities to use the Chinese-made equipment, the project enables U.S. electric grid suppliers to use this Chinese equipment, and the Chinese vendors to embed themselves into U.S. electric grid suppliers' technologies.

The U.S. Department of Energy (DOE) is developing technologies to detect electric grid cyberattacks such as C3D.⁶ The C3D technology does not address hardware issues, nor do they address known issues such as Aurora. Additionally, C3D can utilize data from **Doubletree System** products as input. With the Chinese-made equipment and services, the lack of implementing Aurora hardware protection, and the

⁶ See: <https://www.controlglobal.com/blogs/unfettered/results-from-threatconnect-webinar-on-mitigating-risks-in-critical-infrastructures-and-on-going-actual-risks>

gaps in protection inherent in the NERC CIPs, one has to ask how is it possible to claim the grid is being protected against cyber threats?

Conflicts between the EO 13920 and DOE/industry response

The equipment explicitly identified in the EO is out-of-scope for the NERC CIPs and the NERC Supply Chain criteria. Conversely, the equipment and networks identified as being in scope for the NERC CIPs and the NERC Supply Chain effort are out of scope for EO 13920. That is, the network devices such as firewalls were not included in the EO as they are ineffective with embedded hardware vulnerabilities that can initiate communications from inside the firewall-protected perimeter. It also requires changes in procurement requirements, yet the EEI-developed procurement requirements did not address any control system-unique requirements. Additionally, software bills of materials (SBOMs) are not effective means of mitigation when the equipment is coming from China yet that has become a focus for grid supply chain cyber security.

General Recommendations for Improving Grid Cybersecurity

- Authenticate the process sensors to help minimize the impact of the hardware backdoors and man-in-the-middle cyberattacks.
- Implement requirements for periodic monitoring of the transformers starting with site acceptance testing and continuing with testing every 6 months.
- Develop procurement specifications specifically addressing cyber security of control system field devices need to be developed.
- Assess the potential impact on the regional grid when transformers and other critical grid equipment are compromised (not just catastrophic damage of the transformer).
- Reassess the applicability of the NERC CIPs and NERC Supply Chain criteria for hardware cyber security issues. Consider the use of the EO and the ISA 62443 series of control system cyber security standards.
- Reassess the technical exceptions in the CIPS such as the Electronic Security Perimeter (ESP) that excludes control system devices. Modify the NERC Critical Infrastructure Protection (CIP) standards and the NERC Supply Chain requirements to include monitoring of the process sensors.
- Provide requirements to train transformer engineers and technicians on cyber security issues.
- Do not use Chinese-made equipment or services in critical grid applications. Replace existing Chinese-made equipment as soon as possible. In the interim, monitor system performance and assure all process sensor measurements are authenticated.

Relief Sought

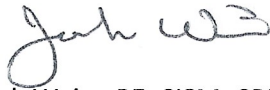
As Michael Mabee sought in his complaint, I am providing my concurring recommendations (my additions in bold):

1. 1.FERC should direct 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 **and how they are being used.**
2. FERC should direct NERC to submit to the Commission a proposed reliability standard for testing and monitoring the security of Chinese equipment or systems are currently in use in the Bulk Power System or purchased for future use **as identified in EO 13920. FERC should direct NERC**

to revise the NERC CIPs and NERC Supply Chain requirements to explicitly include the equipment identified in EO 13920. This should include technology to authenticate the integrity of process sensors to minimize the impact of the hardware backdoors and potential man-in-the-middle cyberattacks. FERC should direct NERC to develop cyber security procurement guidelines for the equipment identified in EO 13920. FERC should direct NERC to assess the potential grid impacts from compromise of critical grid monitoring and control equipment and develop appropriate recovery options.

3. FERC 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.

Respectfully,



Joseph Weiss, PE, CISM, CRISC
Managing Partner, Applied Control Solutions, LLC