

**UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION**

Complaint of Michael Mabee)	
Related to Critical Infrastructure)	Docket No. EL20-46-000
Protection Reliability Standards)	

**MOTION TO INTERVENE AND MOTION TO REQUIRE CERTIFICATION PRIOR TO INTERVENTION FOR
TRADE ASSOCIATIONS AND RESEARCH ORGANIZATIONS INTERVENING IN DOCKETS INVOLVING U.S.
NATIONAL SECURITY**

Submitted to FERC on May 14, 2020

The Secure the Grid Coalition files these motions pursuant to 18 CFR § 385.214 (Rule 214) and 18 CFR § 385.212 (Rule 212) respectively.

MOTION TO INTERVENE:

The Secure the Grid Coalition is an ad hoc group of policy, energy, and national security experts, legislators, and industry insiders who are dedicated to strengthening the resilience of America’s electrical grid. The Coalition aims to raise awareness about the national and international threat of grid vulnerability, and encourage the steps needed to neutralize it. Our group and its individual members have been frequent participants in FERC dockets related to issues of grid security. We bring a wide variety of expertise in cybersecurity, physical security, public policy and believe our perspective is in the public interest – specifically, the interest of citizens and businesses that depend on the security of the electric grid. Therefore, the Commission should grant the Secure the Grid Coalition’s Motion to Intervene as it is in the public interest.

MOTION TO REQUIRE CERTIFICATION PRIOR TO INTERVENTION FOR TRADE ASSOCIATIONS AND RESEARCH ORGANIZATIONS INTERVENING IN DOCKETS INVOLVING U.S. NATIONAL SECURITY

On May 11, 2020, Michael Mabee, a private citizen who conducts public interest research on the security of the electric grid, filed the complaint related to Critical Infrastructure Standards which precipitated the opening of this legal docket. On May 13, 2020, Michael Mabee filed a motion to exclude the Edison Electric Institute (EEI) from intervening in this docket and for FERC to require electric industry and trade association intervention in this docket only after an organization could “certify that it has no affiliation, members, interests or shareholders who are entities or governments that are a foreign adversary as defined in Executive Order 13920.”

The Secure the Grid Coalition supports that motion this for the reasons established in Mr. Mabee’s filing and further moves that that the Commission also require electric power research organizations, particularly the Electric Power Research Institute (EPRI), to make the same certification. This motion is to inform the Commission that EPRI maintains its own ties with the Peoples Republic of China and that it should therefore be excluded from commenting on this docket without such certification. The Commission should consider the following side-by-side timeline:

Open Source information on EPRI engagement with Chinese Researchers

Timeline of EPRI/China Engagement from Publicly Available Information:

- Early 2000s: EPRI engagement with China commences with in-country meetings with key nuclear industry personnel.¹
- 2006: A formal and ongoing relationship is established between China General Nuclear Power Corporation (CGN) and EPRI's Nuclear Maintenance Applications Center (NMAC) program.¹
- 2011-2012: EPRI leaders meet key leaders visit Chinese nuclear utilities in the wake of the 2011 World Association of Nuclear Operators (WANO) biennial meeting.¹
- 2013: CGN joins four EPRI nuclear research programs.¹
- 2013: China National Nuclear Corporation (CNNC) joins two EPRI nuclear research programs.²
- 2015: CNNC joins two more EPRI nuclear research programs.¹
- 2016: EPRI publishes "Guidance for Instrumentation and Control Equipment Reliability Management Based on China General Nuclear Power Company Experience"³
- 2017: EPRI reports that 25% of its research funding comes from international members.⁴
- 2019: EPRI reports working with Chinese utilities enter data on nuclear plant single point vulnerabilities (SPVs) into a new analysis tool developed by EPRI.⁵
- 2019: the U.S. Commerce Department added China General Nuclear Power Group (CGN) and three of its affiliates to the Commerce Department's "Entity List." This means U.S. and non-U.S. companies are prohibited from exporting or transferring to the listed Chinese entities any goods, software or technology that is subject to control under the U.S. Export Administrations Regulations (EAR)⁶

Excerpt Taken Directly from U.S. Cyberspace Solarium Commission Report

Major Cyber Operations Publicly Attributed to China: 2006–2019

- 2006–18: APT10 conducts a systematic cyber espionage campaign stealing intellectual property and compromising computer systems containing personally identifiable information on over 100,000 U.S. Navy personnel.¹⁹
- 2008: Operators exfiltrate terabytes of data and schematics from the F-35 and F-22 stealth fighter jet programs.²⁰
- 2012: China compromises computers in a new African Union headquarters it helped build in Ethiopia with malware that exports massive amounts of data nightly to servers in Shanghai.²¹
- 2012: Chinese groups target oil and natural gas pipelines in the United States.²²
- 2013: *IP Commission Report* highlights Chinese efforts at intellectual property theft efforts linked to an estimated \$300 billion in business losses a year.²³
- 2014: Cloud Hopper campaign attacks managed service providers to access their client networks, including those of leading international technology companies, and steal their clients' intellectual property.²⁴
- 2014–15: The Office of Personnel Management is breached, exposing sensitive information used for security background checks on 21 million federal employees.²⁵
- 2017: Chinese military hackers breach the networks of Equifax, an American credit reporting agency, stealing the personal information of over 145 million Americans.²⁶
- 2018: Hackers breach servers of Marriott International, extracting information on 500 million guests.²⁷
- 2019: Operators compromise iPhones in a domestic spying campaign targeting Uighurs, a Muslim minority in China.²⁸

Timeline Sources:

Left hand column:

¹ <https://eprijournal.com/building-a-research-bridge-to-china/>² <https://www.power-eng.com/2013/10/14/epri-china-team-on-nuclear-energy-research/>³ <https://www.epri.com/#/pages/product/000000003002008025/?lang=en-US>⁴ https://www.mncee.org/getattachment/Resources/Resource-Center/Presentations/2017-Energy-Technology-Forum/Tech-Forum-2017_EPRI_Ram-N.pdf.aspx⁵ <https://eprijournal.com/a-new-tool-to-address-single-point-vulnerabilities/>⁶ <https://www.pillsburylaw.com/en/news-and-insights/china-industry-entity-list.html>

Right hand column:

<https://www.solarium.gov/report>

The Secure the Grid Coalition recognizes that EPRI is the collaborative research arm of the electric utility industry, that collaboration among utilities can be beneficial, and that EPRI's model enables smaller utilities to benefit from shared-cost research that would otherwise be too expensive to conduct on their own.

However, in Executive Order 13920 the President of the United States found:

“...that the unrestricted acquisition or use in the United States of bulk-power system electronic equipment, designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries augments the ability of foreign adversaries to create and exploit vulnerabilities in bulk-power system electric equipment, with potentially catastrophic effects.”

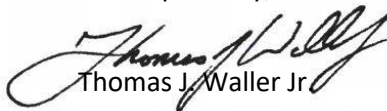
With EPRI's collaboration reaching outside of the United States and specifically involving Chinese state-owned utilities beholden to the intelligence gathering apparatus of the Chinese Communist Party – including at least one which has been placed on the U.S. Commerce Department's “Entity List” – there should be great concern about what kind of access they have to EPRI's research since it could clearly augment the ability of foreign adversaries to exploit vulnerabilities in the bulk-power system.

Mr. Mabee's motion described the consistent lobbying executed by Edison Electric Institute in relation to grid security and, often, as an intervenor and commenter on FERC dockets. During EEI's lobbying efforts, it routinely makes use of research conducted by EPRI. Since EPRI has reported that 25% of its funding comes from its international members there should also be a concern as to how influential these international members might be in affecting EPRI's research priorities and methodology.

Therefore, we request that the Commission direct the Office of Energy Infrastructure Security (OEIS) to establish a certification criteria and procedure for organizations intervening in dockets involving U.S. National Security to certify that they have no affiliation, membership, interests or shareholders who are entities or governments that are a foreign adversary as defined in Executive Order 13920.

The Secure the Grid Coalition, and the Center for Security Policy which sponsors it, makes that certification with the filing of this motion.

Respectfully,



Thomas J. Waller Jr.