



Secure the Grid Coalition
A Project of the Center for Security Policy
2020 Pennsylvania Avenue, N.W., Suite 189
Washington, D.C. 20006

Aug 24, 2020

Mr. Charles Kosak
Deputy Assistant Secretary
Transmission Permitting and Technical Assistance Division
Office of Electricity
Mailstop OE-20, Room 8G-024
U.S. Department of Energy
1000 Independence Ave, SW
Washington, DC 20585

VIA <http://www.regulations.gov>

**Re: Comments of Secure the Grid Coalition Regarding Bulk-Power System EO RFI
FR Doc. 2020-14668**

Dear Mr. Kosak:

Our Secure the Grid Coalition¹ has long worked to improve the security of our nation's most critical infrastructure – the electric grid. We applaud the President of the United States for having issued Executive Order 13920 and for the Department of Energy seeking inputs on how best to rapidly implement this order.

Executive Summary:

Executive Order 13920 is long overdue. This executive action on the part of the federal government to Secure the Bulk Power Electric System is vital and we know that it has been initiated by the President on the heels of more than thirty (30) years of warnings to and by Congress that our electric grid is in perilous danger to both manmade and natural hazards.

For the benefit of your agency and the civil servants working to implement the President's Executive Order(s) related to protecting the grid, we have provided **Appendix A**. This is a list of both hearings to and legislation from the Congress that relates to the protection of the grid. While this list demonstrates an immense concern of the Congress and those experts who have testified to it, we must warn you that the overwhelming majority of bills that would have resulted in grid protection have FAILED. It is on backdrop of these three decades of failure of legislative efforts to protect our grid that our President has taken executive action and we ardently hope that your agency will carry out his intent to remedy these yawning vulnerabilities. We hope that these comments will help you do just that.

We recognize that your Request for Information (RFI) sought information on specific questions, many of which pertain to energy sector asset owners and/or vendors. While our Coalition is comprised of nationally renowned security professionals drawn from a wide range of experiences and expertise (some of which do own or operate energy sector assets), our comments will focus more from the "outside looking in" perspective. Because our Coalition and its members receive no funding from the

¹ 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. It is parented by the Center for Security Policy, a 501(c)(3). More info can be found here: www.SecureTheGrid.com

energy industry we are an unconstrained, unbiased observer and we believe that our observations are important to share with civil servants in government who are working diligently to “keep the lights on” every day.

With respect to the specific questions in the RFI, we primarily address question A-2 concerning foreign ownership, control, and influence (FOCI) of suppliers and question A-4, concerning available information on BPS cyber vulnerabilities.

Finally, our Coalition observes that the Executive Order puts “in scope” a comprehensive list of hardware and control systems. However, the RFI asks a series of questions about equipment and protocols which are good questions, but which are “out of scope” and have less to do with the specifics of the Executive Order. We commend DOE for asking additional questions which are out of scope of the Executive Order and, thus, we are submitting additional comments which are also outside the scope of the RFI.

These additional comments focus on four (4) main areas that are, perhaps, not covered by other comments submitted thus far, but that are of the utmost importance. These comments are in the form of fervent requests on the part of our Coalition, specifically that DOE:

- (1) Immediately Identify and Remedy Vulnerabilities to Large Power Transformers;
- (2) Prohibit the Use of Robotics, Including Drones, That Introduce & Highlight Grid Vulnerabilities;
- (3) Withstand Influence on the Part of Industry Lobbyists to Maintain a “Business as Usual” Approach to Grid Security; and
- (4) Demand Trusted Personnel & Organizations to Immediately Cease Ties With Foreign Adversaries.

(A-2) Foreign Ownership, Control, and Influence (FOCI) of Suppliers

Supply chain risks from sub-tier suppliers are a grave threat to the Bulk Power System (BPS). FOCI of counterfeit or trojan horses being placed within the microelectronic component is well known within the military supply chain. This threat remains unmitigated in the energy industry.

Microelectronics are the building blocks of all critical infrastructure and assurance of all sub-tier suppliers of these components must be guaranteed. Members of our Coalition have proven a decade ago that creating a digital fingerprint of each microelectronic is doable. Combining a repeatable full characterization (i.e digital fingerprint) of each building block (microelectronic) with block-chain technology would guarantee that trojan horses or counterfeit microelectronics are ever inserted into U.S. critical infrastructure going forward. If your agency would like to know more about this capability, please contact us (our POC information at the bottom of this document.)

(A-4) Available Information on BPS Cyber Vulnerabilities.

We believe that a comprehensive summary of BPS cyber vulnerabilities can be found in the comments made on FERC Docket EL20-46. This docket was opened by FERC after one of our

Coalition members submitted a complaint to FERC ten days after the President issued Executive Order 13920, stating, among other things, that “*The mandatory Critical Infrastructure Protection (CIP) standard CIP-013-1 (Cyber Security Supply Chain Risk Management) does not comport with Presidential Executive Order.*”²

We believe that your staff should review the original complaint and all the motions to intervene on this docket³, but we would like to particularly draw your attention to three sets of motions submitted by internationally renowned cybersecurity expert George Cotter.⁴ Mr. Cotter deeply researched both the NERC CIP Standards and NERC’s non-CIP Reliability Standards as well as NERC’s compliance assessments of these sets of standards. The results of his research are detailed in these three motions, which are included as **Appendix B**.

Request (1) **Immediately Identify and Remedy Vulnerabilities to Large Power Transformers**

We commend and vigorously support the comments on transformers submitted by AK Steel and Gueta Mezzetti and need not repeat their wise observations and recommendations with respect to Large Power Transformers.

We intend to complement those comments with four additional recommendations:

1- Immediately Track & Report Large Power Transformer Data Important to National Security

We believe immediate and improved public reporting on critical energy equipment (particularly large power transformers) imports from China and other nations listed as “foreign adversaries” will assist the U.S. Government with prioritizing how best to secure these assets.

Since at least year 2004, the International Trade Commission, a U.S. government entity, has tracked imports of high voltage transformers (including more than 200 high voltage transformers imported from China since year 2008). Our government already has this information, but ITC databases are often difficult for the public to utilize.

We have already requested that the Energy Information Agency (EIA), a sister component of DOE, adapt the ITC time series on critical grid equipment that have been imported from China and other nations since 2004. If EIA were to publish a publicly-facing time series on key types of equipment and their country of origin, EIA could make available to the government and the public a more comprehensive understanding of what needs to be done to develop “whitelisted” or other better protected transformers, hardware, software, and firmware.

Attached as **Appendix C** is a July 6, 2020 letter our Secure the Grid Coalition provided to EIA with this request. We request that your staff engage EIA on this topic to enlist that agency’s capabilities to assist with your efforts to fulfill Executive Order No. 13920.

² <https://securethegrid.com/2020/05/12/supply-chain-cybersecurity-complaint-filed-with-ferc/>

³ Visit this site and enter “EL-20-46” into the search bar: https://elibrary.ferc.gov/idmws/docket_search.asp

⁴ After serving in the U.S. Navy as an intelligence analyst, George Cotter joined the National Security Agency in 1952 and served there for more than forty years, rising to the rank of Chief Information Officer (CIO.)

Finally, one significant issue is the criticality of these transformers. There may only be a small percentage of the total number of transformers that are extremely critical to the operation of the BPS but the RFI doesn't ask about this criticality. Determining this criticality should be an immediate priority alongside determining which of these have been manufactured by or compromised by foreign adversaries. Of course, this criticality determination should NOT be made public but rather inform DOE's process of triaging those which must be inspected/addressed first.

2 - Test Duke's Large Power Transformer Against Realistic EMS and Cyber Threats

Pictured below is a Large Power Transformer donated by Duke Energy to the U.S. Government's Savannah River National Laboratory (SRNL) and Clemson University to be tested against realistic electromagnetic spectrum (EMS) threats such as High Altitude Electromagnetic Pulse (HEMP) and Intentional Electromagnetic Interference (IEMI) as well as realistic cyber threats. This transformer has been sitting idle and deteriorating for over two years for lack of less than a million dollars from your Department of Energy (DOE) to ship it up the Savannah River to SRNL to prepare it for testing in an already prepared location. Our Coalition believes that this inaction is absolutely unacceptable, and that this transformer should be immediately transported and funded for intensive, but easily affordable, testing according to proposals submitted to the DOE many months ago. If DOE requires point-of contact information for those involved with donating this transformer as well as appropriate DOE points-of-contact, please contact us (our POC information at the bottom of this document.)



3 - Immediately Protect Large Power Transformers from Direct Current:

We suggest neutral blocking as an immediate priority – to quickly protect the critical and very hard to replace transformers, generators and high voltage breakers of the bulk power system using tested and available hardware at relatively low cost.

Our alternating current (AC) bulk power system and its major components are not designed for direct current (DC). The significant effects of solar storms on the power grid are very similar to E3 HEMP in that they both induce quasi-DC currents in the ground which enter the bulk power system through the high voltage transformer neutral wires. A large Solar Storm or HEMP event could induce high levels of DC that are orders of magnitude greater than anything we have ever experienced on the

modern grid. The results would be catastrophic to the grid and cause widespread and protracted blackouts.

We must keep DC out of our AC grid to allow critical components to operate as designed and remove the risks of voltage collapse, damage, cascading failures as well as many uncertainties in a HEMP attack or large Solar Storm event. With long lead times required to replace and the ever-increasing dependence on foreign entities for the critical components on our bulk power system, the mission to protect what is already installed on our grid is even more important.

Any protection plan against the threats of (intentional) HEMP and (statistical) major Solar Storms, must include blocking these induced DC currents from invading our AC bulk power system, as recommended by the Electric Power Research Institute (EPRI), US Congressional EMP Commission, Idaho National Laboratory, US Air Force Electromagnetic Defense Task Force and many others, as noted below:

“A capacitor in the neutral of transformers was determined to be the most effective and practical blocking device.”

-EPRI EL-3295, Project 1770-1, Mitigation of Geomagnetically Induced and DC Stray Currents, 1983

“...inserting blocking devices in the neutral leads appears to be the most logical and effective means of preventing GIC flow.”

-EPRI TR-100450, Proceedings: Geomagnetically Induced Currents Conference, 1992

“The E3 pulse is similar in a great many respects to geomagnetic effects induced by solar storms... Steps taken to mitigate the E3 threat also would simultaneously mitigate this threat from the natural environment.”

-Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, 2008

“Installation of blocking devices in the neutral to ground connections of transformers will significantly reduce the probability of damage from solar storms and ... EMP E3”

-Risk-Based National Infrastructure Protection Priorities for EMP and Solar Storms, Report to the Commission to Assess the Threat to the United States from EMP Attack, Baker, July 2017, p. 8

“The use of capacitors in the neutral of grounded-wye transformers...is an effective means of blocking the flow of GIC in transformer windings.”

-EPRI 3002014979, High-Altitude EMP and the Bulk Power System, Potential Impacts and Mitigation Strategies, April 2019

“Recommendations For Further Action...Invest in the \$2.5 billion to protect existing EHV transformers (all hazards = neutral ground blockers ...”

-Electromagnetic Defense Task Force 2018 Report, Stuckenberg, Woolsey, DeMaio, p. 48 – 49

“...there must be a priority to protect the most critical large power transformers in place... estimates are that this would cost less than \$4 billion if we made it a priority to install NBD’s [neutral blocking devices] at our most critical EHV substations. This is a small fraction of the value of replacement units, but more importantly is negligible compared to the loss of civilian life and long term recovery costs to the economy should they fail during a GMD or EMP event.”

-Statement before the U.S. Senate Homeland Security & Government Affairs Committee, Scott A. McBride, Infrastructure Security Manager, National & Homeland Security, Idaho National Laboratory, 2018

[Importantly, our Coalition receives no funding from the corporations that could profit from protecting these transformers from Direct Current.]

4 - Immediately Protect Large Power Transformers from Physical Sabotage / Small Arms Fire:

The comments submitted by AK Steel provide ample evidence of the need for our Large Power Transformers to be protected from physical sabotage, including small arms fire.

Meanwhile, the North American Electric Reliability Corporation (NERC) has established CIP-14-2 (Physical Security) as the only mandatory physical security standard that is supposed to protect the bulk power electric system. Your agency should be fully aware through the OE-417 report data that since CIP-14-2 became effective on October 2, 2015, there have been 245 physical attacks on the grid.

Members of our Secure the Grid Coalition, including its Co-Chairman Ambassador R. James Woolsey (former Director of Central Intelligence) have long argued that this standard is insufficient since it does not actually require protection of these transformers from sabotage or small arms fire and since it is fraught with loopholes.⁵ Unfortunately, the electric power industry and NERC disagreed and were successful in lobbying the Federal Energy Regulatory Commission (FERC) to maintain a “hands off” approach to strengthening the physical security standard or ensuring that it is aggressively enforced.⁶

This has convinced our Coalition that it will be up to the Department of Energy to rapidly identify the most important and most vulnerable transformers and begin protecting them using existing protection technologies, funded by American tax dollars. Our Coalition is ready and willing discuss with appropriators in Congress the importance of allocating funding for this necessary action.

Ballistic protection of transformers can be installed by numerous vendors, ranging from SIEMENS PreTact to OmniThreat Structures, to GigaCrete. In fact, GigaCrete’s substation protection capabilities have been known by leaders in your agency who six years ago witnessed its ability to provide ballistic protection to vital grid assets.

Appendix D is a copy of the capabilities presentation provided to the Department of Energy’s Special Assistant to the President at B&W Y-12, Judy Johns, in August of 2014. GigaCrete’s cost-effective protection against ballistic threats to transformers has been available for six years and yet not a single industry or government entity has demonstrated interest in using it to protect vital assets, which

⁵ <https://securethegrid.com/2020/03/04/former-cia-director-james-woolsey-on-grid-physical-security/>

⁶ For the official public record on this unfortunate saga, see FERC Docket No. EL20-21-000. For a succinct summary, visit this site, maintained by one of our Secure the Grid Coalition Members, retired U.S. Army Command Sergeant Major Michael Mabey: <https://michaelmabee.info/ferc-denies-grid-physical-security-complaint/>

underscores the necessity of the President's most recent Executive Order to secure the bulk power electric system. We encourage your agency to take this order and move as aggressively as possible to protect these vital assets from physical sabotage and small arms fire.

[Importantly, our Coalition receives no funding from the corporations that could profit from protecting these transformers.]

Request 2

Prohibit the Use of Robotics, Including Drones, that Introduce & Highlight Grid Vulnerabilities

The threat of espionage and cyberattack using industrial control systems are a well-known vulnerability of the power grid. These vulnerabilities, however, are not limited to the devices and systems that make up or are permanently attached to the grid. The surveillance, inspection, and maintenance of the US power grid is increasingly exposed to a new vector for these types of attacks in the form of robotics. A wide array of robotic technology is being integrated into the routine operations of the national power grid.

For example, drones are now utilized to inspect powerlines and substation installations. Wire-crawling robots inspect and make repairs of transmission lines.⁷ Ground and aerial robotics are utilized for direct installation, repair, and corridor maintenance.⁸ Many of these robotic systems are made in or source key technology components from foreign countries such as China. In fact, the U.S. Government is on alert having identified this security threat in Chinese drones and banned the operation of the popular drones that are Made in China across multiple federal agencies.⁹

There is no doubt robotic technology provides significant advantages in the safety, speed, and scale of operations needed to detect problems and prevent failures in our aging power infrastructure. Unfortunately, these systems also introduce dangerous new vulnerabilities. The rapid pace of innovation and cost advantages of introducing new technologies have often taken on greater importance than security considerations. Without proper regulation, the industry is disincentivized to properly consider the threats introduced by robotics.

Foreign adversaries can utilize this technology to aid multiple attacks on our grid. For example, previous examples include Chinese drone-maker DJI collecting and storing data collected by unsuspecting drone operators in unsecured cloud repositories.¹⁰ This information can be utilized to not only assess grid equipment condition and vulnerability but may also be used to identify targets and aid planning for cyberattacks. Less obviously, many foreign drones also require that these devices “phone home” to authorize each operation in order to comply with airspace regulations and license agreements. This forced collection of metadata provides information about the location, frequency, and other operations data that can be analyzed for vulnerabilities.

Finally, as in all networked devices, there is the threat of hostile takeover to control or disable these robotic devices, which may be utilized to disrupt operations or worse. New vulnerabilities are routinely discovered in these seemingly innocent consumer devices. In fact, the Heritage Foundation

⁷ <https://www.therobotreport.com/overhead-transmission-line-inspection-robots/>

⁸ <http://krafttelerobotics.com/industries/electric/distribution.html>

⁹ <https://www.doi.gov/pressreleases/secretary-bernhardt-signs-order-grounding-interiors-drone-fleet-non-emergency>

¹⁰ <https://cybersafe.mcttrainingconsultant.com/securityattack/researchers-reveal-new-security-flaw-affecting-chinas-dji-drones/>

recently published a comprehensive report on this topic, mostly directed toward DoD, DOJ, and DHS. Its summary reads:

The vast majority of commercial drones used in the U.S. are manufactured in China, and their operating systems are impressive and worrisome. The technology is advancing rapidly, and the capabilities currently found in large drones is now being miniaturized and will likely migrate to smaller drones in the near term, which will significantly broaden the threat. However, the understanding of the risk and/or the willingness for state and local agencies to thwart those drones from collecting sensitive data is limited—at best. The United States government needs to address and stop the collection and transfer of data by drones to any foreign-based corporation before this incredible capability is turned against us.

-Heritage Foundation report titled “Chinese-Made Drones: A Direct Threat Whose Use Should Be Curtailed”, John Venable and Lora Ries, 19 August 2020¹¹

We therefore urge *your agency* to consider security requirements for all robotic devices being utilized for operations on the electric grid in order secure this emerging threat. These include developing appropriate policies to safeguard the networked operations of robotics from both external and internal threats, the proper identification, labelling, and control of data and metadata related to robotic operations on critical national infrastructure, and in general to receive the same level of security scrutiny as industrial control networks. The time to act is now, to promote mitigation of this threat before the rapid growth of robotics becomes a dangerous critical dependency of the bulk power system.

[Importantly, our Coalition receives no funding from corporations that produce drones or counter drone technology.]

Request 3

Withstand Influence on the Part of Industry Lobbyists to Maintain a “Business as Usual” Approach to Grid Security

As your agency can see clearly in Appendix A, the focus on grid protection in Congress has failed to result in meaningful and adequate action to secure the grid against all hazards. A large part of this failure has been the result of industry organizations and associations working in concert to lobby elected officials and pressure government officials NOT to require and/or enforce much-needed grid protections. In fact, according to the Center for Responsive Politics, the electric utility industry spent \$24,725,200 in political contributions and spent \$122,281,276 on lobbying in 2018¹². While we recognize that it is not illegal for our elected officials to take money from an industry tied to their oversight responsibilities, the net result has been a catastrophically vulnerable electric grid.

One of the largest and most effective lobbying organizations for the electric utility industry is Edison Electric Institute (EEI). For an example of how EEI can successfully influence Congress to avoid stricter security regulations for the bulk power electric system, we point your agency to a hearing

¹¹ <https://www.heritage.org/technology/report/chinese-made-drones-direct-threat-whose-use-should-be-curtailed>

¹² <https://www.opensecrets.org/cong/cmtes/profiles?cmte=HENE&cmtename=Energy+and+Commerce&cong=115&cycle=2018&indus=E08>

nearly a decade ago. On May 5th, 2011, the Committee On Energy And Natural Resources of the United States Senate, assembled to discuss a “Joint Staff Discussion Draft Pertaining To Cyber Security Of The Bulk-Power System.”

The opening statement of the Chairman, New Mexico Senator Jeff Bingaman, included the following relevant warnings:

As we upgrade and expand the Nation’s electric system we are also modernizing that system. Information technology and communication systems have come to play a significant role in ensuring the reliability and security of the electric sector. While modernization allows us to achieve a variety of important economic and environmental objectives, it also introduces new security concerns. As this process unfolds, preserving and enhancing the cyber security of our electric infrastructure must be among our top priorities.

So, let me highlight 2 things.

*First, the electric sector is already subject to a set of mandatory and enforceable cyber security standards that are developed by industry stakeholders and approved by the Federal Energy Regulatory Commission. This fundamentally distinguishes the electric sector from virtually all other critical infrastructure sectors. **However, I do not believe that the existing suite of reliability standards and the process for developing them is sufficient to defend electric infrastructure against deliberate cyber attacks and to address system vulnerabilities.** The new authorities contemplated in the discussion draft that we’ve circulated fill these gaps in a way that will help to complement current cyber security standards.*

*The second point I wanted to make is that today it’s almost 2 years since the day—since our cyber security hearing occurred in the 111th Congress. In fact, we are fortunate to welcome many of the same witnesses. The draft legislation we’re discussing today is very similar to the legislation we discussed in 2009. It recognizes positive changes in the standards development and approval processes. However, in the time since our last hearing the security environment has also changed and certainly much more quickly. Cyber related threats can arise virtually anytime/anywhere and change without warning. **For these reasons, there is no reason we should not delay in acting to enhance the cyber security of our electric system.***

During this hearing, EEL’s Executive Vice President for Business Operations, David Owens, provided the following testimony:

*“Section 215 mandatory reliability framework reflects years of work and broad consensus reached by industry and other stakeholders in order to ensure a robust, reliable grid. It should not be undermined so early in its implementation. While the open stakeholder processes used for developing industry-wide reliability and critical infrastructure protection standards admittedly are not well-suited to emergencies requiring immediate mandatory action with confidential handling of information, the vast majority of cyber security issues do not rise to the level of national security emergencies. **Rather than creating broad new federal regulatory authorities that could undermine the consensus-driven policy framework developed through years of stakeholder input and memorialized in section 215, legislation should be focused on addressing a relatively narrow set of potential threats that legitimately merit special federal emergency authority.** Because of its extraordinary nature and potentially broad impacts on the electric system, any additional federal emergency authority in this area should be used judiciously. Legislation granting such authority should be narrowly crafted and limited to*

address circumstances where the President or his senior intelligence or national security advisors determine there is an imminent threat to national security or public welfare.”

We observe that nearly a decade after this hearing, EEI’s (and its industry partners’) successful lobbying to promote the industry’s “consensus-driven policy framework” has consistently reduced federal (and state) authorities and necessitated that the President of the United States declare a “grid security emergency” with his Executive Order 13920.

We recognize that EEI’s lobbying of Congress to avoid grid security enhancing legislation and/or regulations is outside the purview of your agency but we still believe it is relevant since it should drive home the importance of your agency recognizing the need to “run with” the authority granted you in Executive Order 13920 to rapidly secure the grid. It is also relevant because your agency can be influenced and lobbied by industry groups like EEI and potentially misinformed by industry research organizations like the Electric Power Research Institute (EPRI).

Your agency should take, for example, the relationship between EPRI’s research into High Altitude Electromagnetic Pulse (HEMP) and the course of lobbying by the electric power industry to avoid aggressive HEMP protection efforts.

In EPRI’s journal in a 2017 article titled “*From Doomsday to Reality*” *EPRI Research to Inform Smart Decisions on High-Altitude Electromagnetic Pulses*,” EPRI stated that its research “is meant to provide utilities, federal and state regulators, and policymakers with information to guide policy and investment decisions.”¹³

Three years later, when EPRI released its HEMP research findings, EEI Vice President for Security and Preparedness Scott Aaronson confirmed that EPRI “research enables electric companies to make science-informed decisions for developing, testing, and deploying EMP-resistant grid components. Sound policy should be informed by sound science.”¹⁴

This coordinated effort between EEI and EPRI helped generate significant media buzz about EPRI’s HEMP research. Wired Magazine ran an article on April 30, 2019 titled “*The Grid Might Survive an Electromagnetic Pulse Just Fine*”¹⁵ and Forbes published one three days later stating that “*The country’s preeminent electric research institution has diminished the idea that a high-altitude electromagnetic pulse (HEMP) from a nuclear missile attack above Earth’s atmosphere would fry the U.S. electric grid and bring our economy to a screeching halt.*”¹⁶

This coordinated EEI & EPRI public messaging misled the very “utilities, federal and state regulators, and policymakers” who were the intended recipients of this research into falsely and optimistically believing that a HEMP attack on the United States would cause only localized or regional blackouts of relatively short duration.

In its report titled “*Electromagnetic Pulse Threats to America’s Electric Grid: Counterpoints to Electric Power Research Institute Positions*” and published on August 27, 2019, the U.S. Air Force’s Electromagnetic Defense Task Force (EDTF) concluded “**that the methodology and findings of the**

¹³ <http://eprijournal.com/wp-content/uploads/2017/05/epri-journal-2017-no-2.pdf>

¹⁴ <https://www.eei.org/resourcesandmedia/newsroom/Pages/Press%20Releases/EEI%20Statement%20on%20EPRI%E2%80%99s%20New%20Report%20on%20the%20Potential%20Impact%20of%20an%20Electromagnetic%20Pulse%20on%20the%20Electric%20Transmission%20System.aspx>

¹⁵ <https://www.wired.com/story/the-grid-might-survive-an-electromagnetic-pulse-just-fine/>

¹⁶ <https://www.forbes.com/sites/dipkabhambhani/2019/05/03/emp-study-threat-to-u-s-grid-is-manageable-electric-sector-says-it-would-be-ready/#2fc2d59c7c27>

EPRI report are inconsistent with the 60+ years of DOD research and experience in understanding EMP environments, system effects, and protection requirements and that the report dangerously and inadequately characterizes impacts on the US electric grid for an EMP event.”¹⁷

The EDTF pointed out dozens of flaws with EPRI’s research but perhaps the most significant illustration of just how unrealistic EPRI’s assertions were, came in the EDTF’s comparison of their HEMP research to the 2003 Northeast blackout. The EDTF Report stated:

*“According to EPRI’s test results, a high-altitude EMP attack would cause relay malfunctions at thousands of points in the grid, simultaneously. Notably, large-scale grid blackouts have occurred in the past from single-point failures, such as the Northeast Blackout of 2003 which was caused by overgrown trees contacting electric transmission lines. According to the North American Electric Reliability Corporation (NERC) technical analysis of this blackout, it affected more than 70,000 megawatts (MW) of electrical load and left an estimated 50 million people without power. In contrast, **EPRI’s report concludes that a HEMP attack on the same Eastern Interconnection would cause limited regional voltage collapses and affect roughly 40 percent of the electrical load lost in the 2003 blackout.** Experience with cascading collapse in the Eastern Interconnection shows EPRI’s finding to be optimistic in the extreme.”* (Emphasis added)

This example of the EEI/EPRI research/messaging collaboration is provided for your agency as part of these comments because it is highly relevant to your agency and especially at this very moment in time. The HEMP research itself was conducted as part of “A Collaborative Effort of the U.S. Department of Energy and the Electric Power Research Institute” as noted on the title of your agency’s “Joint Electromagnetic Pulse Resilience Strategy.”¹⁸

The public messaging campaign by EEI and EPRI, which made effective use of their collaboration with *your agency*, took place immediately following President Trump’s issuance of Executive Order on Coordinating National Resilience to Electromagnetic Pulses¹⁹ and **provided policymakers the opportunity to point to “research” that dangerously downplayed the HEMP threat.** This effective influence on the part of EEI/EPRI with respect to HEMP puts our nation in grave danger.

Now that the President of the United States has declared a national emergency and issued Executive Order 13920: “Securing the United States Bulk-Power System”²⁰ your agency can expect comments and influence from electric industry trade associations and research institutes like EEI and EPRI to potentially downplay the need for aggressive action to realize the goals of the Executive Order. We implore you to resist this influence and to move forward rapidly and aggressively as though your lives, and that of your families, depend upon it – because they do.

[Importantly, our Coalition receives no funding from corporations that, can protect the grid and, as a 501c3 non-profit, can conduct only limited lobbying activities, all of which are directed toward encouraging sound national security policy.]

¹⁷ <https://othjournal.com/2019/08/27/electromagnetic-pulse-threats-to-americas-electric-grid-counterpoints-to-electric-power-research-institute-positions/>

¹⁸ https://www.energy.gov/sites/prod/files/2016/07/f33/DOE_EMPStrategy_July2016_0.pdf

¹⁹ <https://www.whitehouse.gov/presidential-actions/executive-order-coordinating-national-resilience-electromagnetic-pulses/>

²⁰ <https://www.govinfo.gov/content/pkg/FR-2020-05-04/pdf/2020-09695.pdf>

Request 4

Demand Trusted Personnel & Organizations to Immediately Cease Ties With Foreign Adversaries

We believe that a trusted supply chain is only one part of the equation when it comes to grid security. Perhaps even more important are trusted personnel and organizations influencing grid-security policy – personnel and organizations free from influence by nation’s defined as “foreign adversaries.”

If your agency is to fulfill the spirit and intent of the Executive Order, it must take an extremely hard look at the personnel and organizations that comprise the entities trusted most by your agency, such as the Electricity Subsector Coordinating Council (ESCC). The ESCC “serves as the principal liaison between the federal government and the electric power industry, with the mission of coordinating efforts to prepare for, and respond to, national-level disasters or threats to critical infrastructure.”²¹ According to your agency’s regulations, specifically 10 CFR § 205.38:

“Electricity Subsector Coordinating Council (ESCC) means the organization that aims to foster and facilitate the coordination of sector-wide, policy-related activities and initiatives designed to improve the reliability and resilience of the electricity subsector, including physical and cyber security infrastructure.”²²

...and according to 10 CFR § 205.383 – Consultation:

(a) To obtain information related to a particular grid security emergency and recommended emergency measures from those government entities, electric reliability organizations, and private sector companies, and their respective associations where applicable, affected by the emergency, the Department of Energy's Office of Electricity Delivery and Energy Reliability will conduct consultation related to each emergency order. Before an emergency order is put into effect and, to the extent practicable in light of the nature of the grid security emergency and the urgency of the need for action, efforts will be made to consult with at least the following, as appropriate:

(1) The Electricity Subsector Coordinating Council;²³

Clearly, the ESCC is a highly trusted entity by your agency and other agencies within the federal government. Meanwhile, this highly trusted entity contains both EEI and EPRI as formal members.²⁴ Both of these organizations have deep ties with at least one nation defined as a “foreign adversary” – the People’s Republic of China. In addition to being on the ESCC, EEI is on this official DOE advisory committee, the Electricity Advisory Committee (EAC)²⁵.

Because of the highly-problematic and potentially dangerous association between EEI, EPRI and the PRC, members of our Coalition submitted two motions to the Federal Energy Regulatory

²¹ <https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure>
<https://energycollection.us/Energy-Security/ESCC-Electricity-Subsector.pdf>
<https://www.naseo.org/Data/Sites/1/documents/2017-institute/escc-initiatives-june-2017.pdf>
<https://www.cisa.gov/sites/default/files/publications/Energy-Electricity-SCC-Charter-2013-508.pdf>
https://www.electricitysubsector.org/-/media/Files/ESCC/Documents/ESCC_Brochure_July2019.ashx

²² <https://www.govinfo.gov/app/details/CFR-2020-title10-vol3/CFR-2020-title10-vol3-sec205-380>

²³ <https://www.govinfo.gov/app/details/CFR-2020-title10-vol3/CFR-2020-title10-vol3-sec205-383>

²⁴ <https://www.cisa.gov/energy-electricity-subsector-charters-and-membership>

²⁵ <https://www.energy.gov/oe/electricity-advisory-committee-eac>

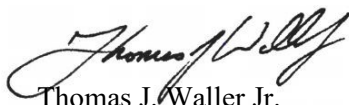
Commission suggesting that these organizations be excluded from intervening on dockets involving national security and further suggesting that the Office of Energy Infrastructure Security (OEIS) establish a certification criteria and procedure for organizations intervening in dockets involving U.S. National 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. Our motions went unanswered. Thus, we trust that the civil servants in your agency will take this notification seriously. **Appendix E** and **Appendix F** are copies of these motions filed with FERC and provide your agency ample evidence of the dangerous entanglement of EEI and EPRI with the People's Republic of China.

After our Coalition filed these motions to FERC, the U.S. Department of Defense (DoD), fulfilled a statutory requirement to disclose the presence inside the United States of companies tied directly or indirectly to the Chinese Communist Party's People's Liberation Army (PLA).²⁶ This list included two companies actively working with EPRI on nuclear research. We find it extremely disturbing that that EPRI can work with your agency and other government entities on important national security research/collaboration and also work with the preeminent elements of the PRC's military-industrial complex such as its two state-owned nuclear corporations. Therefore, we believe that your agency MUST require that any entity on the ESCC 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.

[Importantly, our Coalition receives no funding from any foreign entity or from any government within the United States.]

In conclusion, Mr. Kosak, our Secure the Grid Coalition would like to offer you and your staff any and all assistance we can provide to help you rapidly implement the tasks associated with Executive Order 13920. We hope that these comments will provide you with helpful suggestions and that you will take action upon them posthaste.

Sincerely,



Thomas J. Waller Jr.
Director, Secure the Grid Coalition
Contact: info@SecureTheGrid.com

²⁶<https://www.cotton.senate.gov/files/documents/Sen%20Cotton%20NDAA%20FY%201999%20Sec%201237%20Response%2006242020.pdf>

Appendix A

Hearings to and Legislation from the Congress relating to the Protection of the Grid

1997-07-16	Threat Posed By Electromagnetic Pulse (EMP) to US Military Systems and Civil Infrastructure, Before US House Subcommittee on Military Research and Development of the Committee on National Security, 105th Congress (July 16, 1997). http://bit.ly/379LVry
1999-06-01	Electromagnetic Pulse (EMP): Should This Be a Problem of National Concern to Private Enterprise, Businesses Small and Large, As Well As Government? Before the US House, Subcommittee on Government Programs and Oversight of the Committee on Small Business, 106th Congress (June 1, 1999). http://bit.ly/37eCFIS
2001-09-05	S.1407 Critical Infrastructures Protection Act of 2001. 107th Congress. http://bit.ly/342xK51
2003-09-03	Blackout 2003: How Did It Happen And Why? Before the Committee on Energy and Commerce. (108th Congress) September 3, 2003. http://bit.ly/2qXsgKY
2003-09-04	Implications of Power Blackouts For The Nation's Cybersecurity and Critical Infrastructure Protection, Before the US House, Joint Hearing of the Subcommittee on Cybersecurity, Science, and Research and Development, and the Subcommittee on Infrastructure and Border Security of the Select Committee On Homeland Security, 108th Congress (September 4 & 23, 2003). http://bit.ly/2qV9La3
2003-09-10	Keeping The Lights On: The Federal Role In Managing The Nation's Electricity. Before the Committee on Governmental Affairs, Oversight of Government Management, the Federal Workforce and the District of Columbia Subcommittee. (108th Congress) September 10, 2003. http://bit.ly/357GCHh
2003-09-23	Keeping The Lights On: Removing Barriers To Technology To Prevent Blackouts. Before the Committee on Energy. (108th Congress) September 25, 2003. http://bit.ly/2qk0R5U
2003-10-30	What Is Space Weather and Who Should Forecast It? Before the US House, Subcommittee on Environment, Technology, and Standards, Committee on Science, 108th Congress (October 30, 2003). http://bit.ly/2Qqpdpl
2004-07-22	The Report of the Commission to Assess the Threat to the U.S. from Electromagnetic Pulse Attack, Before the US House Committee On Armed Services, 108th Congress (July 22, 2004). http://bit.ly/2KuCiHg or http://bit.ly/2NSq14l
2005-03-08	Terrorism and the EMP Threat to Homeland Security, Before the US Senate, Subcommittee on Terrorism, Technology and Homeland Security of the Committee on the Judiciary, 109th Congress (March 8, 2005). http://bit.ly/2Qri9c6
2005-09-15	Cyber Security: US Vulnerability and Preparedness, Before the US House, Committee on Science, 109th Congress (September 15, 2005). http://bit.ly/2NSSjvB

2007-01-04	H.R.61 - To amend the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 to extend the deadline for the submission of the final report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack, to provide for the appointment of additional members for the Commission, to ensure the availability of funds for the Commission, and for other purposes (110th Congress) January 4, 2007. http://bit.ly/32PIJhn
2007-10-17	The Cyber Threat to Control Systems: Stronger Regulations Are Necessary To Secure the Electric Grid. Before the Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology. (110th Congress) October 17, 2007. http://bit.ly/2qk3Dbk
2008-05-21	Implications of Cyber Vulnerabilities on the Resilience and Security of the Electric Grid. Before the Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology. (110th Congress) May 21, 2008. http://bit.ly/32S7TvX
2008-07-10	Threat Posed by Electromagnetic Pulse (EMP) Attack, Before the US House, Committee on Armed Services, 110th Congress (July 10, 2008). http://bit.ly/2qXzYEU
2008-09-16	Defeating the Improvised Explosive Device (IED) and Other Asymmetric Threats: Today's Efforts and Tomorrow's Requirements, Before the US House, Oversight and Investigations Subcommittee of the Committee on Armed Services, 110th Congress (September 16, 2008). http://bit.ly/32UAHE7
2009-04-29	H.R.2165 - Bulk Power System Protection Act of 2009. 111th Congress. http://bit.ly/2t00ezz
2009-04-30	S.946 - Critical Electric Infrastructure Protection Act of 2009. 111th Congress. http://bit.ly/2YtyDCh
2009-04-30	H.R.2195 - To amend the Federal Power Act to provide additional authorities to adequately protect the critical electric infrastructure against cyber attack, and for other purposes. 111th Congress. http://bit.ly/2Yvk1Ta
2009-07-15	Addressing a New Generation of Threats from Weapons of Mass Destruction: Department of Energy Nonproliferation Programs and the Department Of Defense Cooperative Threat Reduction Program. Before the House Committee on Armed Services. (111th Congress) July 15, 2009. http://bit.ly/2rR735P
2009-07-21	Securing the Modern Electric Grid from Physical and Cyber Attacks, Before the US House, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology of the Committee on Homeland Security, 111th Congress (July 21, 2009). http://bit.ly/2CS026R
2009-10-15	H.R.3832 - Peace Through Strength Act of 2009 (111th Congress) October 15, 2009. http://bit.ly/2QsHnXo
2009-10-27	Protecting the Electric Grid: H.R. 2165, The "Bulk Power System Protection Act of 2009," and H.R. 2195, Before the US House, Subcommittee on Energy and

	Environment of the Committee on Energy and Commerce, 111th Congress (October 27, 2009). http://bit.ly/376IKCd
2009-11-18	Resourcing the National Defense Strategy: Implications of Long Term Defense Budget Trends, Before the US House, Committee on Armed Services, 111th Congress (November 18, 2009). http://bit.ly/375gBtY
2010-04-14	H.R.5026 - "Grid Reliability and Infrastructure Defense Act" or the "GRID Act." 111th Congress. http://bit.ly/2LATTKt
2010-05-25	Grid Reliability and Infrastructure Defense Act. House Report 111-493. (111th Congress) May 25, 2010. http://bit.ly/32Wk5M6
2010-08-04	Government Preparedness and Response to a Terrorist Attack Using Weapons of Mass Destruction, US Senate, Subcommittee on Terrorism, Technology and Homeland Security of the Committee on the Judiciary, 111th Congress (August 4, 2010). http://bit.ly/32QoJuX
2010-09-27	Grid Reliability and Infrastructure Defense Act. Senate Report 111-331. (111th Congress) Sept. 27, 2010. http://bit.ly/2OfRb4i
2010-12-01	H.R.6471 - EMP Weapons Accountability Assessment Act (111th Congress) December 1, 2010. http://bit.ly/2XpCDDh
2011-02-11	H.R. 668 Secure High-voltage Infrastructure for Electricity from Lethal Damage Act; SHIELD Act. (112th Congress) February 11, 2011. http://bit.ly/2CNHGUv
2011-05-05	Cyber Security, Before the US Senate, Committee on Energy and Natural Resources, (112th Congress) May 5, 2011. http://bit.ly/33Pq5HP
2011-05-31	Protecting the Electric Grid: H.R. - - - , The Grid Reliability and Infrastructure Defense Act, Before the US House, Subcommittee on Energy and Power of the Committee on Energy and Commerce, (112th Congress) May 31, 2011. http://bit.ly/2puAaes
2011-06-24	H.R.2348 - EMP Weapons Accountability Assessment Act (112th Congress) June 24, 2011. http://bit.ly/2KqgvmT
2011-07-11	Senate Report 112-34 Grid Cyber Security Act. (112th Congress) July 11, 2011. http://bit.ly/378xXGI
2011-07-11	S.1342 - Grid Cyber Security Act (112th Congress) July 11, 2011. http://bit.ly/2NSZh3N
2011-10-13	Update On Kc-46a and Legacy Aerial Refueling Aircraft Programs, Before the US House, Subcommittee on Seapower and Projection Forces of the Committee on Armed Services, 112th Congress (October 13, 2011). http://bit.ly/2Xk1dpa
2012-02-14	S.2105 - Cybersecurity Act of 2012. (112th Congress). http://bit.ly/346BLoO
2012-02-16	Senate Hearing: S.Hrg. 112-524 Securing America's Future: The Cybersecurity Act of 2012. (112th Congress) http://bit.ly/36f90rB Transcript: http://bit.ly/2E1Yjwm

2012-07-17	Electric Grid Security, Before the US Senate, Committee on Energy and Natural Resources, 112th Congress (July 17, 2012). http://bit.ly/32UHPAh
2012-07-17	S. Hrg. 112-529 Senate Hearing: Electric Grid Security. (112th Congress) July 17, 2012. http://bit.ly/36A0SCn
2012-08-02	H. Res. 762: Expressing the sense of the House of Representatives regarding community-based civil defense and power generation (112th Congress) August 2, 2012. http://bit.ly/37m9mOC
2012-09-12	The EMP Threat: Examining the Consequences. Hearing before the Homeland Security Committee, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies. Serial No. 112-115. (112th Congress) September 12, 2012. http://bit.ly/2NT4c4G
2013-05-21	Cyber Threats and Security Solutions, Before the US House Committee on Energy and Commerce. (113th Congress) May 21, 2013. http://bit.ly/2NTmlQ5
2013-05-21	Markey, Edward J. and Waxman, Henry A. Electric Grid Vulnerability: Industry Responses Reveal Security Gaps. US House of Representatives. May 21, 2013. http://bit.ly/2K896IU
2013-06-07	House Report 113-102 National Defense Authorization Act. (113th Congress) June 7, 2013. http://bit.ly/35a8sTj
2013-06-18	H.R. 2417 Secure High-voltage Infrastructure for Electricity from Lethal Damage (SHIELD Act), (113th Congress) June 18, 2013. http://bit.ly/37exdja
2013-08-01	H.R. 2962 - The Saving More American Resources Today (SMART) Grid Study Act of 2013. (113th Congress) August 1, 2013. http://bit.ly/2PdHhIA
2013-10-30	H.R. 3410 To amend the Homeland Security Act of 2002 to secure critical infrastructure against electromagnetic pulses, and for other purposes. (113th Congress) October 30, 2013. [This Act may be cited as the "Critical Infrastructure Protection Act" or "CIPA"] http://bit.ly/37asZJe
2013-10-30	H.R.3410 - Critical Infrastructure Protection Act (113th Congress) http://bit.ly/2qDkTbO
2013-10-31	S. 1638 - the Cybersecurity Public Awareness Act of 2013. (113th Congress) October 31, 2013. http://bit.ly/2selUpY
2013-12-11	H.R.3696 - National Cybersecurity and Critical Infrastructure Protection Act of 2014 (113th Congress) http://bit.ly/2P0KEMk
2014-03-26	Grid Reliability and Infrastructure Defense Act (GRID) Act. (113th Congress) March 26, 2014. Senate Bill S. 2158 http://bit.ly/2CMCJvr House Bill H.R. 4298 http://bit.ly/2NVP1aU
2014-04-10	S. Hrg. 113-271 "Electric Grid Reliability." (113th Congress) April 10, 2014. http://bit.ly/2rA99qV

2014-05-08	Electromagnetic Pulse (EMP): Threat To Critical Infrastructure. Before the House Committee on Homeland Security. 113th Congress (May 8, 2014). http://bit.ly/2qbyneG/a
2014-07-10	S. 2588 - The Cybersecurity Information Sharing Act of 2014 H.R. (113th Congress) July 10, 2014. http://bit.ly/2PEA8ti
2014-07-17	S.2620 - Grid Reliability Act of 2014 (113th Congress) July 17, 2014. http://bit.ly/38vszO8
2014-11-20	House Hearing: "Cybersecurity threats: the way forward" Before the House Select Intelligence Committee. November 20, 2014. Video: https://cs.pn/2rTDG2V Transcript: http://bit.ly/2Ku3UiV
2015-05-08	H.R.2244 - To establish a Strategic Transformer Reserve program, and for other purposes. (114th Congress) May 8, 2015. http://bit.ly/2NSq9Ys
2015-05-13	The EMP Threat: The State Of Preparedness Against the Threat of an Electromagnetic Pulse (EMP) Event. Before the House Subcommittee on National Security; Oversight and Government Reform. 114th Congress (May 13, 2015). http://bit.ly/2rK7WNk
2015-07-22	S. Hrg. 114-483 - Protecting the Electric Grid from the Potential Threats of Solar Storms and Electromagnetic Pulse. (114th Congress) July 22, 2015. http://bit.ly/2qY0ldS
2015-07-23	S.1846 - Critical Infrastructure Protection Act of 2016. 114th Congress. http://bit.ly/342aGDI
2015-08-04	House Report 114-240 - Critical Infrastructure Protection Act. (114th Congress) August 4, 2015. http://bit.ly/2OhMGq4
2015-11-16	H.R. 1073 Critical Infrastructure Protection Act. (114th Congress) November 16, 2015. http://bit.ly/2QB9p3d
2015-12-01	House Report 114-359 Providing for Further Consideration of the Bill (H.R. 8) to Modernize Energy Infrastructure. (114th Congress) December 1, 2015. http://bit.ly/2NUy5Sk
2015-12-02	H.R. 8 North American Energy Security and Infrastructure Act of 2015. (114th Congress) December 2, 2015. http://bit.ly/2CSu6Q2
2015-12-02	H. Amdt. 842 to H.R.8 North American Energy Security and Infrastructure Act of 2015. (114th Congress) December 2, 2015. http://bit.ly/2CSu6Q2
2016-04-14	House Hearing before the Subcommittee on Economic Development, Public Buildings, and Emergency Management. "Blackout! Are We Prepared to Manage the Aftermath of a Cyberattack or Other Failure Of The Electrical Grid?" (114th Congress) April 14, 2016. http://bit.ly/356HSdN
2016-05-09	Senate Report 114-250 - Critical Infrastructure Protection Act of 2015. (114th Congress) May 9, 2016. http://bit.ly/2CMEZCS

2016-05-09	Critical Infrastructure Protection Act of 2015, Report of the Committee on Homeland Security and Governmental Affairs United States Senate to Accompany S. 1846, (114th Congress) May 9, 2016. http://bit.ly/2CMEZCS
2016-05-17	House Hearing - Oversight of Federal Efforts to Address Electromagnetic Risks. (114th Congress) May 17, 2016. http://bit.ly/2KupeVe
2016-05-18	Assessing the Security of Critical Infrastructure: Threat, Vulnerabilities, and Solutions. Before the Committee on Homeland Security & Governmental Affairs. (114th Congress) May 18, 2016. http://bit.ly/2q259P9
2016-07-12	House Hearing - Value of DHS's Vulnerability Assessments in Protecting our Nation's Critical Infrastructure. (114th Congress) July 12, 2016. http://bit.ly/2pg7Jyd
2016-09-08	S.2012 - North American Energy Security and Infrastructure Act of 2016. (114th Congress) September 8, 2016. http://bit.ly/2OkDirV
2017-02-07	H.R.945 - Terrorism Prevention and Critical Infrastructure Protection Act of 2017. (115th Congress) February 7, 2017. http://bit.ly/355YS3V
2017-03-28	Senate Report 115-12. Activities of the Committee on Homeland Security and Governmental Affairs. (115th Congress) March 28, 2017. http://bit.ly/2Of5PZC
2017-05-04	House Hearing: Hearing to examine the threat posed by electromagnetic pulse and policy options to protect energy infrastructure and to improve capabilities for adequate system restoration. (115th Congress) May 4, 2017. http://bit.ly/2Q7JY91
2017-05-04	Testimony of Cheryl LaFleur Acting Chairman, Federal Energy Regulatory Commission Before the Committee on Energy and Natural Resources United States Senate May 4, 2017. http://bit.ly/2qbO7yi
2017-05-04	The Threat Posed by Electromagnetic Pulse and Policy Options to Protect Energy Infrastructure and To Improve Capabilities for Adequate System Restoration. May 4, 2017. http://bit.ly/33Uzspv
2017-05-17	H.R.2479 - Leading Infrastructure for Tomorrow's America Act (115th Congress) May 17, 2017. http://bit.ly/2Ktfwm6
2017-07-06	House Report 115-200 - National Defense Authorization Act for Fiscal Year 2018 (115th Congress) July 6, 2017. http://bit.ly/2NV9HA7
2017-07-10	Senate Report 115-125 - National Defense Authorization Act for Fiscal Year 2018 (115th Congress) July 10, 2017. http://bit.ly/2NTyu7D
2017-07-18	H.R. 2810 - National Defense Authorization Act for Fiscal Year 2018. (115th Congress) July 18, 2017. http://bit.ly/37eYWzY [See section 1699B: "Commission to Assess the Threat to the United States from Electromagnetic Pulse Attacks and Events."]

2017-07-20	Senate report 115-132 - Energy and Water Development and Related Agencies Appropriations Act, 2018 (115th Congress) July 20, 2017 (see page 74 "Infrastructure Security and Energy Restoration"). http://bit.ly/2XiRNKE
2017-09-12	S.1800 - Securing the Electric Grid to Protect Military Readiness Act of 2017. (115th Congress) September 12, 2017. http://bit.ly/37fs1LG
2017-09-27	H.R. 3855 - Securing the Electric Grid to Protect Military Readiness Act of 2017. (115th Congress) September 27, 2017. http://bit.ly/32UCsAU
2017-10-12	House Hearing, Homeland Security Committee. "Empty Threat or Serious Danger: Assessing North Korea's Risk to the Homeland" (115th Congress) October 12, 2017. http://bit.ly/2qbdX5y
2018-01-23	Senate Hearing, Committee on Energy and Natural Resources. "Full Committee Hearing to Examine the Performance of the Electric Power System Under Certain Weather Conditions." (115th Congress) January 23, 2018. http://bit.ly/356OBo0
2018-03-01	Senate Hearing, Committee on Energy and Natural Resources. "Full Committee Hearing to Examine Cybersecurity in our Nation's Critical Energy Infrastructure." (115th Congress) March 1, 2018. http://bit.ly/33Vkf7U
2018-03-09	H.R.5240 - Enhancing Grid Security through Public-Private Partnerships Act (115th Congress) March 9, 2018. http://bit.ly/2PcgOok
2018-05-22	H.R.4120 - Grid Cybersecurity Research and Development Act. (115th Congress) May 22, 2018. http://bit.ly/2qbeULa
2019-01-02	House Report 115-1127. Legislative and Oversight Activities of the Committee on Homeland Security 115th Congress. January 2, 2019. http://bit.ly/354XsXa
2019-01-09	H. Rept. 116-303 - Pipeline and LNG Facility Cybersecurity Preparedness Act. 116th Congress. http://bit.ly/37FV2ka
2019-01-09	H.R. 370. Pipeline and LNG Facility Cybersecurity Preparedness Act. 116th Congress. http://bit.ly/2rnkRo9
2019-02-14	Senate Hearing, Committee on Energy and Natural Resources. "Hearing to Consider the Status and Outlook for Cybersecurity Efforts in the Energy Industry." February 14, 2019. http://bit.ly/358p8dR
2019-02-27	Senate Hearing, Senate Committee on Homeland Security and Governmental Affairs. "Perspectives on Protecting the Electric Grid from an Electromagnetic Pulse or Geomagnetic Disturbance." February 27, 2019. http://bit.ly/2Ktg4lx Testimony of Dr. George Baker http://bit.ly/2rTPuCh
2019-05-02	H.R.2500 - National Defense Authorization Act for Fiscal Year 2020. 116th Congress. http://bit.ly/37u1nio

2019-05-02	H. Rept. 116-120 - National Defense Authorization Act for Fiscal Year 2020. 116th Congress. http://bit.ly/37w4WVu
2019-05-15	H.R.2741 - Leading Infrastructure for Tomorrow's America Act. 116th Congress. http://bit.ly/2QJrITS
2019-09-26	S.2556 - Protecting Resources On The Electric grid with Cybersecurity Technology Act of 2019. 116th Congress. http://bit.ly/2XO9GBr

Appendix B

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

April 11, 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 Motion to Intervene filing on Docket No. EL20-46-000
Related to Critical Infrastructure Supply Chain Reliability Standards.

Respectfully,

George R. Cotter

Enclosure: a/s

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

**Motion to Intervene in Docket)
Related to Critical Infrastructure)
Supply Chain Reliability Standards)**

Docket No. EL20-46-000

Submitted to FERC on June 11, 2020

Introduction

I, George R. Cotter, a private citizen, am filing this Motion to Intervene in Docket No. EL20-46-000 in accordance with 16 U.S. Code § 824o(d)(5) and 16 U.S. Code § 824o(e) in support of Mr. Mike Mabee's Complaint on this docket dated May 11, 2020. Mr. Mabee's Complaint focuses on the lack of transparency in Regulatory actions on Critical Infrastructure Protection violations by utilities, and the conflict of FERC Order No. 850 with Executive Order 13920. My Intervention adds significant background and additional challenges to Federal Energy Regulatory Commissions actions on Supply Chain vulnerabilities, and more importantly, the deliberate Commission policy of dissembling on security standards, the distortion and suppression of vulnerabilities in the North American Grid, and a conspiracy of cover-up actions in regulatory management of ERA Section 215 responsibilities to protect critical electric infrastructure.

Of note:

1. Eight years of delay, and counting, on Supply Chain risks after major penetrations of vendors by Russia in 2012, a full decade since, with major Supply Chain regulatory actions that will still be open past 2022.
2. Suppression of the FBI report on the follow-on 2014 lengthy Federation reconnaissance of the U.S. Electric Grid enabled by Supply Chain vulnerabilities.
3. Failing to secure electric power service to critical National Security facilities nearly totally dependent on commercial power; specifically, facilities known to be critical to response to such attacks.
4. Total failure to effectuate a 24/7 nation-wide utility BPS situational awareness, warning network.
5. Violating a public trust by facilitating a decade-long cover-up of electric system vulnerabilities and intrusions by foreign nation/state adversaries.
6. Despite the clear language of EPA Section 215, approving the exclusion of Grid communications and networks from CIP Standards, CIP-002.5.1a; the major pathway for adversary exploitation of Supply Chain, and other vulnerabilities.
7. Deliberate denial of Congress, the GAO, oversight Departments, Federal Agencies and State governments on security of BPS power feeds to Distribution systems through misuse of FAST Act provisions for protection of critical assets, i.e., CEII actions on CIP Violations
8. Ensuring that CIP Standards, all subject to approval by FERC, do not reveal and therefore compromise, the massive and insecure interconnection of BES and Distribution systems; i.e., less than 10% of BPS substations subject to CIP Standards, (see NASPI synchrophasor map Page 13.)

9. Prohibiting utility actions for vendors' culpability in Supply Chain attacks, including US vendors that supply major IT underpinnings for electric instrumentation (i.e., IT firms).

Comment: Most prior filings and White Papers have described CIP Standards as a veritable "House of Cards", superficially protecting management, organizational, internal systems; hardly a deterrence to the nation's adversaries targeting the electric power system. For this filing, the entire stack of "Reliability Standards" was shredded into CIP and non-CIP elements, and "Operational" cyber systems standards stood out in stark contrast to non-power cybersecurity standards, revealing the NERC/FERC cybersecurity protocol as the charade it is. Examine the table on P7, 476 pages of critical "operational" protection systems standards, whose cyber assets are absolutely devoid of cybersecurity wrappings.

Background

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.

For many years, this filer, and others have documented vulnerabilities and threats directly linked to current Critical Infrastructure Protection (CIP) standards.¹ These filings have intervened in NOPRs and Final Orders in public comment periods, with mixed but usually poor results. Filings have also been made on issues arising from questionable NERC and industry reports of CIP and other violations of Reliability Standards. And more recently, challenges including FOIAs objecting to the industry, NERC and FERC practice of redacting violation reports including inappropriate use of CEII to obscure utility identifications and critical details of infractions.

It would be a gross understatement to say that filers have seen steady deterioration of protection of the electric system from nation/state adversaries, largely due to weak standards, major delays on implementation, and negative effects on vendors from "Security through Obscurity". FERC has consistently used "divide and conquer" techniques in its policies of denial. The effect has been to add grave risk to unprotected Distribution systems, electrical supply to Critical Infrastructures, and place the Grid-dependent national security facilities responsible for protection of the nation, in dire jeopardy.

Additionally, for many years, FERC chairmen have also received this filer's White Papers on "***Security in the North American Grid***" with cover letters to key Congressional and Administration leadership. Themes included CIP Standards, utility vulnerabilities including Supply Chain issues, significant threats including malware development, U.S. incursions, testing abroad, and direct connectivity to 2016 and 2018 U.S. elections. FERC Commissioners have generally ignored these warning papers.

¹ See for example Isologic LLC, filing NOPR Supply Chain Risk Management Reliability, Docket No. RM17-13-000 Jan 18, 2018

In early days, these White Paper distributions were followed up with constructive meetings with Chairmen or Commissioners but this has ended. Chairman Chatterjee was sent the most recent White Paper² along with cover letters to Secretary of Defense and Co-Chairs of the Congressional Cyberspace Solarium Commission. That report was mainly to document the dire condition in the overall national Grid arising out of the growing divide between the reality of threats and contributions to that debacle by the FERC/NERC cover-up conspiracy.

Details

This filing centers on the frailties of Order No. 850 as well as the systemic weaknesses of what passes for BES security. The public, critical infrastructures, the national security community, and Congress is asked to believe that Order No. 850 will provide adequate Supply Chain protection of electric supply to their facilities. This filing will prove otherwise.

Those interested might fairly ask ***“What overall cybersecurity structure is in place to accommodate these changes to protect the end user?”***

So, Commissioners, let us examine your cybersecurity infrastructure ***and the stack of cyber assets, industry systems needing cybersecurity protection from adversaries, top down and end-to-end:***

1. Two national authorities, FERC and NRC, and 50 state authorities independently regulate cybersecurity protection for electric services but ***with no operational security coordination mechanism across the Grid as a whole.*** Supply Chain standards (Order No. 850) are applicable only to FERC-regulated Bulk Energy Systems (***but by no means, all such vulnerable systems, as will be documented in this filing.***)
2. NRC-controlled, nuclear generation sites transfer their power to Transmission (BES) substations and Distribution facilities to users but must import power for safety-critical systems. This import of power is generally considered contractually regulated, not federally regulated, ***i.e., outside the scope of Order No. 850.***
3. There is ***no Grid-wide operational “situational awareness” or alerting structure functioning across this three way digital divide*** to warn of Supply Chain attacks, incursions, incidents, campaigns, etc.
4. Coincidentally, therefore, there is ***no operational data exchange between these three separate domains***, no nation-wide data base on operational data, no concentrated examination of operational data for Supply Chain threat determination or actual adversary penetrations.
5. Further, ***a major source of Supply Chain vulnerabilities of domestic IT firms and which are endemic to BES/Transmission and Distribution facilities*** is exploited by nation/state adversaries; example: the 2014 U.S. Grid attack facilitated by a zero-day Microsoft system vulnerability.

² “Security in the North American Grid-Cybersecurity, CEI and the Digital Divide”, A White Paper, April 25, 2020

6. Bulk power is transmitted to/through state-regulated “Distribution” systems within and across 48/50 states to end users. ~1400 independent/semi-independent “registered” Generation and/or Transmission entities (i.e., utilities) ***independently categorize BES cyber systems*** (consisting of ***BES cyber assets***). That is what is subject, in theory, to Order No.850.
7. But many operational technology (OT) systems remain uncharacterized as ***BES*** cyber systems, although clearly have substantial ***cyber assets***. NERC’s extensive compendium of Reliability Standards³ differentiates, i.e., separately lists **CIP** standards from a plethora of Operational (OT) standards, labeled **BAL, COM, etc.** These **non-CIP** standards’ characterizations differing them from **CIP** standards, and are BES operational functions. ***There is no EPA 2005 Section 215 authorization for this policy and NERC is silent with no logical justification for such practice. This gives the nation’s adversaries engaged in Supply Chain attacks freedom of choice on industry targets.***

Comment: As cited above, a significant element of Supply Chain attacks is the exploitation of extensive security vulnerabilities in commercial Information technologies (IT). Most utility operational capabilities use commercial systems for data management, communications interfaces, enterprise management systems. Many such commercial IT systems host security vendor software for gateway protection. Importantly, these IT systems underpin energy-unique systems supplied for control systems and other energy-unique functions. If vulnerable to cyberattack, they represent a major complication in defense of Supply Chain attacks although not explicitly identified as such in Order No. 850. In 2014, a Microsoft system vulnerability was, in fact, the major portal for the Russian Federation attack using previously (in 2012) hacked control systems of three major industry control system vendors. An FBI investigation report was never made public. Federation tools were accordingly updated and tested the following year in the Ukraine. That relationship to the 2014 U.S. attack was significantly underplayed by FERC.

8. **BAL non-CIP** standards are where Balancing Authorities these days make extensive use of **DDR** and **Synchrophasor** systems as well as Data Processing Centers to manage operational power flows. These tools are now the principal source of quality data supplementing SCADA flows with higher precision results. NERC and the industry assiduously avoid characterizing these operational cyber assets under **CIP** standards, but the Russian Federation is targeting them you can be sure; see **Synchrophasor** map on Page 13.
9. Several other **non-CIP** Reliability Standards (e.g., **COM, EOP**) show clearly they are thinly-disguised efforts to keep Operational activities out of **CIP** categorization. Modern communications systems are heavily digital, highly automated, and therefore susceptible

³ NERC publication titled: “**Reliability Standards for the Bulk Electric Systems of North America**, Updated January 2, 2020” . This publication hosts all Reliability Standards; both CIP and non-CIP.

to Supply Chain attacks. Many of the **EOP**, non-CIP standards involve digital systems whose loss would jeopardize the operation of the BES, incident identification and reporting, also available vectors for Supply Chain attacks **but not covered by Order No. 850**.

10. **FAC** standards, notably Facility Interconnection requirements, Transmission Vegetation Management, System Operating Limits, Maintenance, Transfer Limits, etc., involve complex data aggregations, interoperability capabilities, real time monitoring functions and a host of planning and data exchange capabilities. These **non-CIP** cyber asset activities are natural targets for sophisticated information operations and therefore Supply Chain attacks by the nation's adversaries. The **PG&E** massive data base compromise and the abject vegetation management failure of this major utility had deadly consequences. All these **FAC** functions **are excluded from Order No. 850**.
11. The functions and capabilities required of Reliability Coordinators (RCs) are (major utilities) reflected in the **IRO** Reliability standard are replete with descriptions of data compilations, logging information and similar tools that are heavily automated both in data processing but also data exchange. **Such activities are massive operational cybersecurity targets in the heart of the Bulk Electric System**, but as with other **non-CIP** standards, **not covered by Order No. 850**.
12. Transmission operations, **TOP**, is a catch-all Reliability Standard that ensures that **each utility** involved in operations understands its unique (i.e., individual utility) responsibilities to the overall **BES**. As such, every cyber asset and cyber system within a utility is, **in principle**, subject to all of the NERC Reliability Standards. **TOP non-CIP** standards requirements are totally oriented to "Operations" and include 24 separate requirements each dealing with real-time actions and protection function. There are separate requirements addressing planning, data collection and retention, and monitoring and analysis activities. **TOP** activities therefore require each utility to employ cyber assets/systems applicable to any Reliability-Standards requirement across its entire footprint, from Enterprise Management Systems to each substation's interface with Distribution Systems. **There are no requirements citing Cybersecurity Standards, thus no obligatory utility linkages to Order No. 850**.
13. **TPL, non-CIP** Transmission System Planning Performance Requirements, is the Reliability Standards category describing all regulated functions involved in planning performance for the **BES**. Note that planning is collectively viewed as being so critical to the BES that utility's "**performance**" of the planning function is included in these standards. **TPL** therefore deals with cyber assets used in the performance of control systems, operations, data management, communications, monitoring and analysis. Although such **TPL** cyber systems are certain to be targeted by the nation's adversaries for Supply Chain vulnerabilities, they are **excluded from Order No. 850 controls**.
14. **TPL non-CIP** standards are even more concerning on emerging national cyber threat issues coupled to modernization (e.g., Synchrophasors, GPS, and "natural" events; weather, climate-change solar/wind systems, and solar storms (Global Magnetic

Disturbances, GMD.) The GMD threat to the BES is well established through largely Canadian experiences, **despite concerted efforts by the industry to avoid requirements for GIC devices** and critical protection for **step-up transformers** in major areas of the Northeast, the Canadian Maritime Provinces, the Pacific Northwest. ***Note over 200 Chinese high voltage transformers have been installed in the US, including Northwestern GMD-susceptible federal generation facilities.*** Significant TPL actions on cyber systems critical to **GMD**, forced on NERC and FERC by relentless pressure from technical and scientific sources, carefully avoid cybersecurity requirements in the extensive **TPL GMD** documentation. A reasonable assumption is that the Russian Federation might target those transformers in a “false flag” operation coupled to election intrusions. ***However, there are no hooks to Supply Chain controls, i.e., Order No. 850, in the extensive NERC Reliability Standards GMD documentation.***

15. **VAR** is a category of Reliability Standards that covers measurement, monitoring and control of real time voltages and reactive systems critical to the exchange of power from one utility to another. Power system stability is critical to functioning of the BES and **VAR** standards apply to systems important in the handoff of power from one utility to another. Cyber assets/cyber systems vulnerable through “Supply Chain” firmware or malware ***should be covered by Order No. 850***, but VAR requirements are devoid of this factor.
16. **PRC** Reliability standards include a massive set of over 30 BES Protection requirements covering Transmission, Generation and “connected” Distribution functions. Note this is the largest set of Reliability rules for protection of the Bulk Power System, what should be at the heart of Supply Chain protection needs, but they are **non-CIP**, not covered by Order No. 850.
17. A revealing example of this **non-CIP/CIP** “digital divide” comes to light from a SERC RE Compliance audit⁴ that aggressively cited TVA for “serious” violations of **PRC-001-1**, maintenance failures of less than 1% of over 45000 TVA protection devices. TVA protested to no avail and since the SERC RE penalty assessment of \$852,000 was null and void (TVA is a Federal Corporation), SERC RE sanctioned TVA for three years for quarterly reports on all 45000 protection devices. Part of the SERC RE charge incredibly claimed that TVA failed to consider **CIP** Communications risks in its violation of **non-CIP** Standards.
18. **PRC non-CIP** requirements cover the entire gamut of BES cyber assets/cyber systems that involve BES Protection Systems. Requirements bear dates as early as 2005 to the present day. The Eastern Blackout of 2003 and the technical reviews that followed are the genesis of many of these requirements. More recent requirements arise from the trend to solar and wind generation and of course the complexity of absorbing such power into the grid. There are 476 pages devoted to PRC non-CIP Protection issues. Writeups are often lengthy and highly technical on complex engineering matters, a testimonial to hard working utility engineers and utility operators and executives who have engineered one of the marvels of modern American and Canadian technology. The simple table that

⁴ NERC Full Notice of Penalty Re: Tennessee Valley Authority, Docket No. NP18-000, July 31, 2018

follows is included here to try to illustrate the comprehensive nature of Protection measures inherent in the BPS⁵. Page counts are a good indicator of complexity. The PRC topics undoubtedly also reflect similar Distribution system functions. ***Note however that in scanning and assembling the foregoing summary, not a single cybersecurity mention was encountered. This was understandable in 2003; in 2019 it is incomprehensible.*** There were, however, frequent admonitions about the importance of communications systems to coordination, data exchange, real time calculations, measurements, and operations.

RQMT	Description	Page Count	Comment
PRC-001-1	Protection Coordination System	6	Across Entities
PRC-002-2	Disturbance Monitoring & Reporting	38	Data needs, precision
PRC-004-5	Mis-operation, Identification, Correction	32	
PRC-004-6	WECC Remedial Action Scheme	7	Occasional Regional Variation
PRC-005-1b	Transmission& Generator Maint & Testing	40	Voltage/Current Sensing Device
PRC-008-0	Under Frequency Load Shedding	2	Auto Switching
PRC-010-2	Under Voltage Load Shedding	29	Transmission lines, Reactors
PRC-011-0	Maintenance and Testing	2	Relays, Transformers, Batteries
PRC-012-2	Remedial Action Scheme, RAS	49	Ditto
PRC-013-1	RAS Database, Disturbance Monitoring Equip	2	Installation, Data Recording
PRC-014-1	RAS Assessment	2	
PRC-015-1	RAS Data & Documentation-Capabilities	2	Coord Generator Unit & Plant Controls
PRC-016-1	RAS Mis-operations	2	
PRC-017-1	RAS Maintenance and Testing	2	
PRC-018-1	Disturbance Monitoring Equipment	4	Data Reporting
PRC-019-2	Coord Gen Unit and Plant capabilities	11	Voltage Regulation
PRC-023-4	Coord Transmission Relay Loadability	15	Transformers !!!
PRC-024-2	Generator Freq & Voltage Protection	12	Relay Settings
PRC-025-2	Generator Relay Loadability	114	Step-up Transformers
	Application Guidelines	1	
PRC-026-1	Relay Performance	84	During Stable Power Swings
PRC-027-1	Coordination	17	Across Entities/Functions
	Total	476	

⁵ The 476 pages of text, data and diagrams show no coverage of cybersecurity standards or sensitivity of the cyber assets or cyber systems to vulnerabilities, even Supply Chain vulnerabilities. These are fundamental protection devices but reflect no cybersecurity protection.

--	--	--	--

There are 3X the number of pages in NERC’s Reliability Standards publication devoted to **non-CIP** Standards compared to **CIP** standards. How, then, do the **CIP** Standards provide adequate security to BES cyber systems? Let’s add the following **CIP BES** Transmission and Generator data to the above “Stack”to complete this summary of the focus of NERC Reliability Requirements.

1. **CIP-002** cyber system categorization excludes Nuclear sites and Distribution facilities, and of course Alaska and Hawaii, non-sensible but blame the EPA. But this **CIP** standard also excludes categorization of all **BES** Communications and Network cyber systems, despite contrary language in EPA Section 215. **Why?** Any examination of **non-CIP** standards shows that to have included this in **CIP** standards would compromise the separation of OT Operational standards from cybersecurity (**CIP**) envelopment. The previous chart shows why.
2. NERC and FERC assert that **CIP** standards are conditioned on risk to the **BES**, not risks to the Grid writ large. This is absurd on the face of it; **BES** protection does not ensure protection of Distribution or Nuclear facilities. The nation’s cyber adversaries have demonstrated ability to penetrate the overall Grid through multiple portals and move laterally. GAO has tasked FERC to show how the Grid would respond to simultaneous attacks.⁶ Nevertheless, **CIP-002** excludes from **CIP** standards any facility that does not pose a risk to the **BES** within 15 minutes of assault. Further, CIP also excludes from its standards, any facility/substation that is below a graduated set of MW limits for the BES, ignoring plausible attack vectors. Cyber systems also are graded into Low, Medium and High categories, dependent on impact of loss to the BES.
3. Furthermore, it is left to individual utilities to define a cyber system subject to **CIP** standards; be it a single cyber asset, a collection of cyber assets, even an entire substation. This produced a weird set of disparate candidates for **CIP v4**, approximately only 5% of Transmission substations covered by **CIP** Standards. Even FERC could not stomach these numbers, **CIP v4** gave way to **CIP v5**. Nevertheless, the candidate numbers did not change and FERC has steadfastly refused to divulge what is covered by **CIP** standards and what facilities are not. Thus, the very base for **CIP** coverage is unspecified and thus **the actual cyber systems subject to Supply Chain Standards, Order No. 850 remains unknown**, presumably even to NERC and FERC.

⁶ GAO Report 19-332 Critical Infrastructure Protection, August 2019

Comment: NERC and FERC may try to assert that BPS Operations are exempt from cybersecurity controls or assert that **CIP** Standards are effective for all cyber systems in Reliability Standards labeled **non-CIP** in this filing. **Either would be utter nonsense.** The mass of documentation in NERC's **non-CIP** Reliability Standards compendium are totally devoid of **CIP** linkages. Further, Compliance audits avoid any cross connection. And given these major **CIP-002** uncertainties, it is impossible to judge the efficacy of standards subordinate to **CIP-002**. Given what has preceded, in the foregoing stack, it is reasonable to assume this obscurity was by design. With the large number of variables on categorization of cyber assets and cyber systems, registered entities (utilities) could easily confuse compliance authorities (RCs) on periodic assessments. Very large utilities would incur increased costs if the conflict of **CIP** and **non-CIP** systems was exposed and use categorization vagueness to minimize such conflicts, for example in hundreds of substations housing both Transmission and Distribution assets. CIP-002 exceptions and vagueness make a nonsense of the term "standard" for the Bulk Power System.

4. **CIP-003** Security Management Controls assert separate protection requirements for medium/high impact and low impact cyber systems. A fundamental condition is that all electronic aspects involve a concept of a Secure Electronic Perimeter, ***given the total exclusion of communications and network cyber systems from CIP Standards***. This is a theoretical but thoroughly impractical condition that ignores security of data flows and interactive electronic functions critical to operations, all of which would have to be ignored in compliance assessments. Even controls on vendors are impractical considering extensive direct maintenance contracted out. And those are ideal venues for Supply Chain attacks. Most other security management functions in this standard affect subsequent CIP standards (e.g., CIP 004 Personnel and Training). ***It is important to note that CIP-003 and subsequent standards detail management, planning and other, often idealistic, security hygienic functions and rigorously avoid direct relevance to Operations.***
5. **CIP-004** Personnel and Training Standard exists as part of a suite of CIP Standards "***related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES.***" There are, in fact, no linkages of this standard to actual "Operations". Operational here can only mean the functions of personnel security. Here again, the process involves the bureaucratic (documentation, planning, hygienic) stages of security management of BES Cyber Systems, ***not security management of utility's power operations (covered by non-CIP standards.)***
6. **CIP-005** Electronic Security Perimeter standard, previously mentioned, is an artifice to account for ***exclusion*** of communications and networks from categorization of Cyber Systems. It is maddening to try to understand the standard, ***applicable only to BES Cyber Systems***, when it cites registered entities such as Balancing Authorities controlling

systems such as load shedding, cranking paths, systems carried under non-CIP Reliability Standards. Is this the “carny” game of “which shell is the peanut under?” And ***“Each Responsible Entity shall implement one or more documented [processes, plan, etc]”*** is the end game, not “Operations”. ***But let’s take the 10,000 foot view and ask “How do tens of thousands Transmission, Generator and Distribution Provider ESPs in a connected Grid, lacking cybersecurity controls on their ESP communications and network connectivity, protect even the Bulk Electric System from penetration, and more importantly, Supply Chain attacks? More utter nonsense.***

7. **CIP-006** Physical Security of BES Cyber Systems, **CIP-007** Systems Security Management, **CIP-008** Incident Reporting and Response Planning and **CIP-009** Recovery Plans for BES Cyber Systems is more of the same. Applicability to BES Cyber Systems is asserted but applicability to Cyber Systems organic to Operational functions, i.e., cyber assets of **non-CIP** cyber systems with different Reliability Standards. ***This conundrum is not addressed in Order No. 850, Supply Chain Standards.***
8. **CIP-010** Configuration Change Management and Vulnerability Assessments purpose is to prevent and detect unauthorized changes to BES Cyber Systems. In respect to systems not categorized as such, i.e., Operational Cyber Systems under **non-CIP** Reliability Standards, it has no applicability. The use of cyber security controls refers specifically to controls referenced and applied according to **CIP-005** and **CIP-007**. Therefore, if those standards only apply to cyber assets categorized under CIP-002 as BES Cyber Systems, **CIP-010** is further excluded from applying to **non-CIP** Reliability Standards. **CIP-011** Cyber Security Information Protection is to prevent unauthorized access to BES Cyber System Information and therefore is linked only to foregoing **CIP** standards.
9. **CIP-012** Cyber Security – Communications between Control Centers is to protect the confidentiality and integrity of Real-time Assessment and Real-time monitoring data transmitted between Control Centers. It is not an exception to **CIP 002** since it deals with data exchange, not the communications media itself. Also, although it is a **CIP** standard, its only requirement is for a “plan” on how protection is applied, and stops short of any reference to Cyber Assets or Cyber Systems. FERC had originally directed NERC to ***“develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers.”*** However, the requirement to protect, at a minimum, communication links was dropped in the final Order No. 822 rule. Thus, the **CIP-002** exception was essentially retained.
10. **CIP-013** Cyber Security - Supply Chain Risk Management addresses Order No. 829 directives for entities to implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts. The plan(s) would apply to BES medium and high impact but not low impact Cyber Systems. And while the **plan(s)** must address.....

- (1) Software integrity and authenticity
- (2) Vendor remote access
- (3) Information system planning; and
- (4) Vendor risk management and procurement controls,

.....but there are no meaningful guidelines for plan(s) to ensure effective mitigation of risks and no “standardization” of measures to ensure effectiveness, across 1400 Registered Entities separate Order No. 850 plans.

Comment: The Order No. 850 Supply Chain standard hardly exceeds good hygienic security procedures for ordinary procurements and implementations. It totally fails to recognize the sophistication of adversaries’ cyber capabilities and the realities of flaws and vulnerabilities of commercial IT systems linked to energy industry vendor offerings. And inclusion of access control systems, e.g., EACMS, is delayed several years. Further, a single, recent CISCO vulnerability assessment, **for example**, listed over 3600 CVEs that are totally beyond a utility’s ability to understand, let alone relate to unique energy industry products. Supply Chain threats are at a stage where the only sensible activity in a proposed Supply Chain Standard is **Whitelisting** and **Blacklisting**, and, in the interest of costs, a funded, industry-wide vulnerability evaluation program for critical procurements. FERC Order no. 850 is dead on arrival.

“Exposure” Summary

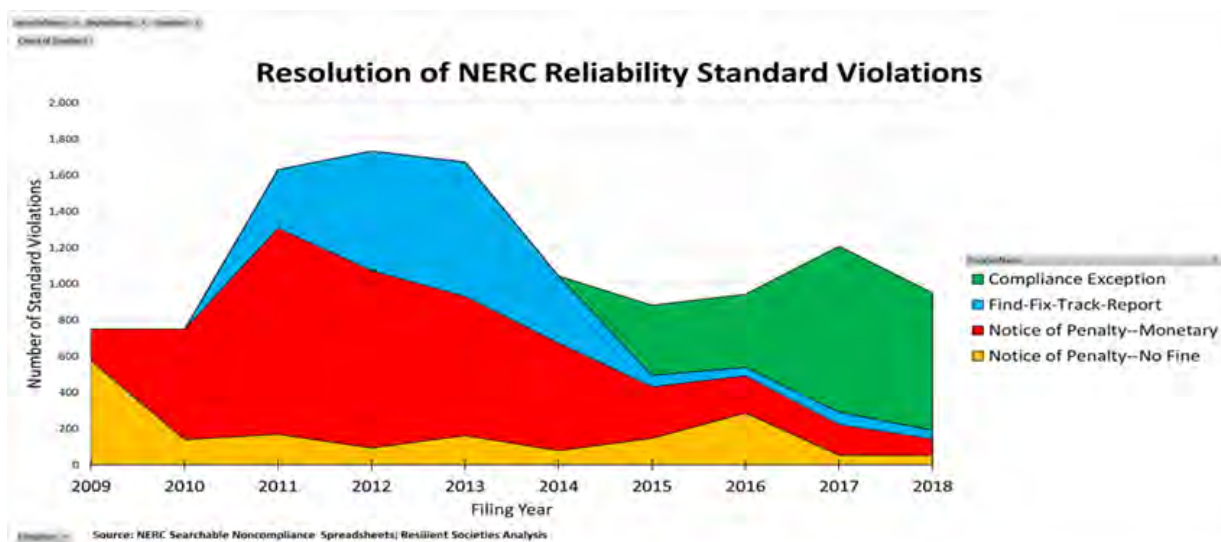
It is admittedly difficult for anyone caught up in the cyber risks to this nation to understand the actual effects of the foregoing summary of flaws in what is defended as protection for the Bulk Electric System. It is probably more complex than predicting the economic aftereffects of the current pandemic. But experts in the five or six critical infrastructures, including the Conus national security functions, have grave concerns and some actual experiences (i.e., malware-related election intrusions), in the capabilities of the Russian Federation to seriously disrupt the Grid. The current Congress in bi-partisan frustration created the Congressional Cyberspace Solarium Commission to address cyber threats to the nation and is strongly recommending a National Deterrence Policy. That key finding is driven by a prior Defense Science Board Deterrence recommendation directly coupled to national security risks of a Grid takedown. FERC has had this filer’s interventions on precisely this evolution, yet continues abetting these risks from the Federation out of deference other industry priorities.

Comment: At this point, what should be obvious to any reader of this filing is that Regulators are excluding most if not all operational functions of the BES from cybersecurity controls, This was clearly not the intention of Congress in its EPA legislation of 2005. Nevertheless, Standards authorities (e.g., NERC and FERC) have created a CIP and non-CIP separation of operational systems and non-operational systems and have been careful to maintain this separation in regulatory matters since implementation of Section 215 of the EPA. This has required cooperation between utilities, NERC, and FERC taking conspiracy to defeat EPA Section 215 to new heights. Reliability Coordinators have been careful to avoid compliance monitoring of very large utilities for fear of exposing the seams of this digital divide. Conflation of CIP and non-CIP standards has been rigorously avoided. Minimization of compliance reporting, redactions and CEII are used to further obscure the near-universal avoidance of cybersecurity controls on most operational cyber assets.

Compliance (?)

There is little point to repeat in this filing the many issues raised by this, and other filers over the last eight years expressing fears of Supply Chain vulnerabilities, actual subversion of vendors' systems used in the Grid, related malware challenges, and systemic weaknesses in CIP Standards. A few highlights are in order, however.

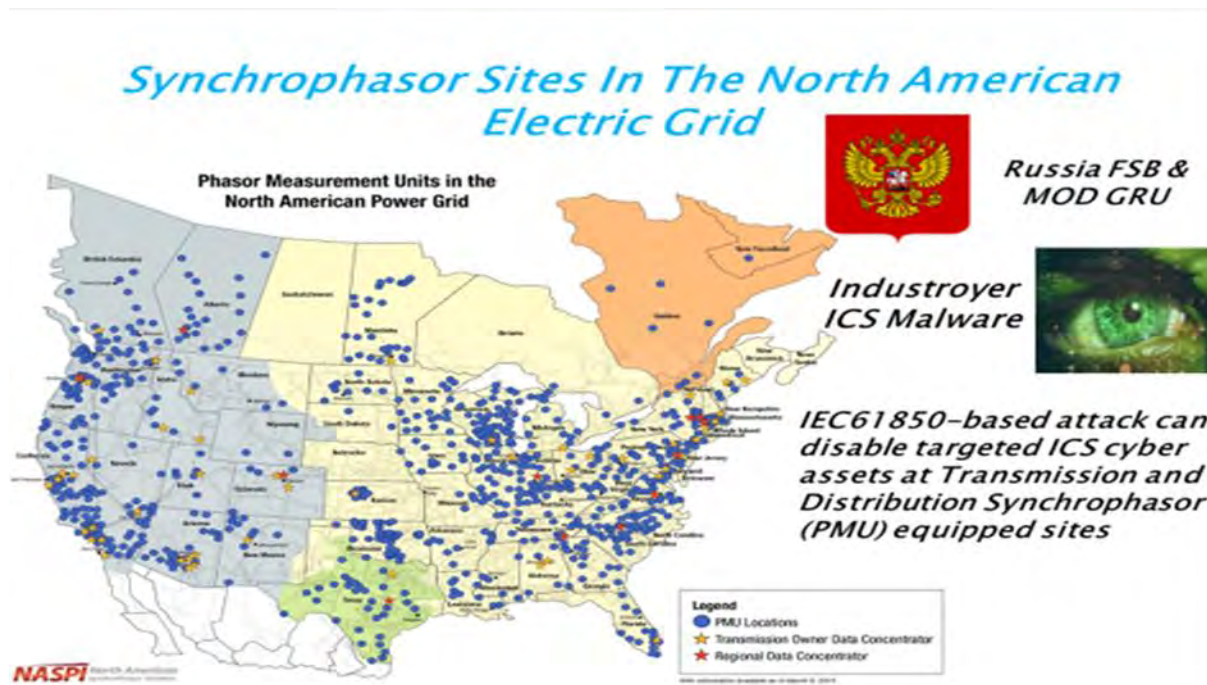
1. Redactions of RC compliance assessments including utility identifications⁷ is being challenged, in FOIA cases, but what has remained obscure is NERC's steady attack on any public awareness. While not quite successful in convincing FERC of the need, it has steadily whittled down the process with FERC until it is practically meaningless. Witness what the following chart reveals in the trend to zero compliance:



Courtesy of the Foundation for Resilient Societies

2. Modernization activities often complicate the NERC/FERC cybersecurity regime. Nowhere is this more evident than in the Synchrophasor evolution from utilities' digital data recorder (DDR) systems to capture in real time, power fluctuations for stability maintenance or post-event analysis. In due course, these systems wired together in networks with centers for data processing totally compromises the separation of Transmission systems and Distribution systems, as can be seen on the map that follows. NERC's CIP Standards, or even the other, cybersecurity-unprotected NERC Reliability Standards cannot admit even the existence of these technologies and networks.

⁷ Protest and Comments of Michael Mabee, Dockets RM15-4-000, RM16-22-000, RM17-1-000, RD18-4-000, April 10, 2020



Modernization of the electric grid is relentless, examples are in solar and wind power generation and energy storage. And chasing Synchrophasors is a major upgrade in precision measurement, which in combination with machine learning will lead to extensive automation of the overall system.⁸ NERC and FERC must realize they are fighting a losing battle in minimizing cybersecurity protection for the Grid. Indeed, the separation of State authorities from Federal authorities is now being challenged by modernization.

3. Several audits of very large, multi-state utilities have exposed seams in the NERC/FERC regime.

The Duke Energy audit redacted in a 700+ page NoP⁹ reported on 127 separate infractions of CIP Standards. None of these violations applied directly to Duke Energy operations; operations of cyber assets critical to the protection of generation, transmission and distribution of electric power. Further, no unredacted audit of the non-CIP Reliability Standards of Duke Energy linked to these 127 violations could be identified in the NERC audit database. Thus we are asked to believe that all the linkages between **CIP** Standards and **non-CIP** standards, i.e., the cyber assets and cyber systems audited in 127 instances had no critical effect on the cyber assets and

⁸ NASPI "Synchronized Measurements and their Application to Distribution Systems, DRAFT, An Update", May 12, 2020

⁹ Full Notice of Penalty NP19-4-000 Docket January 25, 2019

cyber systems otherwise described in the **non-CIP** NERC Reliability Standards publication including any cyber assets/cyber systems reflected in the 467 page PRC chart on page 7. The NERC/FERC scheme is simply mind boggling.

Conversely, the SERC RE **non-CIP** audit of the Tennessee Valley Authority, a Federal Corporation, from 2015-2018¹⁰ revealed a direct connection between a **PRC-001** violation of maintenance and testing of 45000 operational protection devices and **CIP** standards. This was mistakenly cited in the Settlement Agreement. Conveniently, for the auditors, **CIP-002-5(1a)** lists communications and networks as being exempt from **CIP** standards.

Summary and Conclusion

This filing's depiction of the cybersecurity regime that the industry, its ERO (NERC), and FERC created under Federal Power Act, Section 215 tasking, reveals the Act's intention was quite deliberately distorted to insulate, repeat insulate BPS Operations from effective federal cybersecurity controls. A set of Operational Reliability Standards, largely in existence before 2005, was maintained apart from **CIP** standards in the extended 2010-2012 period leading to **CIP v3**, the first FERC-approved cybersecurity standards. Today, they continue to exist separately from **CIP v5/6** cybersecurity standards. And an organized coverup of the resultant gaps in overall cybersecurity for the entire North American Grid continues, everything from systematic avoidance of meaningful compliance with the weak **CIP** standards, to enormous payoffs to key Congressional energy committees, a war chest funded by excess profits conveniently provided by padded FERC-approved tariffs.¹¹

To extend this conspiracy throughout intervening years, a policy and practice of obscuring the implementation of this regime took several additional forms -- minimization of public knowledge of vulnerabilities, suppression of incident reporting of actual incursions by adversaries, denial of relevant adversary testing of malware abroad, misleading testimony before Congress, and misuse of CEII (Critical Enterprise Infrastructure Information) in sanitization of utility compliance audits. And now underway is promotion of Senate Bill S.3688 to codify misused CEII procedures.

These practices have aided and abetted the threat to hazard the Grid, national elections, and invade social media. The seams in this NERC/FERC regime have widened, an Executive Order complicates procurements and a Congressional Commission is forcing a national deterrence

¹⁰ See Footnote 4.

¹¹ **"Operator of Power Grid Accused of Overcharging Utility Customers Billions of Dollars"** Tom Johnson | March 17, 2020 | Energy & Environment. Study faults **PJM** Interconnection for inaccurately forecasting energy requirements and sticking utility customers with the costs. **PJM** is the largest U.S. Transmission Operator, 14 States

policy that must defeat S.3688 to be effective. FOIAs and lawsuits are forcing the industry and FERC to greater coverup lengths. As a 60-year veteran of cyber wars, there is not a chance those practices contribute to Security in the National Grid, rather they are efforts to keep federal cybersecurity regulation at arm's length. In fact, and to this experienced cryptologist, the technical and procedural content of the NERC publication **"Reliability Standards for the Bulk Electric Systems of North America"** has undoubtedly proven far more valuable to Russia and China than **all** of the CEII-protected violation reports, together.

Further, the Commission should really recognize that their practice of "Security Through Obscurity" is causing grave risks to Distribution facilities and local gas, electric firms, and also to the national security facilities, dependent on commercial power. Hopefully, this filing should help the Congress, the federal government, state PUCs, and the public to understand what has been in play. The commission may wish to deny the conclusions of this filing but they would be better advised to actively support the Congressional Cyberspace Solarium Commission's efforts to authorize a deterrence policy that would buffer the Grid from attacks and permit a far less costly industry protection regime.

Respectfully Submitted

George R. Cotter

CC:

Director Federal Bureau of Investigation
 Chairman, SEC
 50 State PUCs
 Congressional Cyberspace Solarium Commission
 Secretary Department of Energy
 Secretary, Department of Defense
 Commander, Cyber Command/Director National Security Agency

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)
Related to Critical Infrastructure)
Reliability Standards)

(Docket No. EL20-46-000
(Docket No. AD20-19-000
(Docket No. RM20-12-000

Introduction

The FERC Staff White Paper¹, 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 Intervene² 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 Standards³ 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 NP19-4-000⁴ 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 Synchronphasor 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 **Operational** 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 Board⁷ 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: Synchronphasor Sites in the North American Electric Grid

Respectfully Submitted,

George R. Cotter

⁷ DoD DSB Task Force on Cyber Deterrence, February 2017

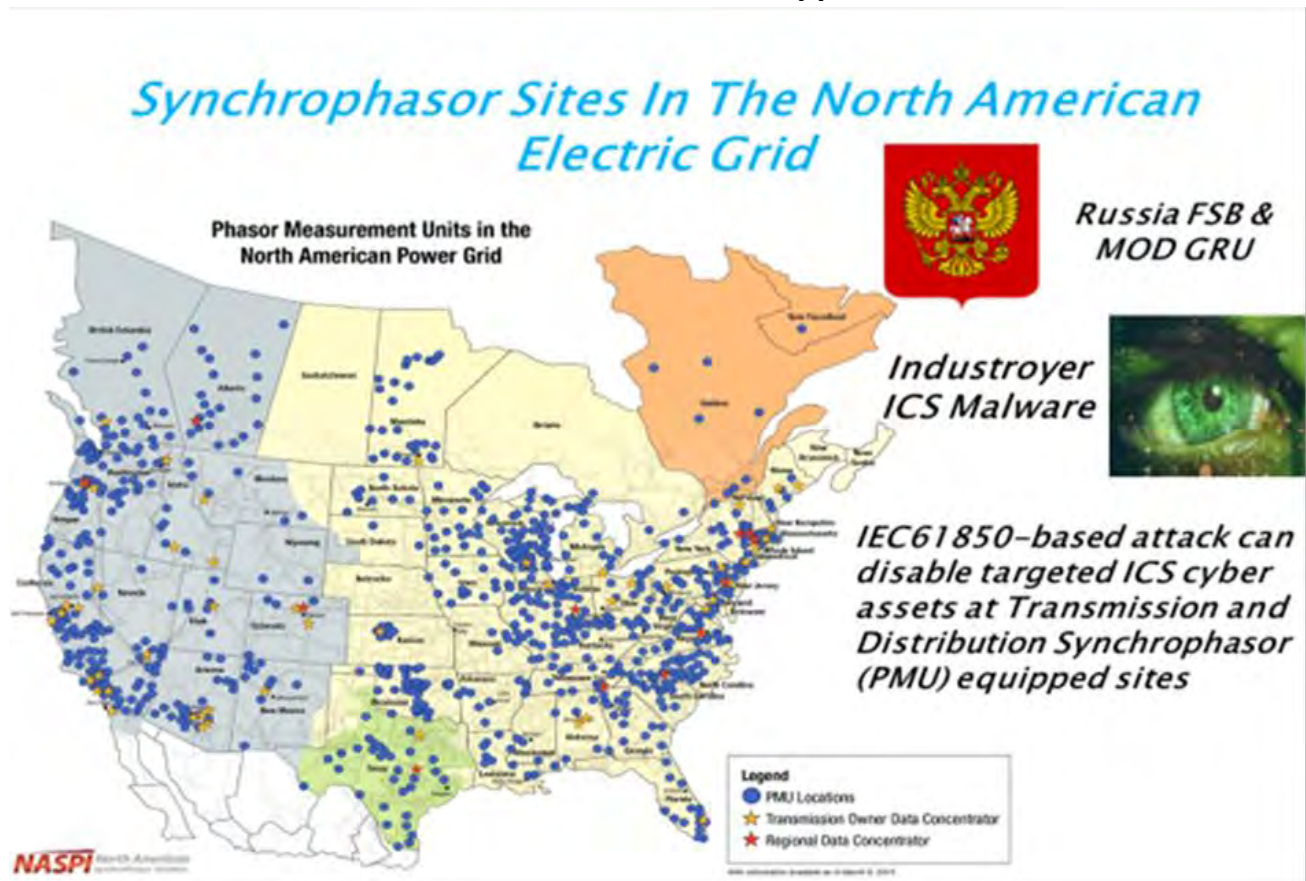
⁸ Congressional Cyberspace Symposium Report, March 2020

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.

193 Southdown Road
Edgewater, MD 21037

grcotter@comcast.net

August 7, 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 3rd Motion to Intervene on Dockets Nos. EL20-46-000, RM20-12-000 and AD20-19-000, all Related to Critical Infrastructure Reliability Standards.

Respectfully,

/s/

George R. Cotter

Enclosure: a/s

UNITED STATES OF AMERICA

BEFORE THE

FEDERAL ENERGY REGULATORY COMMISSION

3rd Motion to Intervene in Dockets)
Related to Critical Infrastructure)
Reliability Standards)

(Docket No. EL20-46-000
(Docket No. AD20-19-000
(Docket No. RM20-12-000

Introduction

A recent joint Cybersecurity Advisory titled ***“NSA and CISA Recommend Immediate Actions to Reduce Exposure Across all Operational Technologies and Control Systems”***¹ described steps to be taken immediately to address risks to critical infrastructures from the nation’s adversaries, risks focused on OT and Control Systems known to be vulnerable to malware attacks and held in high priority by the nation’s cybersecurity adversaries. **Previous filings on these dockets built the case for the Bulk Electric Systems (BES) being a major example of OT and Control System vulnerabilities since BES cyber assets controlling real time operational power flows are devoid of cybersecurity protections.** Thus, this joint guidance issuance has the BES OT and Control Systems directly in its gunsights, unless of course FERC and NERC attempt to further cloud this reality from the organizations that issued the guidance, the Congress, and the public. This 3rd Motion to Intervene in related FERC dockets is intended to convince FERC and its overseers, the Congress, DOE and DHS, and the Administration to address this self-induced vulnerability, hopefully in parallel with the declaration of a National Deterrence Policy and Strategy that puts the North American Grid off-limits to the nation’s adversaries.

Background

Few individuals and even fewer organizations can fathom the complexities of this engineering marvel --the nation’s electric system, the complex of thousands of independent and semi-independent utilities that over the past hundred years or more have successfully connected and modernized their generation, transmission and distribution systems. However, it became increasingly difficult to create wide area power flows without developing and agreeing on conformance standards that would produce reliable power service to industry and the public. The reliability standards that work so well today grew out of a half century of collaboration, initially between a few utilities but ultimately through regional and national cooperation and regulation. This of course also required regulation of power markets and controlling tariffs,

¹ NSA and CISA Recommend Immediate Actions to Reduce Exposure Across all Operational Technologies and Control Systems, July 22, 2020

necessarily split between the federal and state levels (power flows arbitrarily labelled “Transmission” and “Distribution” systems, respectively.)

Growth and Grid integration had succeeded well until the major Northeast power outage of 2003, a cascading outage that exposed deep technical and operational flaws in the Grid. The joint US/Canadian study that followed for almost two years resulted in a major rewrite of the Energy Power Act of 2005. Cybersecurity had emerged over the previous decade that raised national concerns on the vulnerability of critical infrastructures including the electric Grid, and Congress added a new section 215 to the EPA that empowered an industry “not for profit” corporation, NERC, as the Electric Reliability Organization (ERO) responsible for developing cybersecurity standards for the Bulk Electric System and the Federal Regulatory Energy Commission for their oversight.

Critical Infrastructure Protection (CIP) Standards

CIP Standards have had a rocky evolution beginning with CIP v1 under FERC Order No. 706 in January 2008, with several iterations leading eventually to a version, CIP v3 formally approved in 2010 under FERC Order No. 712. FERC’s approval came with directions for further modifications leading to CIP v4 to be followed rapidly with CIP v5. The nearly continuous iteration between the industry, the NERC standards development teams, and FERC occurred throughout. One continuing disconnect was uncertainty over which Cyber systems would be covered by versions of standards. Statistics were publicly revealed for CIP v4; widely variant across eight Reliability Entities.² CIP v4 was approved by FERC but never really implemented by NERC. FERC approved CIP v5 in Order 791 on November 22, 2013, the first semi-stable version, but fully 8 years after passage of the EPA. Changes to CIP v5 trickled out but were eventually added to CIP v5 in an expanded CIP v5/v6.

The evolution of CIP Standards occurred out of the public and congressional consciousness but did extensively involve industry leadership, exercising control of the NERC Board of Trustees, a substantial NERC staff with oversight of a succession of standards bodies, and FERC which ultimately had to go through the formalities of public review of standards. Industry positions on contentious issues were strongly supported by active industry organizations, NEI, EPRI, etc.³ However, cyber vulnerabilities were seldom discussed and threats, almost never. As the Russian Federation began incursions in 2012 (supply chain penetrations) and active attacks in 2014 (with extensive malware testing in the Ukraine in 2015 and 2016),

² Characterization of CIP facilities averaged less than 10% for Generator, Transmission and Distribution satisfying the “BES impact within 15 minutes” guidance in CIP v4, substantially unchanged in transition to CIP v5.

³ See Tom Aldrich Blog dated Monday, January 1, 2018 “An (Impressionistic) History of NERC CIP”. This “history” of CIP evolution provides a capsule (but biased) review of this evolution, a near continuous exercise in futility, a back and forth contest between an industry that viewed cybersecurity regulations as a reversal of federal deregulation, and a Regulatory Commission obviously sensitive to the increasing threat from Russia but lacking the depth and continuity to hold NERC in check.

NERC and FERC showed little inclination to link cyber standards to BES vulnerabilities and Federation threats. An FBI report on the 2014 incursions was never publicly released.

CIP Compliance

CIP standards compliance audits largely by Reliability Entities (RE's) essentially mandated by the EPA but under control of NERC, were slow to emerge. Depending on severity of the infraction, these could range from self-reported by utilities with little or no penalty to lengthy assessments by RE's with financial fines and/or sanctions. NERC's annual, generalized Compliance report to FERC has consistently requested that all compliance reporting be made non-public. FERC has never agreed although succumbing to pressures to substantial weakening of compliance programs and, more critically, substantial redactions in published assessments to hide violations, utility identifications and almost anything that would trace to the violator. The practice is ostensibly to protect information that could be used by an attacker but without documentation of cause and effect, but is more likely intended to protect utilities from liability charges by the SEC, insurance firms, and the public. These practices have been contested by public-spirited individuals and organizations. The industry succeeded in getting some protection written into the FAST Act and has recently succeeded in getting comprehensive support in a proposed Senate Bill (s.3688) dedicated to outlawing FOIA's, regulatory filings, and actions by State PUCs.

Cybersecurity-Related Developments

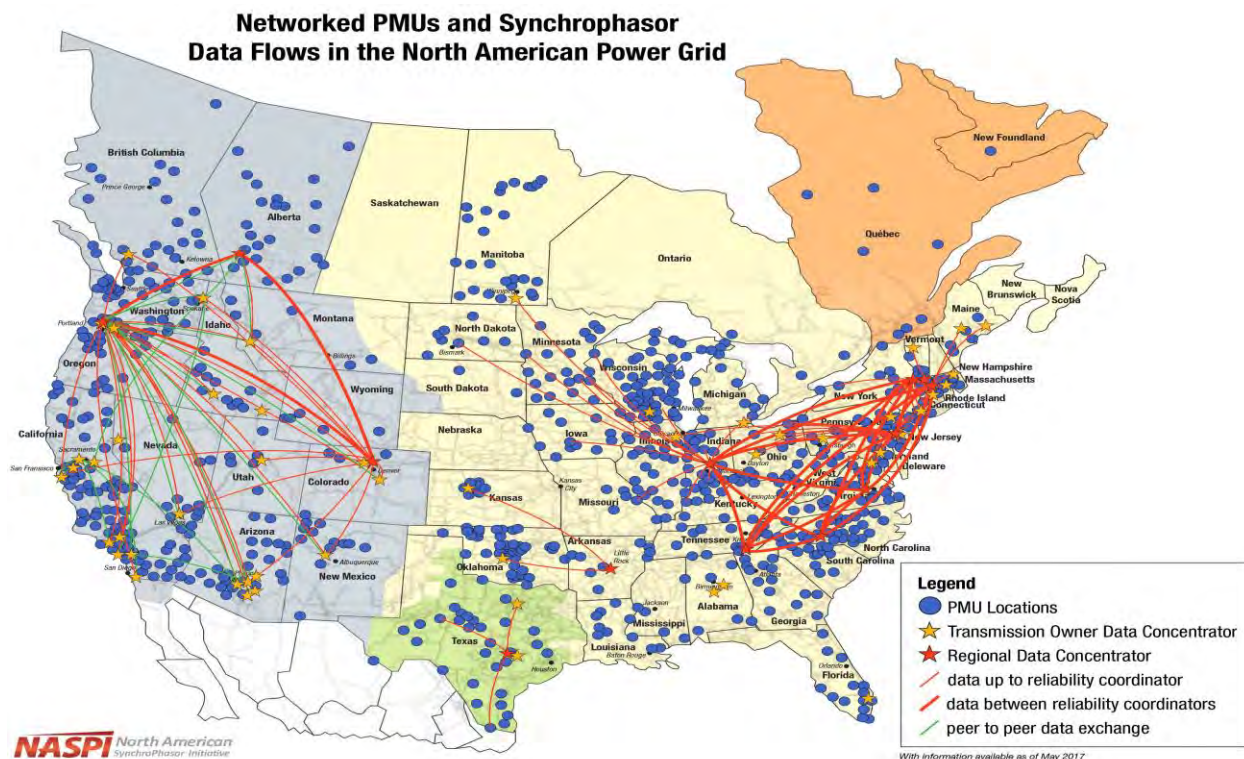
That a disaggregated electric industry has faced many apparently adverse developments over the past two decades⁴ that affect implementation of cybersecurity controls will not be debated. These include cybersecurity issues associated with groundbreaking changes in energy sources (solar, wind), nation-wide environmental concerns with pollution from coal and other thermal energy sources, fracking for oil and gas, energy industry economic competition, climate change contentions, threats to the industry from nation/states and criminal groups, and modernization pressures, induced by all of the foregoing.

Among all modernization activities has been the clash between utility independence and utility interdependencies; critical engineering issues arising from the peculiarities of "electricity", its stability, integration pressures that result in lengthening of power flows, and growth and complexity of power demands. Automation of inter-utility systems is a constant concern. Sensors are essential, the trends from analogue to digital controls, data exchanges and the like have increased in complexity. Over several decades the use of digital data recorders (DDR's) to record and manage current, voltage, frequency and phase conditions in power exchanges

⁴ This exposition will only address major cybersecurity related developments since the implementation of PD 63 in 1998!

between utilities. They have largely been replaced by “Synchrophasor Systems feeding SCADA systems supporting energy management

There has been an explosion of “Synchrophasor Systems” higher precision instrumentation replacing DDRs. With precise timing system accuracies, these permit wide area coordination of power flows and, in fact, have been useful in resolving wide area “flaws” in generation systems and interconnections. Data collections and their aggregations at processing centers amount to a Synchrophasor explosion, easily seen on the following map, produced by NASPI, an informal association of utility users. These systems are now the principal input to management of Distribution systems across the lower 48.



Synchrophasors and CIP Standards

A reasonable question, therefore, is how does this modernization initiative interface with CIP Standards, since these systems are not only extensively used in the BES but also must be the principal means for controlling operational power flows from Transmission networks to and through, Distribution networks. Strangely, Synchrophasor technologies appear to be totally missing from any description or categorization of BES Cyber Systems. Not a mention, Nil. Well, how are they reflected in the massive NERC Reliability Standards document⁵ that contains, in enormous detail, the engineering standards that essentially control the technical interfaces for

⁵ NERC Reliability Standards for the North American Bulk Power System, Updated June 23, 2020

all networks, and digital (cyber) devices used to manage operational power flows? A once-over examination of thousands of pages of such standards fails to turn up any references to Synchrophasor systems, although their earlier characterization, DDRs, are prominently featured. Furthermore, the term is also missing from CIP sections of the NERC Reliability Standards document.

There could be only one reason for this anomaly, deliberate suppression of this modernization program. Why? One possible answer is that the industry and NERC did not want any questions raised on how, repeat how, power flows from the CIP-protected BES Cyber Systems into unprotected Distribution networks could be managed? But of course, CIP-002 **exclusions** of communications and networks (from the inception of CIP, a profound exclusion mystery) meant that these power flows were not, technically, in conflict with CIP cybersecurity regulations. **Did this mean that all Grid operational power flows have been deliberately left unprotected by CIP cyber regulations since the passage of the EPA? Regrettably, the answer is yes.**⁶

Further Indications of Deliberate Exclusion from CIP

Did this revelation imply that other CIP Standards or their requirements bypassed (i.e., had no effect) on operational power flows? **Regrettably, the answer is also yes.** Engineering (non-CIP) Reliability Standards show no linkages between (1) systems and technologies controlling operational power flows, and (2) CIP Standards. This is extensively documented for both non-CIP Reliability Standards and CIP Standards in my initial Motion to Intervene filing on Docket No. EL20-46-000 dated April 11, 2020. For example, in over 470 pages of technical data on Protection Systems (PRC) summarized in a table on page 8, in that Motion to Intervene. Digital (i.e., cyber) systems show no cybersecurity requirements or CIP references in this extensive tutorial on Protection Systems. And further, while CIP Standard 002 has occasional references to Reliability Standards (such as **PRC**), these references describe boundary conditions for categorization decisions, not requirements for CIP protection.

One of the major issues complicating application of CIP Standards to operational power flows are important differences between Reliability Entities (example: Balancing Authorities) on some Reliability Standards. As integration of utilities occurred in the early Grid, connectivity needs required agreement on power metrics, e.g, frequency and phase variations in power flows. This of course led to the creation of NERC and Reliability Regions and standardization. Differences between Reliability Entities persist to this day, Balancing Authorities (BAs) must oversee agreed boundary metrics for operational power flows between Reliability Regions. The current issue of NERC's Reliability Standards on **BAL** standards, their calculation, boundary conditions, development history, persistent differences across major interconnections, variances for several

⁶ It is important to note that this analysis addresses only regulatory cybersecurity provisions. An individual utility may voluntarily adopt security features such as encryption of data flows, internal access controls over operational data flow cyber assets, etc. Indeed, in 50/50 funding of Synchrophasor implementations, DoE left it to utilities to include or exclude encryption from their grant proposals.

BAs. The current publication exhaustively describes engineering standards in many other categories though also without linkages to cybersecurity requirements. With the multilevel standards approval process – industry, Reliability Entity, SDT, NERC Board of Trustees, FERC NOPR and Final Rule, there are myriad opportunities to consider cybersecurity protection requirements for cyber assets critical to BES operational power flows. For a single albeit major function, what does the record reveal?

Selecting **PRC-006 Underfrequency and Undervoltage Load Shedding Performance Standards**, what is documented is the complete history, agreements, uncertainties, discontinuities with other requirements, open issues and FAQs covering the complexities of intentional and unintentional load shedding at generator, transmission, and distribution facilities of the BES. We observe at best, only partial standards for the BES, thus continuing efforts within the WECC, SERC, the NPCC and/or Quebec (interconnections and REs) to achieve standardization on these critical functions. The set of associated Remedial Action Schemes (RAS) are a long way from integration for the BES.

Hence, application of CIP Standards to cyber assets essential to UFLS and UVLS, and by extension to BAL, FAC and other Reliability functions, is clearly unattainable.

Comment: Back in April 2005 with FERC initial approval of many Reliability Standards, the emphasis was on fixing interoperability flaws exposed by the Joint US/Canadian study of the 2003 NE power outage. In that context, cybersecurity requirements understandably took a back seat to other reliability issues. It is now clear that in the interval to 2008 and formalization of CIP v1, the industry, NERC and FERC had only two choices on a CIP structure, (1) sets of Cybersecurity Standards largely developed within Interconnections and perhaps Reliability Regions to permit variances across the BES, a process that continues to this day. Alternatively (2), careful development of BES-wide CIP Standards, deliberately avoiding adding complexity to the unresolved interoperability issues extant, and of course BES operational power flows. Option 2 was chosen, without public exposure or debate. Over the past 15 years, it has therefore been essential that implementation and extension of CIP Standards would not compromise BES real time operational power flows. Over time, this has presented NERC and FERC with additional CIP complications, examples such as communications and network data flows, supply chain vulnerabilities, Internet vendor access, incident reporting. And of course, we see the explosion of Synchrophasor PMUs and related Data Concentrator Centers and networks whose precision technologies addressed the very technical issues inherent in non-CIP engineering standards. CIP compliance audits had to be sanitized as this process continued, foreign adversary threats had to be similarly buried, i.e., ***Security through Obscurity***. And today, BES as well as Distribution level operational power flows are largely open and available to these foreign adversaries for malware development and attack planning.

Exclusion of Real Time Power Flow Operations from Non-CIP Compliance Audits

The question naturally arises “How and to what extent are real time power flows addressed in non-CIP Reliability Standards, and therefore in non-CIP Reliability Standards Compliance Audits? For purposes of this Motion to Intervene, an NPCC audit⁷ of a reasonable size utility, the Long Island Power Authority conducted on November 28/29, 2017 was examined. No violations of these standards were identified in the audit. At the time of this audit, LIPA was a TOP, TO, DP and TP; responsibilities to be audited. LIPAs area covered most of Long Island. The NYISO was the RC, BA, PA, and lead TOP for LIPA. NPCC identified the non-CIP Reliability Standards in the following Table⁸ for this audit:

Table 1: Compliance Audit Scope		
Registered Function	Standards	Requirement(s)
TOP	COM-002-4	R1, R5
TOP	EOP-005-2	R1, R6, R9, R12, R13
TOP	EOP-008-1	R2, R4, R5, R6, R7, R8
TOP	EOP-010-1	R3
TOP	EOP-011-1	R1
TOP, TP	FAC-014-2	R2, R4, R5
TOP	PER-005-2	R1, R3, R4
TOP	PRC-001-1.1(ii)	R3, R4, R5
TOP	TOP-001-3	R1, R5, R6, R7, R8, R9, R15, R16, R18, R19
TOP	TOP-002-4	R1, R2, R3, R6
TP	TPL-001-4	R1, R2, R3, R4

The team did not expand the scope of the Compliance Audit beyond what was stated in the notification package.

A comparison of the included standards and requirements against those documented in NERC Reliability Standards was conducted to determine if the audited functions included any cybersecurity-related cyber assets or control functions exclusive to real-time power flows. Observations:

1. All Distribution Provider (i.e., power flow) functions were excluded from the audit.
2. Any applicable standard flagged “**real-time operations**” was also omitted from the audit.
3. Requirements labeled as “event reporting”, “emergency functions”, “system restoration”, related training, and similar operational activities were excluded from the audit.

⁷ NCR07133 Long Island Power Authority Compliance Audit November 28/29 2017 dated 12/8/2017

⁸ A direct comparison was not always possible with time lapses between FERC standard approval and the audit date, also the migration of requirements from one category to another in the NERC Standards process; e.g., COM-001 “no longer enforceable”, included in other ways evidently but not trackable.

4. Explicit requirements for actions related in any way to real-time power flow operations, such as authorities to notify in the event of outages, were excluded from the audit.
5. Most importantly, LIPA's responsibilities to other BES authorities critical to real time operations, e.g, Balance Authorities, generator operators for Black Start operations, etc. were excluded from the Audit implying the former were non-operative.
6. Synchrophasor Technologies and related Data Concentrator facilities, real-time operational activities, are totally missing from this audit as well.

The conclusion is therefore inescapable, this audit and assessment not only lacked linkages to Critical Infrastructure Protection (CIP) standards but rigorously avoided any non-CIP Reliability Standard related to "Real-Time Operational Power Flows".

Thus, all BES digital (cyber) systems for any non-CIP Reliability Standards and control center functions have no cybersecurity protections. Further, all Reliability Standards and control center functions critical to real-time operational power flows including Synchrophasor Systems, their Data Processing and Data Flow technologies are also excluded, repeat excluded from compliance audits of utilities.

It therefore appears that cybersecurity protections afforded BES cyber assets apply only to a very thin set of utilities non-operational functions, characterized under CIP-002.

Summary and Conclusion

Except for what an individual utility might voluntarily do for security, most BES digital (cyber) systems have been deliberately excluded from BES cybersecurity protection, including all systems controlling real-time operational power flows. This is not problematical, the massive NERC Reliability (engineering) Standards compilation contains extensive details of cyber (digital) systems utterly devoid of cybersecurity protection. Modernization, such as Synchrophasor Technologies have made it increasingly difficult for NERC and FERC to hide this violation of the intent, and indeed actual wording, of EPA 2005 Section 215.

Had NERC and FERC developed CIP Standards in parallel with non-CIP (engineering) standards, modernizations of Operational Technologies would have included appropriate cyber protections. Systems such as Synchrophasor PMUs, solar and wind generators, Internet and vendor connectivity, Supply Chain Standards etc., would have had to include cybersecurity protection. Incidentally, there is little doubt that insertion of Synchrophasor technologies, particularly software, is delayed in some utilities over fear of conflict with CIP Standards.

Critical Infrastructure Protection standards are simply inconsequential for protection of cyber systems critical to BES operations. In 2008 the objective might have been otherwise, but CIP has become a façade for utility insular management functions, access controls and physical and electronic isolation of facilities. NERC and FERC claims that the CIP Program reduces the risk to the BES are hollow, for in this decade and a half of CIP evolution, we witnessed:

- BES and Distribution systems in open access to the nation's adversaries,
- suppressed reporting of adversary incursions, including critical malware development
- Further efforts spawned by NERC and FERC to obscure vulnerabilities and threats through the Senate Bill s.3688
- unchallenged follow-on adversary malware testing in the Ukraine
- freedom for adversary's cyber forces to employ that same malware in the 2016 election
- increasing risks to Grid-dependent national security facilities and other critical infrastructures.
- Inordinate costs of ineffective cybersecurity protections for the North American Grid.⁹

The joint NSA and DHS/CSIA Advisory cited in the introduction to this Motion to Intervene provides detailed guidance for the protection of Operational Technologies and related Control Centers, in their continuing campaign focused on access to Industrial Control Systems. It emphasizes the immediacy of necessary actions, the widespread internet access to OT systems, endangerment to DoD and National Security Systems, and recently observed adversary actions.

The North American Grid's operational power complexes and networks could be the poster child for this Advisory. Many of its recommendations should certainly be taken seriously by electric utilities. However, the existential threat to US national interests and to Critical Infrastructures requires much, much more, a threat engineered by the industry, NERC and FERC but hidden from public and Congressional consciousness.

Congress and the Administration must implement the Congressional Cyberspace Solarium's 2020 report recommendation with a law invoking a Declaration of National Deterrence Policy with Measured Retaliation, as originally proposed in 2017 by the Defense Science Board.¹⁰

⁹ N.Y. utility, Siemens Energy plan first-of-a-kind cyber hub, Christian Vasquez, E&E News reporter Published: Wednesday, July 29, 2020. The complete IBM report can be downloaded from this reference. Costs per incursion and magnitude are reportedly higher than any other industry.

¹⁰ Department of Defense, Defense Science Board, Task Force on Cyber Deterrence, February, 2017



Secure the Grid Coalition
A Project of the Center for Security Policy
2020 Pennsylvania Avenue, N.W., Suite 189
Washington, D.C. 20006

Appendix C

Honorable Linda Capuano
Administrator
Energy Information Administration
U.S. Department of Energy
Washington, D.C.

July 6, 2020

Re: EIA Tracking & Reporting on Large Power Transformer Data Important to National Security

Dear EIA Administrator Capuano,

Our Secure the Grid Coalition¹ has long worked to improve the security of our nation's most critical infrastructure – the electric grid. We believe you could assemble information collected by others of great value to both the legislative and executive branches of government, to the electric power industry, and to volunteers like ourselves who seek to assist with that effort. This involves two important issues:

— One concern is that “foreign adversaries are increasingly creating and exploiting vulnerabilities in the United States bulk-power system” — leading to Presidential Executive Order 13920 (May 1, 2020).² Compromised components in our critical Large Power Transformer fleet is one of our greatest concerns.

— Another concern is the dependence of grid infrastructure owners/operators on foreign suppliers. This is an issue which is known, has not been examined for several years,³ and deserves timely attention.⁴ Congress is presently considering legislation on infrastructure and, with the benefit of information that you can assemble and analyze, can address adversarial foreign suppliers in the grid and other critical infrastructures.

For example, because of price and/or availability, electric utilities have installed or have on order equipment such as large transformers manufactured in China. China has a history of providing equipment with surreptitious parts which can be used for data monitoring or extraction (or even as a vector for cyberattacks). Huawei 5G chips are one example and Lenovo keystroke loggers are another. Recently a large electric transformer was found with extraneous electronics that precipitated second large identical transformer to be taken to Sandia National Laboratory for analysis by the US government.⁵

We understand EIA does not itself collect (and we are not asking you to collect) data on age, condition, and place of manufacture of transformers and other critical equipment in the US electric grid. But other

¹ 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. It is parented by the Center for Security Policy, a 501(c)(3). More info can be found here: www.SecureTheGrid.com

² See <https://www.federalregister.gov/documents/2020/05/04/2020-09695/securing-the-united-states-bulk-power-system>.

³ See *Large Power Transformers and the U.S. Electric Grid* (2014), at <https://www.energy.gov/sites/prod/files/2014/04/f15/LPTStudyUpdate-040914.pdf>.

⁴ See: “JiangSu HuaPeng Transformer Co., Ltd. is currently the largest producer of Medium Power Transforms in the world.” <http://www.jshp.com/index.html>.

⁵ Electrical equipment normally associated with electric utilities are also used throughout other industries including in manufacturing, refining, mining, chemicals, railroads, etc. as they use large electric equipment like pumps, motors, generators, motor control centers, transformers, conveyor belts, etc. These large pieces of electric equipment are supported or protected by protective relays, process sensors, equipment monitoring (vibration, temperature, etc.), arc flash detectors, etc.

agencies do. For example, the U.S. International Trade Commission maintains a DataWeb public-facing site which (since 2004) provides annual data on individual large power transformers (category 8504), including those imported from China, which are available to any who know how to search that site.⁶

However, this site and database are difficult to use for those concerned about energy equipment imports that could impact national security. We believe that EIA could harness the U.S. ITC DataWeb system and provide public access on the user-friendly EIA website to the annual time series of large power transformer imports, by capacity, and the national origin of transformers imported from the various foreign suppliers.

Additionally, many transformers in the US are owned and operated by firms which are not electric utilities. For example, the Northeast Corridor railroad lines are electrified and operate many transformers. Also, oil refineries in remote locations, far from the interconnect grid can use large electric transformers. Does EIA keep track of such transformers?

Regarding infrastructure legislation being developed, we believe FERC and NERC have information on the age and condition of critical equipment in the US electric grid (and that NERC has more data since 2016)⁷ which they could make available to EIA in disaggregated form — to be acceptably aggregated by EIA before release, thereby protecting non-public data your staff sees from disclosures to our adversaries (to the satisfaction of data collectors FERC or NERC).

We therefore ask EIA to draw upon data collected by the US International Trade Commission, FERC, and NERC to help Congress and the Executive Branch (and those who advocate before them) better evaluate national security concerns. Specifically, we ask EIA to track to the extent feasible data on:

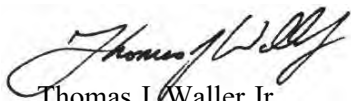
- manufacturer (place and firm),
- condition,
- age and
- loads served (numeric data and load characteristics)

for the large power transformers as now classified by the U.S. International Trade Commission, in categories 85042200, 85042300, etc. for the years starting in year 2004, using in part the databases that are publicly accessible through the U.S. International Trade Commission.

Were EIA to track such data and apply the EIA staff's excellent analytic skills to produce and publish timely reports, this could both discourage investments in insecure supply chains and encourage more domestic manufacturing of critical supply chain components, especially large power transformers.

We thank you for your attention to our concerns and hope that by addressing them you will continue to enhance the value of your service to the nation. We are similarly addressing Assistant Secretary of Energy Walker and Principal Deputy Assistant Secretary Plankey.

Sincerely,



Thomas J. Waller Jr.
Director, Secure the Grid Coalition

c: Tom Leckey, Assistant Administrator for Energy Statistics

⁶ See <https://dataweb.usitc.gov>.

⁷ See Elements Inventory at <https://www.nerc.com/pa/RAPA/tads/Pages/ElementInventory.aspx>.

Appendix D



1. *BallistiCrete Introduction*
2. *BallistiCrete Applications*
3. *BallistiCrete Testing for DOE Y-12*
4. *BallistiCrete Sub Station Protection*
5. *BallistiCrete Official Accreditation*

1. INTRODUCTION

GigaCrete Inc, a US corporation, has a manufacturing and testing facility in Las Vegas, Nevada. The company founder Andrew Dennis has invented a unique and proprietary product originally designed for hurricane protection, that has proven to be bullet resistant.

BALLISTICRETE™ has been tested to National Institute of Justice (NIJ), Level III and also Level IV and is able to stop the following calibers: 7.62x51 NATO rounds, .30-06 AP armor piercing, 7.62x39 AK-47s, Uzi 9mm, .40 caliber .357, .44 and .45 magnums, and even a desert Eagle .50 caliber round with zero penetration into the building.

BALLISTICRETE™ is a worlds first and the only plaster coating in the world to pass NIJ Level IV Armor Piercing ballistic tests.

The product is:

- less cost than AR steel, ballistic fiberglass panels or aramid/Kevlar cloth
- easy to mix and apply over virtually any wall
- can be used to retrofit existing structures
- turn almost any space into a “safe room” environment.
- used to repair blast or bullet damaged walls



TECHNICAL DATA

TEST	METHOD	CRITERIA	RESULT
Compressive Strength	ASTM C-109	PSI	9,300+ @ 14 days
Flexural Strength (MOR)	ASTM C-293	PSI	1100 @ 14 days
Cold Water Absorption	ASTM C-1585	% age by weight	9% @ 7 days
Shrinkage (Air Cure)	ASTM C-157	% age by length	0.002% @ 7 days
Freeze Thaw	ICBO AC 11	> 10 cycles	No cracking or erosion
Corner Room Fire Test	NFPA 286	No flame growth	Pass
Surface Burning Test	ASTM E-84	Flame Spread < 25 Smoke < 450	Zero Flame Spread Zero Smoke
Combustibility Test	ASTM E-136	No combustion	Pass
Fungal Resistance	ASTM G-21	No mold or mildew	Pass
Ballistic Test	NIJ Level III	No penetration	Pass
Ballistic Test	NIJ Level IV	No penetration	Pass





2. BallistiCrete Applications

A NEW ECO-FRIENDLY CONCEPT IN BALLISTIC PROTECTION

BallistiCrete and Terrorist resistance

- Testing has proved we can armor ordinary walls and make them ballistic resistant
- Interior walls, offices, conference rooms, equipment rooms, vault doors
- Exterior walls, vertical surfaces, dome shapes, round buildings, angled or textured surfaces
- Sub-station cement block walls, prone to target practice
- BallistiCrete is not affected by sunlight or intense UV light
- When painted, it is imperceptible from an ordinary stucco wall
- BallistiCrete will bond permanently to all know foam insulation, cement block, brick, drywall, wood, cement board



BallistiCrete is easily installed over almost any surface, flat or curved



Nobody knows the walls are now armored



Mixed and applied onsite to look like ordinary plaster or stucco, interior and exterior coating.





3. BallistiCrete Testing for DOE Y-12

Reason for test:

- Terrorist resistance of Nuclear Power Stations
- Sub-station protection



A few correctly placed bullets can quickly destroy sub stations



Building cement block walls are slow to build and will not stop even a 7.62 bullet unless coated with BallistiCrete or filled with reinforced concrete. Remote locations make lengthy installations even more costly



Easy targets can be protected with precast shapes and still allow air movement for cooling



Installed over flat or round surfaces, BallistiCrete can be applied over concrete and cement block.



BallistiCrete



Test samples set up at Pro Gun Club outdoor range in Henderson Nevada



BallistiCrete testing of:

- hollow cement blocks (CMU)
- Typical walls with gypsum board (drywall)
- Hollow cement block
- A new solid block utilizing recycled rubber tires
- Nuclear power station AR steel vault doors, 3" and 6"

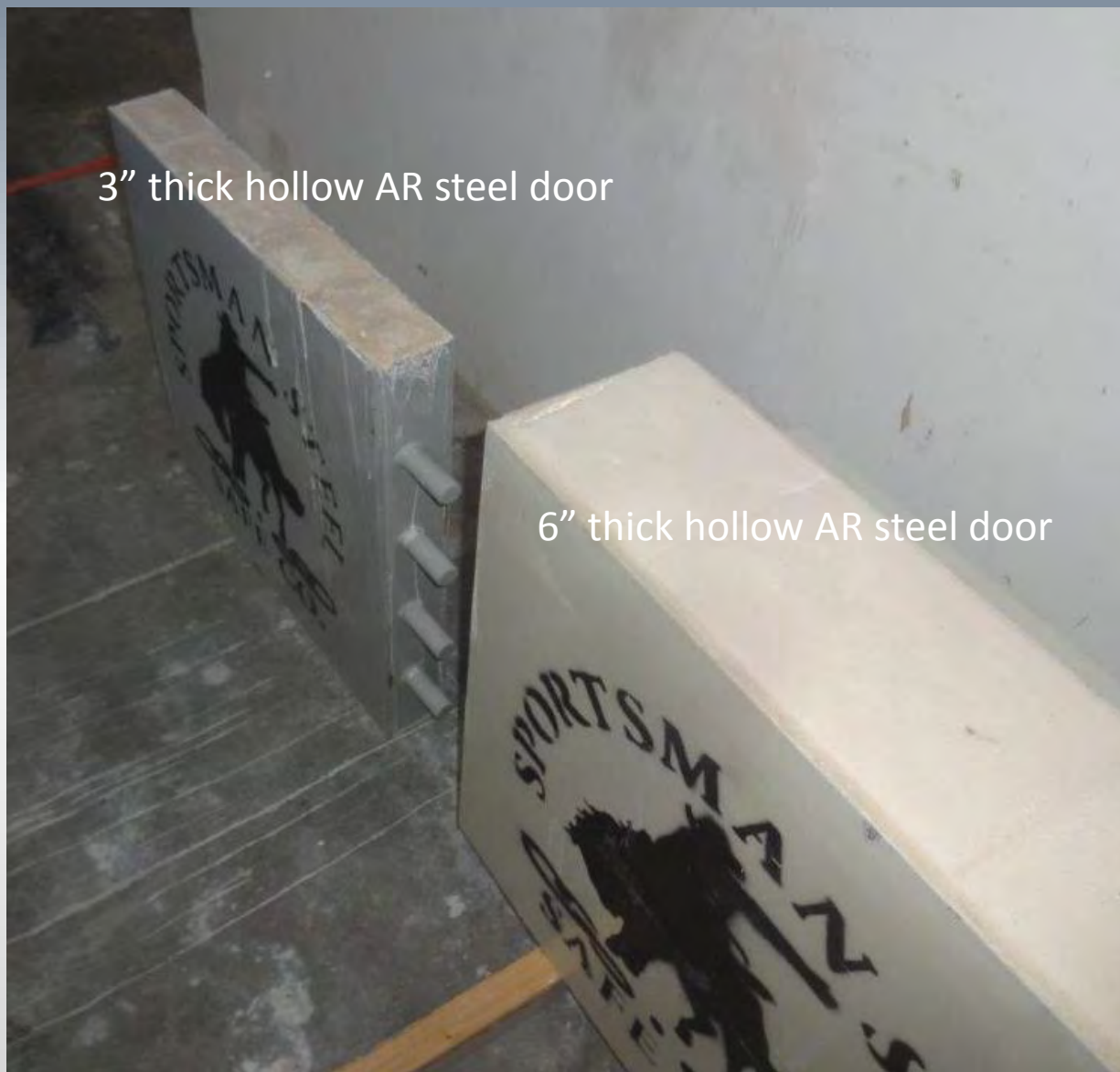




Judy Johns, Special Assistant to the President at B&W Y-12, after visiting GigaCrete requested proof and witnessed the live fire BallistiCrete testing.

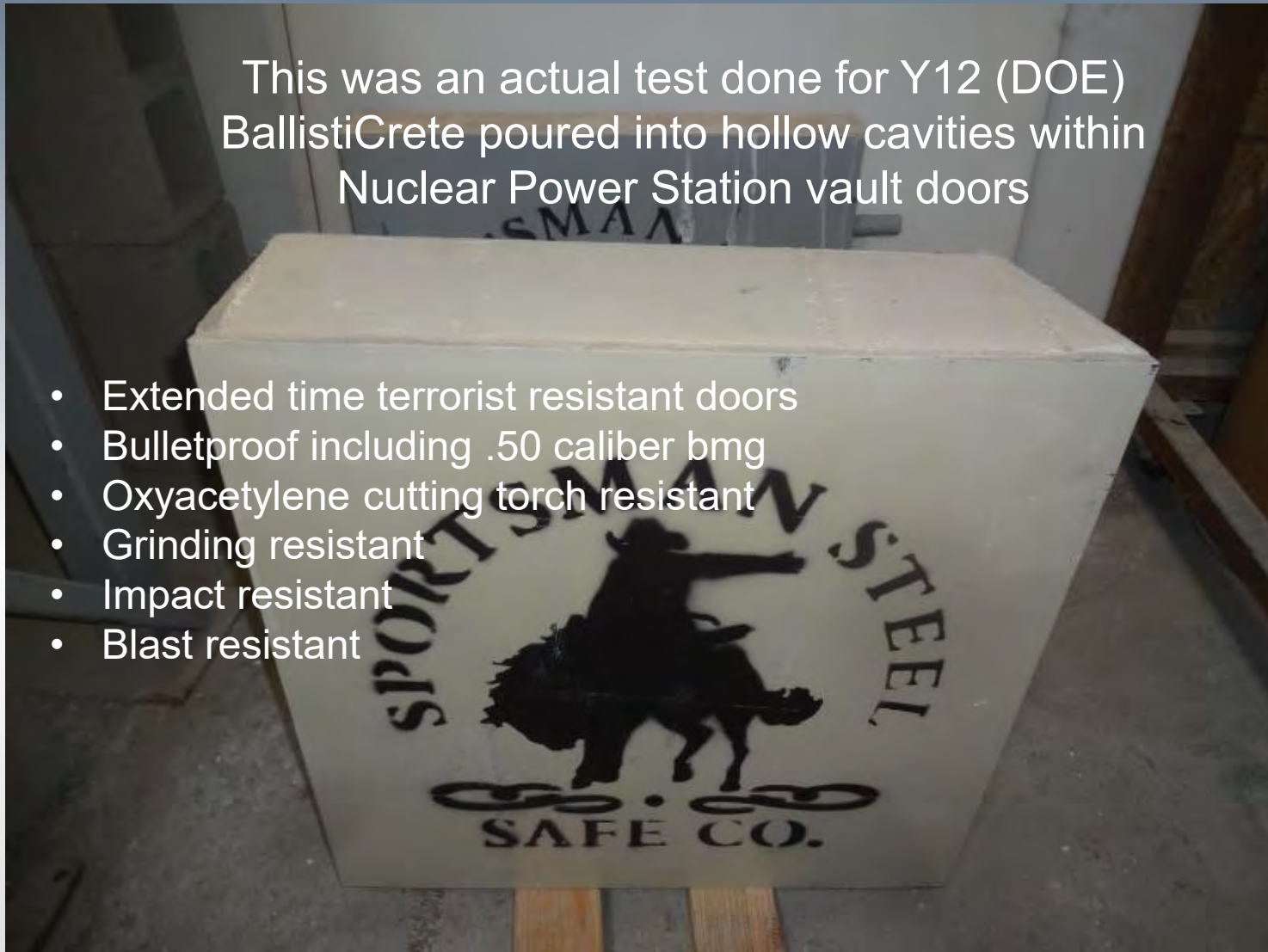


Samples sent from the vault door manufacturer to GigaCrete and filled with BallistiCrete



This was an actual test done for Y12 (DOE)
BallistiCrete poured into hollow cavities within
Nuclear Power Station vault doors

- Extended time terrorist resistant doors
- Bulletproof including .50 caliber bmg
- Oxyacetylene cutting torch resistant
- Grinding resistant
- Impact resistant
- Blast resistant



BallistiCrete



The most powerful and feared sniper rifle, a Barratt .50 caliber rifle.



This test was performed to prove BallistiCrete could be used to stop one of the most feared ammunitions available, a .50 caliber BMG round.





US Army Ranger sniper fires .50 caliber BMG ammo at the vault door filled with BallistiCrete. Distance 50 yards.





The result: .50 Caliber BMG round bounced off both door faces leaving an indent of only 1mm on 6" door and 7mm on 3" door. Both door cores 3" and 6" filled with BallistiCrete reflected energy back through face plate. Witnessed by DOE's department Y12.



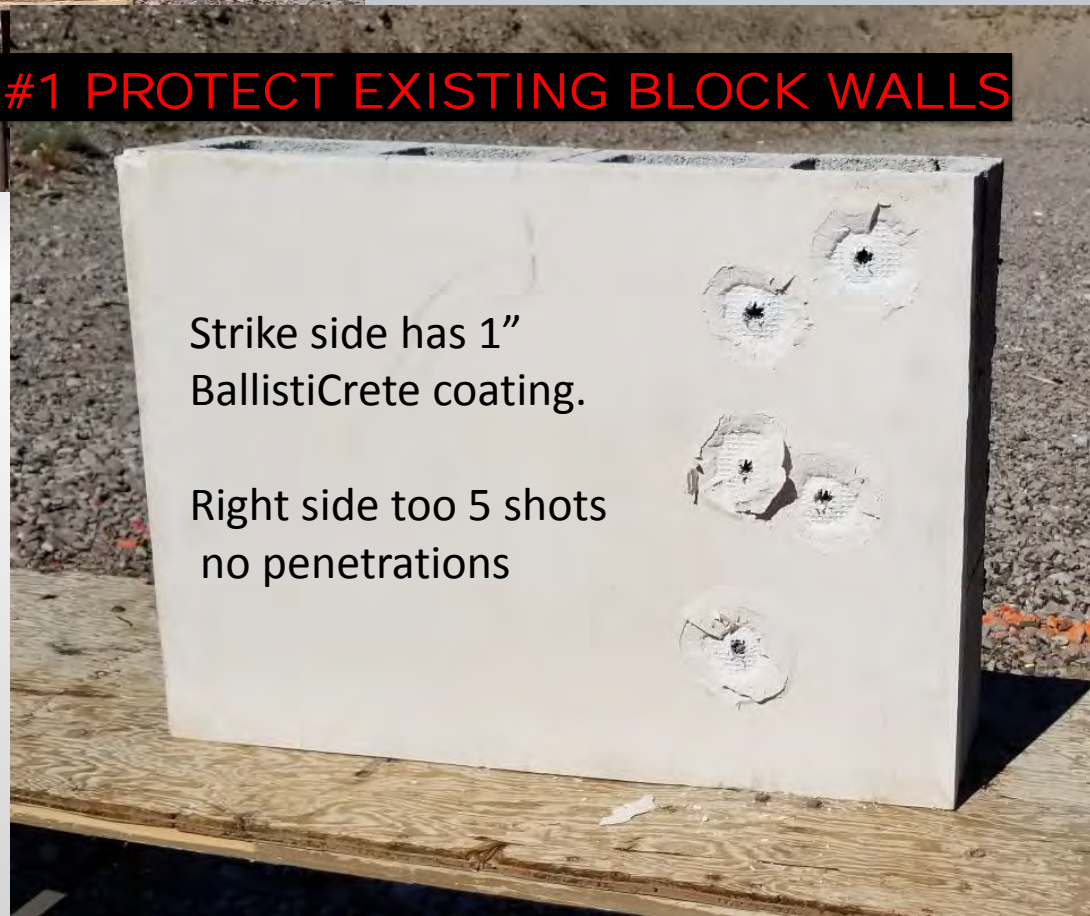


4. BallistiCrete sub-station protection

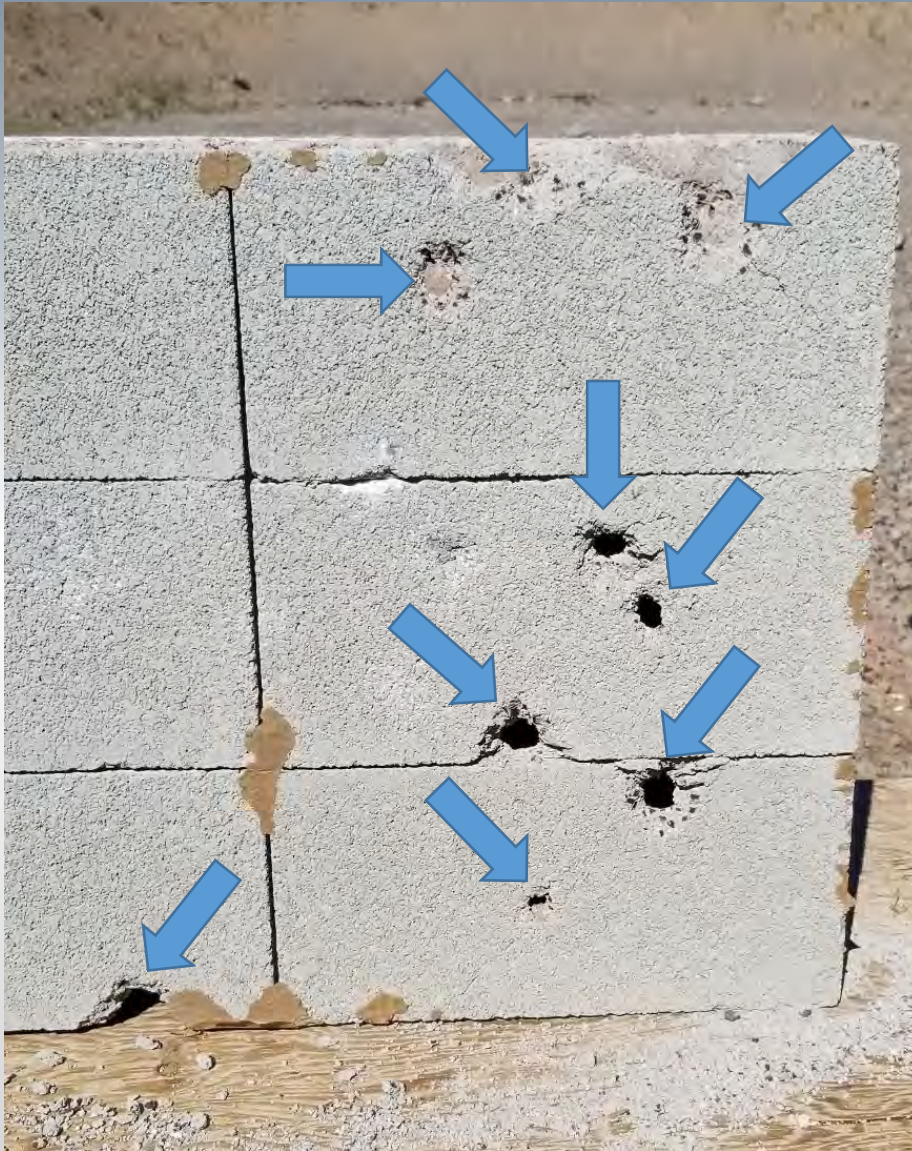
THE MISSION

1. Shoot a typical masonry wall
2. With an AK-47 rifle, 7.62 x 39 ammo.
3. 5 shots, close range
4. From the protected side
5. From the unprotected side

SOLUTION #1 PROTECT EXISTING BLOCK WALLS



Post shoot
9 shots, 7.62 x 39 AK-47



Pre shoot
Back side



Post shoot
No penetrations



SOLUTION #2 REPLACE CMU BLOCK WALLS WITH BALLISTIC RATED BLOCKS UTILIZING RECYCLED MATERIALS



Interlocking blocks create rapidly deployed building components stopping armor piercing rounds and .50 caliber bullets



The Weapon
Remington 700

The ammo
308 tungsten penetrator
New Military AP rounds



6" thick BallistiBlock
3 rounds
No penetrations





The Weapon
Remington 700

The Ammo
308 tungsten penetrator
New Military AP rounds



8" thick BallisticBlock
14 rounds
No penetrations





The Weapon
Barrett 50 Caliber
The ammo
.50 Caliber BMG

12" block with 2" BallistiCrete core



First .50 cal BMG round
Split the block,
no penetration

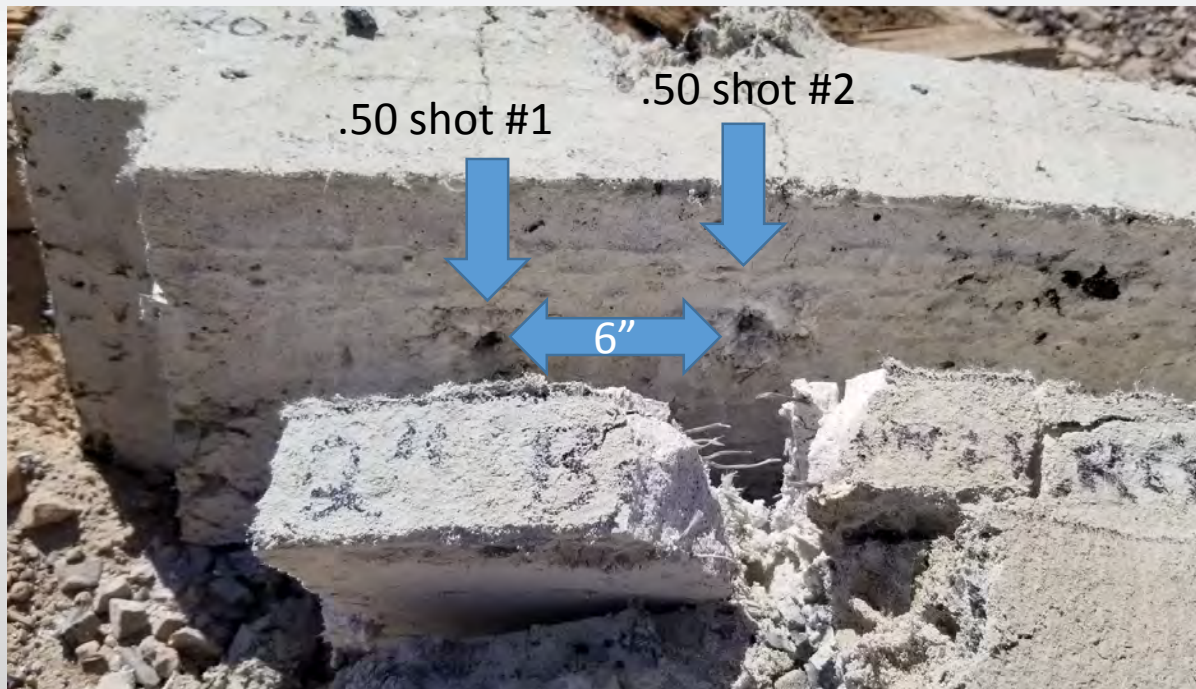




The Weapon
Barrett 50 Caliber

The ammo
.50 Caliber BMG

12" block with 2" BallistiCrete core



Second .50 cal BMG round
Split the block
no penetrations



SOLUTION #3 REPLACE CMU BLOCK WALLS WITH BALLISTIC PRECAST WALL COMPONENTS, RAPIDLY DEPLOYED & INSTALLED

Precast interlocking wall sections cast from BallistiCrete can be shipped to their destinations in various thicknesses creating a bullet resistant barrier system, temporary or permanent



- Filled with sand or concrete onsite
- Relocatable modular panels
- Repairable if damaged



The ammo
all handguns
AK-47 7.62 x 39
.308 (7.62 x 51)
.30-06 AP

.50 CAL BMG





5. BallistiCrete Official Accreditation

NIJ STANDARDS (USA National Institute of Justice)

LEVEL	Caliber	NIJ Standard 0101.06 Velocity
Level IIA	9mm 124 gr. FMJ RN	1225 ft/s
	40 S&W	1155 ft/s
Level II	9mm 124 gr. FMJ RN	1305 ft/s
	.357 Magnum 158 gr. JSP	1430 ft/s
Level IIIA	357 Sig 125 gr. FN	1470 ft/s
	.44 Magnum 240 gr. JHP	1430 ft/s
Level III	7.62mm NATO 148 gr. (.308 Caliber) FMJ	2780 ft/s
	30.06 166 gr. (.30 Caliber) M2AP Armor Piercing	2880 ft/s

All are stopped by BallistiCrete



BALLISTIC TESTS

Testing was conducted by US Government accredited H.P. White Laboratory Inc. in Maryland USA, NIJ-STD-0108.01, BALLISTIC RESISTANT PROTECTIVE MATERIALS, **Level IV, caliber .30-06 Springfield, 166 grain, AP, (armor piercing) M2 ammunition.** The test sample was rigidly mounted on an indoor range 50.0 feet from the muzzle of a test barrel to produce zero (0) degree obliquity impacts. Photoelectric infrared screens were positioned at 6.5 and 9.5 feet which, in conjunction with dual elapsed chronographs, were used to compute projectile velocities 8.0 feet forward of the muzzle. Penetrations were determined by visual examination of a 0.020 inch thick aluminum alloy 2024T3 witness panel positioned 6.0 inches behind and parallel to the test sample.

The test sample was a hollow cement block.

Test Sample			Ballistic Threat					Results
Sample Number	Thickness	Weight (lbs.)	Caliber	Obliquity (degrees)	Shots	Velocity (fps)		Penetrations
						Max.	Min.	
HPW-2	1 inch	85.38	.30 AP, M2	0	1	2852		0
				0	1(a)	2841		0
(a) Shot impacted coating side first.								



Test Results .30 Armor Piercing over hollow cement block

TEST PANEL

Manufacturer : GIGACRETE

Size : 16 x 16 in.

Thicknesses : 1.00, 1.00, 1.00, 1.00 in.

Avg. Thick : 1.000 in.

Description : UNGROUTED CMU BLOCK WITH 1" THICK COATING OF BALLISTICRETE

Sample No. : HPW-2

Weight : 85.38 lbs.

Hardness : NA

Plies/Laminates : NA

Date Rec'd. : 6/25/14

Via : OLD DOMINION

Returned : NA

SET-UP

Shot Spacing : 1 SHOT IN CENTER

Witness Panel : 0.020", 2024-T3 ALUMINUM

Obliquity : 0 deg.

Backing Material : NA

Conditioning : AMBIENT

Primary Vel. Screens : 6.5 ft., 9.5 ft.

Primary Vel. Location : 8.0 ft. From Muzzle

Residual Vel. Screens : NA

Residual Vel. Location : NA

Range to Target : 50.0 ft.

Target to Wit. : 6.0 in.

Range No. : 5

Temp. : 73 F

BP : 30.00 in. Hg

RH : 71%

Barrel No./Gun : R3/ .308

Gunner : GARRETT

Recorder : GORRERA

AMMUNITION

(1) : CAL. .30 AP, M2, 166 gr.

(2) :

(3) :

(4) :

Lot No. : UNKNOWN

Lot No. :

Lot No. :

Lot No. :

APPLICABLE STANDARDS OR PROCEDURES

(1) : NIJ-STD-0108.01

(2) : LEVEL IV

(3) : REQUIRED VELOCITY: 2800-2900 FPS

Shot No.	Ammo.	Time 1 (usec)	Velocity 1 (ft/s)	Time 2 (usec)	Velocity 2 (ft/s)	Avg. Vel. (ft/s)	Penetration	Footnotes
1	1	1052	2852	1052	2852	2852	None	
2	1	1056	2841	1056	2841	2841	None	(a)

BallistiCrete



Ballistic Test Results .308

7.62 x 51 NATO (.308) ballistics testing over hollow cement blocks

In accordance with your instructions, H.P. White Laboratory, Inc. conducted Ballistic Resistance Testing of one (1) un-grouted CMU Block assembly with 1 inch of BallistiCrete applied to one side of the sample. The sample was received 25 June 2014 via Old Dominion.

Testing was conducted in accordance with the general provisions of NIJ-STD-0108.01, BALLISTIC RESISTANT PROTECTIVE MATERIALS, dated September 1985, Level III, using caliber 7.62 x 51mm, 149 grain, M80 Ball ammunition. The test samples were rigidly mounted on an indoor range 50.0 feet from the muzzle of a test barrel to produce zero (0) degree obliquity impacts. Photoelectric infrared screens were positioned at 6.5 and 9.5 feet which, in conjunction with dual elapsed time counters (chronographs), were used to compute projectile velocities 8.0 feet forward of the muzzle. Penetrations were determined by visual examination of a 0.020 inch thick aluminum alloy 2024T3 witness panel positioned 6.0 inches behind, and parallel to, the test samples. Table I presents a summary of the enclosed data record.

TABLE I. SUMMARY OF RESULTS

Test Sample			Ballistic Threat					Results
Sample Number	Thickness	Weight (lbs.)	Caliber	Obliquity (degrees)	Shots (a)	Velocity (fps)		Penetrations
						Max.	Min.	
HPW-1	1 inch	86.0	7.62, M80	0	5	2780	2747	0
(a) 4 on 8" square-1 in center.								



Test Results .308 over hollow cement block

TEST PANEL

Manufacturer : GIGACRETE

Size : 16 x 16 in.

Thicknesses : 1.00, 1.00, 1.00, 1.00 in.

Avg. Thick. : 1.000 in.

Description : UNGROUTED CMU BLOCK WITH 1" THICK COATING OF BALLISTICRETE

Sample No. : HPW-1

Weight : 86.0 lbs.

Hardness : NA

Plies/Laminates : NA

Date Rec'd. : 6/25/14

Via : OLD DOMINION

Returned : NA

SET-UP

Shot Spacing : 4 ON 8" SQUARE - 1 IN CENTER

Witness Panel : 0.020", 2024-T3 ALUMINUM

Obliquity : 0 deg.

Backing Material : NA

Conditioning : AMBIENT

Primary Vel. Screens : 6.5 ft., 9.5 ft.

Primary Vel. Location : 8.0 ft. From Muzzle

Residual Vel. Screens : NA

Residual Vel. Location : NA

Range to Target : 50.0 ft.

Target to Wit. : 6.0 in.

Range No. : 5

Temp. : 73 F

BP : 30.00 in. Hg

RH : 71%

Barrel No./Gun : R3/ .308

Gunner : GARRETT

Recorder : GORRERA

AMMUNITION

(1) : 7.62mm Ball, M80, 149 gr.

(2) :

(3) :

(4) :

Lot No. : UNKNOWN

Lot No. :

Lot No. :

Lot No. :

APPLICABLE STANDARDS OR PROCEDURES

(1) : NIJ-STD-0108.01

(2) : LEVEL III

(3) : REQUIRED VELOCITY: 2700-2800 FPS

Shot No.	Ammo.	Time 1 (usec)	Velocity 1 (ft/s)	Time 2 (usec)	Velocity 2 (ft/s)	Avg. Vel. (ft/s)	Penetration	Footnotes
1	1	1088	2757	1088	2757	2757	None	
2	1	1088	2757	1092	2747	2752	None	
3	1	1092	2747	1092	2747	2747	None	
4	1	1079	2780	1079	2780	2780	None	
5	1	1079	2780	1083	2770	2775	None	

BallistiCrete



United States of America

United States Patent and Trademark Office

BALLISTICRETE

Reg. No. 3,767,956 BALLISTICRETE, INC. (NEVADA CORPORATION)
Registered Mar. 31, 2015 15475 N. GREENWAY-MAVEREN LOOP, SUITE B21
SCOTTSDALE, AZ 85260

Int. Cl.: 19 FOR NON-METALLIC, CEMENTITIOUS BUILDING MATERIALS, NAMELY, HIGH IMPACT
AND BALLISTIC RESISTANT STUCCOS, PLASTERS AND PANELS FOR INTERIOR AND
EXTERIOR APPLICATIONS, (IN CLASS 19 (U.S. CLS. 1, 12, 33 AND 39))

TRADEMARK
PRINCIPAL REGISTER FIRST USE, 12-02-2009; IN COMMERCE, 12-02-2009.

THE MARK CONSISTS OF STANDARD CHARACTERS WITHOUT CLAIM TO ANY PAR-
TICULAR FONT, STYLE, SIZE OR COLOR.

IN 75/04 FOR 1011018-28-2007

THOMAS E. SHARPER JR., EXAMINING ATTORNEY



David J. Kyllas

BallistiCrete





Contact GigaCrete

Providing GREEN technology solutions around the World.

702.643.6363

www.gigacrete.com

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 EXCLUDE EDISON ELECTRIC INSTITUTE FROM INTERVENING IN THIS DOCKET
AND MOTION TO REQUIRE CERTIFICATION FOR ELECTRIC INDUSTRY AND TRADE
ASSOCIATION INTERVENTION

Submitted to FERC on May 13, 2020

I am the Complainant in this docket. I file these two motions pursuant to 18 CFR § 385.212 (Rule 212).

Background

On May 4, 2020, the President of the United States declared a national emergency and issued Executive Order 13920: "Securing the United States Bulk-Power System."¹ The order defines:

The term "foreign adversary" means any foreign government or foreign non-government person engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or its allies or the security and safety of United States persons.

The Government of the People's Republic of China has long been viewed as a foreign adversary of the United States. Specifically, in 2019 the Director of National Intelligence stated:²

Our adversaries and strategic competitors will increasingly use cyber capabilities—including cyber espionage, attack, and influence—to seek political, economic, and military advantage over the United States and its allies and partners. China, Russia, Iran, and North Korea increasingly use cyber operations to threaten both minds and machines in an expanding number of ways—to steal information, to influence our citizens, or to disrupt critical infrastructure.

The director of National Intelligence also stated:

¹ Available at: <https://www.govinfo.gov/content/pkg/FR-2020-05-04/pdf/2020-09695.pdf> (Accessed May 10, 2020).

² Coats, Daniel R. Director of National Intelligence (DNI) "Worldwide Threat Assessment of the U.S. Intelligence Community" Senate Select Committee on Intelligence. January 29, 2019. Available at: <https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf> (Accessed May 10, 2020).

China presents a persistent cyber espionage threat and a growing attack threat to our core military and critical infrastructure systems. China remains the most active strategic competitor responsible for cyber espionage against the US Government, corporations, and allies. It is improving its cyber attack capabilities and altering information online, shaping Chinese views and potentially the views of US citizens—an issue we discuss in greater detail in the Online Influence Operations and Election Interference section of this report.

- *Beijing will authorize cyber espionage against key US technology sectors when doing so addresses a significant national security or economic goal not achievable through other means. We are also concerned about the potential for Chinese intelligence and security services to use Chinese information technology firms as routine and systemic espionage platforms against the United States and allies.*
- *China has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks—in the United States.*

Edison Electric Institute’s Ties to a Foreign Adversary as Defined in Executive Order 13920.

Edison Electric Institute (EEI) is the trade organization that purports to represent “all U.S. investor-owned electric companies.”³ EEI is a frequent intervenor and commenter in FERC dockets related to Critical Infrastructure Protection (CIP) standards and issues.⁴ EEI spends millions of dollars annually lobbying the U.S. Congress on matters pertaining to the U.S. Critical infrastructure.⁵ EEI also makes contributions to key members of Congress involved in critical infrastructure security legislation.⁶

Attached as Exhibit A is EEI’s member list, dated February 2020 which I downloaded from EEI’s website on May 10, 2020.⁷ EEI counts among its members State Grid Corporation of China, which is a state-owned corporation, owned by the government of the People’s Republic of China. EEI also counts as a member Power Assets Holdings, a company based in Hong Kong (which China calls “Hong Kong Special Administrative Region of the People’s Republic of China”).

Attached as Exhibit B is EEI’s member list dated February 2020 which I downloaded from EEI’s website on April 10, 2020. In this version, EEI counted among its members State Grid Corporation of China as well as China Southern Power Grid Co. Both of these are state-owned entities, owned by the government of the People’s Republic of China. EEI also counts as a member Power Assets Holdings, a company based in Hong Kong (which China calls “Hong Kong Special Administrative Region of the People’s Republic of China”).

³ See: <https://www.eei.org/about/Pages/default.aspx> (accessed May 10, 2020).

⁴ See, for example, FERC Dockets EL20-21-000, AD19-18-000, RM15-14-000 and NP19-4-000.

⁵ See: <https://www.opensecrets.org/federal-lobbying/clients/summary?cycle=2018&id=D000000297> (accessed May 10, 2020).

⁶ See: <https://www.opensecrets.org/pacs/pacgot.php?cycle=2018&cmte=C00095869> (accessed May 10, 2020).

⁷ Downloaded on May 10, 2020 from

https://www.eei.org/about/members/uselectriccompanies/Documents/memberlist_print.pdf

Attached as Exhibit C is EEI's member list dated May 2019 which I downloaded from EEI's website on May 29, 2019. In this version, EEI counted among its members State Grid Corporation of China as well as China Southern Power Grid Co. Both of these are state-owned entities, owned by the government of the People's Republic of China. EEI also counts as a member Power Assets Holdings, a company based in Hong Kong (which China calls "Hong Kong Special Administrative Region of the People's Republic of China").

These three Chinese companies have an obligation under the 2017 Chinese National Intelligence Law to "support, assist and cooperate with the state intelligence work." Moreover, under China's 2014 Counter-Espionage Law⁸ a company may not refuse the Chinese government when asked for information. In fact, according Dr. Murray Scot Tanner's Lawfare Institute analysis:⁹

"The Intelligence Law, by contrast, repeatedly obliges individuals, organizations, and institutions to assist Public Security and State Security officials in carrying out a wide array of 'intelligence' work. Article Seven stipulates that 'any organization or citizen shall support, assist, and cooperate with state intelligence work according to law.' Article 14, in turn, grants intelligence agencies authority to insist on this support: 'state intelligence work organs, when legally carrying forth intelligence work, may demand that concerned organs, organizations, or citizens provide needed support, assistance, and cooperation.' Organizations and citizens must also protect the secrecy of 'any state intelligence work secrets of which they are aware'."

So, at least three members or former members of the Edison Electric Institute have an obligation to provide information and assistance to the government of the People's Republic of China.

In other words, the government of the People's Republic China—the very government that has been hacking the North American electric grid for years—is, a for all intents and purposes, a member of Edison Electric Institute through its state owned corporations and other entities that owe their allegiance and obligations to the PRC.

Moreover, Chinese companies have been "affiliates" of EEI since at least 2014,¹⁰ and State Grid Corporation of China has been a member of EEI since at least 2016.¹¹ Exhibit D is EEI's February 2016 Member List.

The relationship seems far from casual: Exhibit E is the EEI's press release on June 6, 2018 when EEI awarded State Grid Corporation of China "Edison Electric Institute's (EEI's) 2018 International Edison Award."¹²

⁸ <https://www.reuters.com/article/us-china-lawmaking-spy-idUSKBN0IL2N520141101> (accessed May 10, 2020).

⁹ <https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense> (accessed May 10, 2020).

¹⁰ See EEI's website on February 14, 2014 archived at:

<https://web.archive.org/web/20140214141920/http://www.eei.org/about/members/internationalaffiliates/Pages/interaffiliatelist.aspx> (accessed May 10, 2020).

¹¹ See EEI's website on October 11, 2016 archived at:

<https://web.archive.org/web/20161011162447/http://www.eei.org/about/members/internationalaffiliates/Pages/interaffiliatelist.aspx> (accessed May 10, 2020).

¹² Also available at: [http://www.eei.org/resourcesandmedia/newsroom/Pages/Press Releases/State Grid Corporation of China Wins EEI's 2018 International Edison Award0606-2042.aspx](http://www.eei.org/resourcesandmedia/newsroom/Pages/Press%20Releases/State%20Grid%20Corporation%20Wins%20EEI's%202018%20International%20Edison%20Award0606-2042.aspx) (accessed May 10, 2020).

Exhibit F is a press release from the State-owned Assets Supervision and Administration Commission of the State Council (SASAC) announcing State Grid Corporation of China's receipt of the EEI "Edison Award."¹³ Note that the SASAC "is an ad-hoc ministerial-level organization directly subordinated to the State Council. The Party Committee of SASAC performs the responsibilities mandated by the Central Committee of the Chinese Communist Party."¹⁴

Exhibit G is a press release from the China Electricity Council (CEC)¹⁵ announcing that EEI and the China Electricity Council (whose "President Member" is the State Grid Corporation of China¹⁶) entered into a formal "memorandum of understanding" (MOU).

Exhibit H is EEI's press release on this MOU between EEI and the China Electricity Council.¹⁷ This picture is included in EEI's press release:



Photo Source: Edison Electric Institute

¹³ Also available at: http://en.sasac.gov.cn/2018/06/07/c_98.htm (accessed May 11, 2020).

¹⁴ See: <http://en.sasac.gov.cn/aboutus.html> (accessed May 11, 2020).

¹⁵ Also available at: <http://english.cec.org.cn/No.105.1619.htm> (accessed May 10, 2020).

¹⁶ See: <http://english.cec.org.cn/No.86.index.htm> (accessed May 11, 2020).

¹⁷ Also available at: <https://www.eei.org/resourcesandmedia/energynews/Pages/EEI%20and%20China%20Electricity%20Council%20Sign%20MOU.aspx> (accessed May 10, 2020).

While Edison Electric Institute may be free to have whomever it wishes as members, associates and awardees, it is not in the public interest for an organization with such ties to a foreign adversary, as defined in Executive Order 13920, to intervene in a docket involving issues of U.S. national security.

Motion to Exclude Edison Electric Institute from Intervening in this Docket

For the reasons above, FERC should EXCLUDE Edison Electric Institute from Intervention in this docket due to their membership including a foreign adversary as defined in Executive Order 13920 and their affiliations with entities controlled by a foreign adversary as defined in Executive Order 13920.

Motion to Require Certification for Electric Industry and Trade Association Intervention

For the reasons above, FERC should require that any trade organization or investor owned utility wishing to intervene in this docket 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.

Respectfully submitted,



Michael Mabee

Attachments: Exhibits A through H

Certification:

I certify that a copy of this document was served on the Electric Reliability Organization (ERO) and Edison Electric Institute (EEI) simultaneously with my filing with the Commission.



Michael Mabee

[LOG IN](#)[DELIVERING THE FUTURE](#)[ISSUES & POLICY](#)[RESOURCES & MEDIA](#)[MEETINGS](#)[ABOUT EEI](#)[FOR MEMBERS](#)

IN THIS SECTION

[Contact Media Relations](#)[Energy News Stories](#)[Press Releases](#)[EEI > Resources & Media > Newsroom > State Grid Corporation of China Wins EEI's 2018 International Edison Award](#)

STATE GRID CORPORATION OF CHINA WINS EEI'S 2018 INTERNATIONAL EDISON AWARD

SAN DIEGO (June 6, 2018) – State Grid Corporation of China (SGCC) today received the Edison Electric Institute's (EEI's) 2018 International Edison Award, the U.S. electric power industry's most prestigious honor. A panel of former energy company chief executives selected SGCC for the annual award from a group of distinguished finalists.

A robust, integrated, and flexible charging network is essential for electric vehicle (EV) growth and deployment in China. SGCC developed the Smart Internet of Vehicles EV Charging Network, which allows the company to expand its EV capacity. In the process, SGCC overcame significant barriers to success, including a lack of standards for manufacturers, to build the largest EV charging network in the world.

"State Grid Corporation of China's exemplary effort to build smarter energy infrastructure that supports the expansion of electric vehicles demonstrates our industry's commitment to customers and to accelerating transportation electrification throughout the world," said EEI President Tom Kuhn. "The reduction of transportation pollution is a global challenge, and the electric power industry is taking significant steps to reduce greenhouse gas emissions throughout the world by building the charging infrastructure that is needed to advance electric vehicle adoption."

SGCC has established, maintained, and continuously expanded the world's largest EV charging network and EV service platform. It has constructed 6,286 stations (last updated April 2018) and 56,000 charging piles throughout China. The "9 East-West Highways, 9 North-South Highways, 2 Beltways" covers almost 20,000 miles (last updated April 2018) of distance in more than 150 cities. The EV charging platform also has enabled access of 183,000 charging pile (last updated April 2018) from other service operators, which effectively promotes the reliability of EV charging as well as the development of the EV industry in China.

"Congratulations to the SGCC team for winning the 2018 International Edison Award," said Kuhn.

Media Contact

EEI Media Relations

Kristin Rudman

krudman@eei.org

202-508-5155

www.eei.org

EEI is the association that represents all U.S. investor-owned electric companies. Our members provide electricity for more than 220 million Americans, and operate in all 50 states and the District of Columbia. As a whole, the electric power industry supports more than 7 million jobs in communities across the United States. In addition to our U.S. members, EEI has more than 65 international electric companies, with operations in more than 90 countries, as International Members, and hundreds of industry suppliers and related organizations as Associate Members.

© Edison Electric Institute. All rights reserved.

[Careers](#) | [Contact Us](#) | [Newsroom](#) | [Privacy Policy](#) | [Terms of Use](#) | [Site Map](#) | [Facebook](#) | [Twitter](#) | [YouTube](#) | [RSS](#)



Home > SOEs News

SGCC wins the 2018 International Edison Award

Updated: 2018-06-07

The Edison Electric Institute, an association representing all the investor-owned electric companies in the United States, recently announced that State Grid Corporation of China (SGCC) won the 2018 International Edison Award for its exemplary effort of building a smart energy infrastructure that supports the expansion of the electric vehicle industry.



State Grid Corporation of China (SGCC) wins the 2018 International Edison Award on June 6. [Photo/sasac.gov.cn]

State Grid is the first Chinese company in the sector to receive the most prestigious honor in the US electric power industry.

It has developed a Smart Internet of Electric Vehicles Charging Network, the largest EV charging network in the world, which reflects SGCC's development goal of becoming a top world energy internet company, and also showcases the company's growing international influence.

As of April, the company had established 6,286 charging stations and 56,000 charging piles throughout China. The plan of "9 East-West Highways, 9 North-South Highways, 2 Beltways" covers almost 31,000 kilometers of distance in more than 150 cities. The EV charging platform also has enabled access of 183,000 charging piles from other service operators, which effectively promotes the development of China's EV industry.



Specials



Your current location : [Home](#) > [Newsroom](#) > [CEC News](#)

Newsroom

CEC News

Industry News



CEC News

CEC signed MOU with EEI

On June 3, 2016, Mr. Liu Zhenya, President of China Electricity Council(CEC), met Mr. Thomas R. Kuhn, President of Edison Electric Institute (EEI)in Beijing. CEC and EEI signed a memorandum of understanding (MOU) to deepen cooperative partnership and promote mutual development between the two organizations and their member companies.

President Liu Zhenya reviewed recent discussions between the two organizations and vowed to cooperate with EEI to serve as a bridge between power industries of both countries. President Kuhn further introduced recent activities and future plans of EEI, and agreed on the positive role of the two associations in the future Sino-US power industry cooperation. EEI Vice President of International Programs Lawrence Jones and CEC Executive Vice President Yang Kun signed the MOU.

EEI is an industry association for power sector of the US with domestic members of power utilities and international members across Europe and Asia.

Home	About Us	Newsroom	Data & Publications	Featured Events & Programs	Power Industry Basics	Contact Us
	CEC in Brief President's Message Executives Functions Structure Members	CEC News Industry News	Reports and Publications Data/Statistics Standards Reliability	Events Programs Multimedia	Generation Distribution/Grids Consumption Sustainability Regulator	

IN THIS SECTION

[Antitrust Compliance Guidelines](#)
[Electric Perspectives Magazine](#)
[Energy Talk](#)
[Industry Data](#)
[Industry Training and Testing](#)
[Master Contract](#)
[Meetings](#)
[Newsroom](#)
[Products](#)

EEI > Resources & Media > Energy News Stories

EEI AND CHINA ELECTRICITY COUNCIL SIGN MOU

In early June, EEI and the China Electricity Council (CEC) signed a memorandum of understanding (MOU) to deepen cooperative partnership and promote mutual development between the two organizations and their member companies. EEI President Tom Kuhn and CEC President Liu Zhenya, who is also the former Chairman of State Grid Corporation of China (SGCC), attended the signing ceremony held June 3 in Beijing. SGCC is an International Member of the Institute.

EEI Vice President of International Programs Lawrence Jones and CEC Executive Vice President Yang Kun signed the MOU, which will serve as a strong foundation for deeper cooperation in the areas of innovation, clean energy, and global energy interconnection.

Founded in 1988, CEC is a joint organization of China's power enterprises and institutions with 939 members engaged in all aspect of the power industry, including power generation, transmission, distribution, engineering, construction, and R&D.





Edison Electric
INSTITUTE

Power by AssociationSM

Members List

U.S. Investor-Owned Electric Companies
International Members
Associate Members

EEI is the association that represents all U.S. investor-owned electric companies. Our members provide electricity for 220 million Americans, operate in all 50 states and the District of Columbia, and directly employ more than 500,000 workers. With more than \$90 billion in annual capital expenditures, the electric power industry is responsible for millions of additional jobs. Reliable, affordable, and sustainable electricity powers the economy and enhances the lives of all Americans. Organized in 1933, EEI provides public policy leadership, strategic business intelligence, and essential conferences and forums.

U.S. Investor-Owned Utilities

AES Corporation	Edison International	NorthWestern Energy
Dayton Power & Light Company	Southern California Edison	OGE Energy Corporation
Indianapolis Power & Light Company	El Paso Electric Company	Oklahoma Gas & Electric Company
ALLETE	Emera Maine	Ohio Valley Electric Corporation
Minnesota Power	Empire District Electric Company	Otter Tail Corporation
Superior Water, Light and Power Company	Energy Future Holdings Corporation	Otter Tail Power Company
Alliant Energy Corporation	Oncor	Pepco Holdings
Ameren Corporation	Entergy Corporation	Pepco
Ameren Illinois	Entergy Arkansas	Atlantic City Electric
Ameren Missouri	Entergy Louisiana	Delmarva Power
American Electric Power	Entergy Mississippi	PG&E Corporation
AEP Ohio	Entergy New Orleans	Pacific Gas & Electric Company
AEP Texas	Entergy Texas	Pinnacle West Capital Corporation
Appalachian Power	Eversource Energy	Arizona Public Service Company
Indiana Michigan Power	Exelon Corporation	PNM Resources
Kentucky Power	Baltimore Gas & Electric Company	PNM
Public Service Company of Oklahoma	Commonwealth Edison Company	TNMP
Southwestern Electric Power Company	PECO Energy Company	Portland General Electric
American Transmission Company	FirstEnergy Corporation	PPL Corporation
AVANGRID	The Illuminating Company	PPL Electric Utilities Corporation
Central Maine Power Company	Jersey Central Power & Light	LG&E and KU
New York State Electric & Gas Corporation	Met-Ed	Public Service Enterprise Group
Rochester Gas & Electric Corporation	Mon Power	Public Service Electric and Gas Company
The United Illuminating Company	Ohio Edison	PSEG Long Island
Avista Corporation	Penelec	Puget Sound Energy
Avista Utilities	Penn Power	SCANA Corporation
Alaska Electric Light and Power Company	Potomac Edison	South Carolina Electric & Gas
Berkshire Hathaway Energy	Toledo Edison	Sharyland Utilities
MidAmerican Energy Company	West Penn Power	Southern Company
NV Energy	Florida Public Utilities Company	Alabama Power Company
PacifiCorp	Great Plains Energy	Georgia Power Company
Pacific Power	Kansas City Power & Light Company	Gulf Power Company
Rocky Mountain Power	Green Mountain Power Corporation	Mississippi Power Company
Black Hills Corporation	Hawaiian Electric Industries	Talen Energy
Black Hills Energy	Hawaiian Electric Company	TECO Energy
CenterPoint Energy	Hawaii Electric Light Company	Tampa Electric
Central Hudson Gas & Electric Corporation	Maui Electric Company	Tennessee Valley Authority – EEI Strategic Partner
Cleco Corporation	IDACORP	UGI Corporation
Cleco Power	Idaho Power Company	UGI Utilities
CMS Energy Corporation	InfraREIT	Unitil Corporation
Consumers Energy	ITC Holdings Corporation	UNS Energy Corporation
Consolidated Edison	ITC Great Plains	Tucson Electric Power
Consolidated Edison Company of New York	ITC Michigan	UniSource Energy Services
Orange and Rockland Utilities	ITC Midwest	Upper Peninsula Power Company
Pike County Light & Power Company	Liberty Utilities	Vectren Corporation
Rockland Electric Company	MDU Resources Group	Vectren South
Cross Texas Transmission	Montana-Dakota Utilities Company	Vermont Electric Power Company
Dominion	MGE Energy	WEC Energy Group
Dominion Virginia Power	Madison Gas and Electric Company	We Energies
Dominion North Carolina Power	Mt. Carmel Public Utility Company	Wisconsin Public Service Corporation
DTE Energy Company	National Grid	Westar Energy
Duke Energy Corporation	NextEra Energy	Xcel Energy
Duquesne Light Holdings	Florida Power & Light Company	
Duquesne Light Company	NiSource	
	Northern Indiana Public Service Company	

International Members

AES Corporation
AltaLink L.P. – Canada
ATCO Electric – Canada
ATCO Power – Canada
Bahamas Electricity Corporation – Bahamas
Belize Electricity Ltd – Belize
Bermuda Electric Light Co., Ltd. – Bermuda
Brookfield Renewable Power Inc. (*formerly Brascan Power*) – Canada
Calcutta Electric Supply Corporation - India
Capital Power Corporation – Canada
Caribbean Utilities Company, Ltd. – Cayman Islands, British West Indies
CEMIG - Brazil
Chubu Electric Power Co., Inc. – Japan
Comisión Federal de Electricidad (CFE) – Mexico
EDF, S.A.. – France
Electricity Generating Company Haina, SA – Dominican Republic
Emera Inc. - Canada
Energias de Portugal (EdP) – Portugal
Enersource
Entegrus Powerlines
Ergon Energy - Australia
Fortis Alberta - Canada
Fortis BC – Canada
Fortis Ontario - Canada
Fortis TCI – Turks & Caicos
Hydro One – Canada
Hydro Ottawa – Canada
Hydro-Quebec – Canada
Iberdrola – Spain
Irbid District Electricity Company – Jordan
Jamaica Public Service Company – Jamaica
J-Power – Japan
Jemena – Australia
Kansai Electric Power Co., Inc. – Japan
Korea Electric Power Corporation – Korea
Korea Southern Power Co., Ltd. – Korea
Maritime Electric – Canada
National Grid plc – England
Newfoundland Power – Canada
Nova Scotia Power Inc. – Canada
Ontario Power Generation – Canada
Powerco Ltd. – New Zealand
Red Electrica – Spain
SaskPower – Canada
SA Power Networks – Australia
St. Lucia Electricity Services, Ltd. (LUCELEC) – St. Lucia, West Indies
St. Vincent Electricity Services, Ltd. (VINLEC) – St. Vincent & The Grenadines
State Grid Corporation of China – China
Tohoku Electric Power Co., Inc. – Japan
Tokyo Electric Power Co., Inc. – Japan
TransAlta – Canada
TransCanada – Canada
United Energy and Multinet Gas - Australia
Wellington Electricity Lines – New Zealand

Associates

Power-Plus Members

GE Power and Water
Navigant Consulting, Inc.
Oracle Utilities Global
SunPower Corp.

Power Members

EY Global Services Limited
Leidos Engineering, LLC
Mitsubishi Electric Power Products, Inc. (MEPPI)
Nest Labs, Inc.
Pike Electric, LLC
Troutman Sanders LLP
Utilities International, Inc.

Associate Members

ABB Inc.
Abengoa
Accenture
Aclara
ADA-ES, Inc.
AECOM
AEGIS Insurance Services, Inc.
Akin Gump Strauss Hauer & Feld, LLP
Alston & Bird LLP
Altec Inc.
Altran North America
Amec Foster Wheeler
American Heart Association
American Stock Transfer & Trust Company, LLC
American Water
American Wind Energy Association (AWEA)
Aquila Energy Services, Inc.
Arcadis U.S., Inc.
AREVA Inc.
Asplundh Brush Control Co.
Autodesk, Inc.
AutoGrid Systems

Babcock & Wilcox Company, The
Bain & Company, Inc.
Baker Botts L.L.P.
Baker Tilly Virchow Krause, LLP
Balch & Bingham LLP
Ballard Spahr LLP
Bates White, LLC
Berkeley Research Group, LLC
Bibb Engineers
Black & Veatch
Borden Ladner Gervais LLP
Bracewell & Giuliani LLP
BRIDGE Energy Group
Brooks Utility Products
Burns & McDonnell Engineering Co. Inc.

Capgemini
Cargill, Inc.
CB&I (formerly Shaw Power)
CBRE Clarion Securities

Centrus Energy Corp.
Chapman and Cutler LLP
Charles River Associates
Choate, Hall & Stewart LLP
Cisco Systems, Inc.
Citi
CLEAResult
Cloud Peak Energy
Collabera, Inc.
Commonwealth Associates, Inc.
Comverge
Concentric Energy Advisors, Inc.
Contract Land Staff, LLC
Credit Suisse LLC
Crowell & Moring LLP
CS Week
Curtis Stout
Cyient, Inc.

Davey Tree Expert Company, The
Davies Consulting LLC
Davis Wright Tremaine LLP
Day & Zimmerman
Day Pitney LLP
DDC Advocacy
Deloitte LLP
Dentons US LLP
DiGioia Gray
Disaster Resource Group
DNV GL Energy Services
Doble Engineering Company
Dorsey & Whitney LLP
Duane Morris LLP
DuPont Sustainable Solutions

E Source
Eaton Corporation
Ecology and Environment, Inc.
Ecova, Inc.
EFACEC USA, Inc.
EHS Partners, LLC
Electrical Consultants, Inc.
Elster Solutions, LLC
EMC, LLC
EN Engineering, LLC
EnergySavvy
EnerNOC, Inc.
Enovation Partners, LLC
Enphase Energy, Inc.
Environmental Consultants, Inc.
Ephektiv
ERM
Esri, Inc.
Evercore

Faegre Baker Daniels, LLP
Faneuil Inc.
Ferrandino & Son, Inc.
Finley Engineering Company, Inc.
First Solar, Inc.
Fluor Corporation
Foley & Lardner LLP

Associate Members (cont'd)

FTI Consulting, Inc.
Fugro ROAMES Pty Ltd.

G4S Secure Integration
General Cable Corporation
Gibson Dunn & Crutcher

Harkins Cunningham LLP
HazTek, Inc.
HD Supply
HDR, Inc.
Heidrick & Struggles
Henkels & McCoy, Inc.
HiLine Nation LLC
Hogan Lovells US LLP
Holland & Knight LLP
Houlihan Lokey
HP Enterprise Services, Inc.
Hunton & Williams LLP
Husch Blackwell LLP

IBM Corporation
ICF International
IHS Global Inc.
IMCORP
Information Services Group, Inc. (ISG)
Infosys Technologies Ltd.
Infratech Corporation
Innovari
International Technology and Trade Associates
Internet Security Alliance
InVizion LLC
ITRON, Inc.

Japan Electric Power Information Center, Inc.
(JEPIC)

K&L Gates LLP
KBR Power & Industrial
Kiewit Corporation
Kleinfelder, Inc.
KPMG LLP

Landis+Gyr Inc.
Lignite Energy Council
Lindsey Manufacturing Co.
Lockheed Martin Corporation
Loeb & Loeb LLP

MacLean Power Systems
MADA Power, LLC
MasTec Transmission – Substation Group
Matrix NAC
McCarter & English, LLP
McGuireWoods LLP
McKinney Drilling Company
McKinsey & Company
Merjent Inc.
Michael Best & Friedrich LLP
Michels Corporation
Microsoft Corporation

Midwest Energy Efficiency Alliance
Milbank, Tweed, Hadley & McCloy LLP
Milwaukee Tool
Mitsubishi Electric Power Products, Inc.
Mitsubishi Heavy Industries America
Mitsubishi Hitachi Power Systems Americas, Inc.
Moelis & Company
Moran Environmental Recovery, LLC
Morgan, Lewis & Bockius LLP
Mosaic
Motive Power Inc.
Motorola Utility Solutions
MYR Group Inc.

Natural Resource Group, LLC
Nexans High Voltage USA Inc.
Normandeau Associates, Inc.
Novar
Nuclear Electric Insurance Limited

Odyne Systems, LLC
Oliver Wyman
OMICRON electronics Corp. USA
OPOWER, Inc.
Osmose Utilities Services, Inc.

Pace Global
Parker Poe Adams & Bernstein, LLP
Pegasus Global Holdings, Inc.
Perkins Coie LLP
Philips Lighting Co.
Pike Corporation
Pillsbury Winthrop Shaw Pittman LLP
PLH Group, Inc.
Power Corporation of America
POWER Engineers, Inc.
PowerPlan, Inc.
PricewaterhouseCoopers LLP
Protiviti, Inc.
Prysmian Communications Cables and Systems
USA

Quanta Services

Radian Research, Inc.
Regional Economic Models Inc.
Regulated Capital Consultants
RES Americas Inc.
Resource Action Programs
RHR International LLP
Robin M. Nuschler, Esq. / Proprietor
Russell Reynolds Associates, Inc.

SafeTec Compliance Systems
Sargent & Lundy, LLC
Saulsbury Industries
Schiff Hardin LLP
Schneider Electric
Schweitzer Engineering Labs (SEL)
ScottMadden, Inc.
Sensus
SEPCON, Inc.

Shapiro, Lifschitz & Schram, P.C.
Shelton Group
Sidley Austin LLP
Siemens Energy, Inc.
Silver Spring Networks, Inc.
Skadden, Arps, Slate, Meagher & Flom LLP
SNC-Lavalin Inc.
Snell & Wilmer L.L.P.
Solar Electric Power Association (SEPA)
Spencer Stuart
SPIDA Software LLC
Stanley Consultants, Inc.
Stantec Consulting Services, Inc.
Stem, Inc.
Step toe & Johnson, LLP
Sterling Group
Stikeman Elliott LLP
Stinson Leonard Street LLP
Stoll Keenon Ogden PLLC
Strategy&
Structure
SWCA Environmental Consultants

Taft Stettinius & Hollister LLP
Tata Consultancy Services
Tecnicas Reunidas, S.A.
TEKsystems
Tenaska Marketing Ventures
Tenaska Power Services Co.
Terex Utilities
TerraForm Power
TestAmerica Laboratories, Inc.
Townsend Corporation, The
Trilliant, Inc.

UC Synergetic, Inc.
United States Energy Association (USEA)
Unmanned Experts Inc.
UtiliCon Solutions, Limited
Valmont Industries, Inc.
Van Ness Feldman, LLP
Varentec, Inc.
VIA Motors, Inc.
ViaSat, Inc.

Wartsila North America, Inc.
Waste Management, Inc.
Waterfall Security Solutions
WESCO Distribution Inc.
West Corporation
White & Case LLP
Wilson Construction Co.
Winston & Strawn LLP
Womble Carlyle Sandridge & Rice, LLP
Wright & Talisman, P.C.

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.”

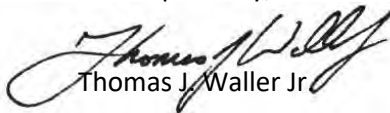
With EPRI's collaboration reaching outside of the United States and specifically involving Chinese state-owned utilities beholden to the intelligence gathering apparatus of the Chinese Communist Party – including at least one which has been placed on the U.S. Commerce Department's “Entity List” – there 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.