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 Coalition[1] 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 docket[3], but we would like to particularly draw your attention to three sets of motions busmitted 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 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 <u>not</u> 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 CigaCrete. 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 Mabee: https://michaelmabee.info/ferc-denies-grid-physical-security-complaint/