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

February 4, 2021

TO: The Honorable Jennifer Granholm, Nominee, Secretary of the Department of Energy

CC: Robert Fairweather, Acting Director of the Office of Management and Budget
David G. Huizenga, Acting Secretary of the Department of Energy
Patricia A. Hoffman, Acting Assistant Secretary of Energy (OE-1)
Charles Kosak, Energy Resilience Division, U.S. Department of Energy (OE-20).

Subj: Improving Executive Branch Policies to Secure the United States Electric Grid

Dear Nominee for Secretary of Energy, Honorable Jennifer Granholm,

I hope that you will be confirmed and in office as soon as possible. I write on behalf of the non-partisan, professional Secure the Grid (STG) Coalition to help you carry out President Biden's assignment in Executive Order (EO) 13990 of January 20, 2021, Subsection 7(c) that you review "Executive Order 13920 of May 1, 2020 (Securing the United States Bulk-Power System), ... [and] ... jointly consider (with the Director of OMB) whether to recommend that a replacement order be issued."

Our Secure the Grid Coalition[1] has long worked to improve the security of our nation's most critical infrastructure – the electric grid. We recognize that a prolonged and widespread electrical blackout would cripple every one of our nation's 16 critical infrastructures, causing immense harm to our economy, our people, our national security, and – especially – our environment.

We are therefore encouraged by your thoughtful confirmation hearing response to Senator Murkowski:

> *". . . We have 5 million miles of distribution wires, 200,000 miles of high-voltage electric wires. I haven't been fully briefed on the national security, and the confidential aspects of the SolarWinds cyber hack, but clearly that's one example and we are getting hacked all the time and attacked all the time. We will have, inside the DOE, a person at a very high level that is responsible for making sure the response to this is coordinated. We have to harden our electric grid for protection of our energy system. I hope that this is a part of the infrastructure package that will be coming from the administration as well." (Emphasis added)*

Understanding that you will appoint a high-level official to coordinate the review of Executive Order 13920, the SolarWinds hack and other important issues surrounding the security of the electric grid, we would like to provide you (and them) with a series of observations and recommendations.

We believe you should, and trust that you will, recommend stronger and more effective protections than did the previous Administration to secure the bulk-power system and other critical electric power facilities, and to safeguard the public. We therefore anticipate you will recommend that President

[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

Biden's Administration carefully improve and strengthen EO 13920 of May 1, 2020, by fixing defects and better enforcing its implementation.

The attached appendix identifies **four key areas where EO 13920 can be strengthened**. These include: (1) recommending a broadened focus down to the state/local "distribution" portion of the grid and the implementation of electromagnetic pulse (EMP) protection provisions required by law, (2) improving the DOE's "Prohibition Order," (3) addressing supply chain vulnerabilities of Large Power Transformers (and related information sharing procedures), and (4) addressing hazards to the grid stemming from the Russian Federation and an ineffective cybersecurity regulation regime developed over the past two decades.

—Regarding supply chain vulnerabilities of Large Power Transformers: **Sandia National Laboratory should brief you as soon as possible** on the "Chinese Transformer" case:

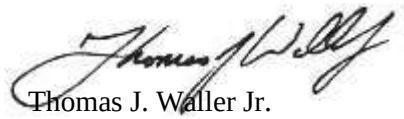
https://www.controlglobal.com/blogs/unfettered/information-sharing-on-control-system-cyber-incidents-isnt-working-the-chinese-transformer-case/

We also re-address concerns we voiced to the previous administration that were not acted upon, including the need to (1) remedy direct current (DC) and EMP vulnerabilities to Large Power Transformers, to (2) prohibit the use of foreign sourced robotics (such as drones) which highlight grid vulnerabilities, to (3) withstand foreign and domestic lobbying for "business as usual" approaches to grid security, and to (4) demand that personnel and organizations trusted with U.S. Government collaboration cut ties with foreign adversaries.

The appendix provides hyperlinks where your staff can access the nearly 200 pages of research and recommendations compiled by experts in our Coalition from May 1, 2020 (when Executive Order 13920 was signed) to the present.

We recognize that President Biden suspended Executive Order 13920 for 90 days, implying that your recommendation should be submitted by April 20, 2021. Even if some recommendations may require more time to mature, we trust that you and OMB will be able to recommend significant improvements by then. Members of our Coalition are ready and willing to support you, your staff, and the Biden-Harris Administration in the effort to Secure the Grid.

Sincerely,



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

Enclosed: Appendix – Improving Executive Branch Policies to Secure the United States Electric Grid

Appendix: Improving Executive Branch Policies to Secure the United States Electric Grid

(1) Strengthening EO 13920 and its Implementation

We count on the Biden-Harris administration to strengthen EO 13920 and to effectively implement protections to the supply chain for all portions of the electric grid (not just the Bulk Power System) and the hardening of the most critical grid components from all hazards. For example:

— EO-13920 was focused on a top-down directed (from Washington down but not to a local level) operation formulated almost entirely on the "Bulk Power Grid," which according to the EO's definition "includes transmission lines rated at 69,000 volts (69 kV) or more *but does not include facilities used in the local distribution of electric energy*." The thus omitted "Distribution Grid" is the final link in the electric power grid that delivers electricity to businesses, military operations, emergency management, and citizens—and composes 90-percent of the overall grid and about 70-percent of the cost of the combined Transmission and Distribution network.

— EO-13920 did not mention severe threats posed by natural (from major solar storms) or manmade electromagnetic pulses (EMPs) that America's enemies consider to be within the cyber warfare domain, since these hazards often affect the same systems that are the targets of cyberattacks.

We observe that President Biden has left in place Executive Order 13865 of March 26, 2019 (Coordinating the Resilience to Electromagnetic Pulses.) It called for a "whole of government" effort led by the National Security Council to counter manmade and natural existential electromagnetic pulse (EMP) threats and is partially codified as Section 1740 of the 2020 National Defense Authorization Act (NDAA) [Public Law 116-92. (6 U.S.C. 195f)]. Your leadership can help the government carry out these and other executive/legislative provisions, overcoming obstacles to EMP resilience for the electric grid.

Links:

— January 20, 2021 **Executive Order 13990,** "Executive Order on Protecting Public Health and the Environment and Restoring Science to Tackle the Climate Crisis".
https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01765.pdf

— **May 1, 2020 Executive Order 13920,** "Securing the United States Bulk Power System".
https://www.govinfo.gov/content/pkg/FR-2020-05-04/pdf/2020-09695.pdf

— March 26, 2019 **Executive Order 13865**, "Coordinating National Resilience to Electromagnetic Pulses"
https://www.govinfo.gov/content/pkg/FR-2019-03-29/pdf/2019-06325.pdf

(2) Improving the Department of Energy's "Prohibition Order"

Although the Department of Energy's "Prohibition Order" became effective, by its terms, on January 16, 2021, it was a product of work that was initiated *years* before the May 1, 2020, EO13920 (in some senses including the Obama-Biden Administration), work which helps explain why EO13920 needed to be issued in the first place.

We expect improvement under your leadership as to supply chain issues only partially addressed by this "Prohibition Order." For example, it should consider distribution and sensor vulnerabilities (see Section 6 of Prohibition Order: "BPS Electric Equipment Subject to this Prohibition Order").

Links:

— Secretary of Energy Brouillette's December 17, 2020, **Press Release** announcing his conclusions and limited Prohibition Order (https://www.energy.gov/articles/secretary-energy-signs-order-mitigate-security-risks-nations-electric-grid).

— Federal Register text of **Prohibition Order** (https://www.energy.gov/sites/prod/files/2020/12/f81/BPS%20EO%20Prohibition%20Order%20Securing%20Critical%20Defense%20Facilities%2012.17.20%20-%20SIGNED.pdf).

(3) Addressing Supply Chain Vulnerabilities of Large Power Transformers

Transformers play a critical role in the functioning of the electric grid and, generally, the larger they are the more difficult and time consuming they are to replace. Because of the criticality of these assets to the functioning of the Bulk Power System, it is imperative that extra high voltage transformers and their components be sourced from reliable and trustworthy vendors. Moreover, these "reliable vendors" need to use "whitelisting" and other safeguards that protect their supply chains from foreign malware or adversarial manipulation.

Based upon data collected by the U.S. International Trade Commission (ITC)[2], approximately 300 electric power transformers have been imported from the People's Republic of China (PRC) for use in the United States over the 14-year period 2006 through 2019. These Chinese transformer imports to the U.S. average more than 20 per year. Of greatest concern are "large power transformers" – which make up the "backbone" of the grid.

Charles Durant, deputy director of the U.S. Department of Energy's Counterintelligence Office, noted in 2019 that over the past decade**, more than 200 Chinese large power transformers have entered the U.S. energy system**.[3]

At least one Chinese transformer in the U.S. grid has been discovered to have a hardware "backdoor" which could be used as a vector of attack to change transformer voltage settings and possibly to damage both the transformers and critical transmission circuits that depend upon transformer operations within authorized parameters.[4]

While the Chinese Chamber of Commerce wrote to the U.S. Commerce Department's Bureau of Industry and Security ("BIS") in 2020 in an effort to minimize the perceived hazards (both as to transformers and spare parts), submitting that most imports to the United States come from other

---

[2] *The U.S. Has 300 Chinese Large Power Transformers. What could possibly go wrong?* https://michaelmabee.info/the-u-s-has-300-chinese-large-power-transformers/

[3] *China and America's 400-ton Electric Albatross*, Blake Sobczak and Peter Behr, E&E News reporters, Energywire: Thursday, April 25, 2019 https://www.eenews.net/stories/1060216451

[4] ICS cyber security is the second coming of the Maginot Line – and the Chinese have breached it https://www.controlglobal.com/blogs/unfettered/ics-cyber-security-is-the-second-coming-of-the-maginot-line-and-the-chinese-have-breached-it/

countries, this submission ignored the reality that manufacturers in other countries utilize hardware parts, control systems and firmware from China, and/or use Chinese designs and software.[5]

— You can appreciate from automobile industry experience that a Honda or Toyota facility in the USA might assemble vehicles with a higher percentage of total USA content than a Ford or General Motors facility if one considered countries where parts originated, for a full, realistic assessment.

— Another issue is sensitivity of locations where large, imported transformers were installed. For example:

The Department of Energy's Western Area Power Administration (WAPA), ordered from China's Jiangsu Huapeng Transformer Company (also known as JSHP) a 500,000 pound transformer to service WAPA's Ault, Colorado substation. This substation serves as an important interconnection between the Powder River, Wyoming basin -- baseline generation -- and baseline power supplies to Colorado, a state with key military installations plus other key national security-essential ground stations. Colorado depends upon just in time gas pipeline supplies for electricity plus renewables without adequate energy storage on site. So, the 345 kV transmission system from Wyoming is critical to national security facility electric supplies in Colorado.

— We trust that you will want to determine how many utilities were (and are still) forced to purchase Chinese transformers due to corporate, government, or regulator low-cost procurement requirements and lack of availability of domestic manufacturers.

— In 2020, a transformer was seized at the Port of Houston by U.S. Government officials and transported, with federal escort, to Sandia National Laboratory (SNL) where it was received and (presumably) fully analyzed.[6]

We believe it is critical that you, your team, and Congressional Committees be briefed on Sandia's conclusions. We also agree with the assessment of internationally acclaimed industrial control cybersecurity expert Joe Weiss regarding this case of the Chinese-made transformer:

> *"The importance of the industry knowing if there are hardware backdoors in the Chinese-made transformer sent to SNL cannot be minimized. If there are hardware backdoors in the Chinese-made transformer at SNL in addition to the known backdoor in the Chinese-made transformer installed at a US utility substation, the question then becomes how many other Chinese-made transformers already installed in the US grid (and elsewhere) have hardware backdoors?"*[7]

Thus, it is essential that the Department of Energy and its national laboratories work with the private sector to improve information sharing, to locate all Chinese transformers, and to develop hardware, sensor and control system monitoring technologies to be able to know how and when to mitigate the types of threats associated compromised supply chains. We understand that these assets cannot be readily removed from the Bulk Power System and they take years to replace so we believe your Department should work with the whole of government and private sector experts to develop guidance

---

[5] The China Chamber of Commerce for Import and Export of Machinery and Electronic Products ("CCCME") filed a written statement pursuant to the request of the Bureau of Industry and Security, U.S. Department of Commerce ("BIS") on Section 232 National Security Investigation of Imports of Electrical Transformers and Electrical Transformers Parts, Vol.85, No.97 Fed. Reg. 29,926 (May 19, 2020) ("Section 232 Investigations of Imports of Electrical Transformers and Electrical Transformers Parts").

[6] U.S. Seizure of Chinese-Built Transformer Raises Specter of Closer Scrutiny
https://www.wsj.com/articles/u-s-seizure-of-chinese-built-transformer-raises-specter-of-closer-scrutiny-11590598710

[7] Information sharing on control system cyber incidents isn't working – the Chinese Transformer Case:
https://www.controlglobal.com/blogs/unfettered/information-sharing-on-control-system-cyber-incidents-isnt-working-the-chinese-transformer-case/

and incentives to expeditiously replace these assets, as prudence requires, with transformers which are domestically sourced and secured against all-hazards (including network and control system cyber threats and natural and manmade electromagnetic spectrum threats such as EMP.)

(4) Addressing How the Russian Federation Hazards the Grid:

Another urgent threat is the Russian Federation's exploitation of cybersecurity vulnerabilities which stem from an ineffective domestic regulation regime developed over the past two decades.

We direct you to the research of George Cotter, one of the world's most experienced cryptologists who began his service to our nation as an intelligence analyst in the U.S. Navy. He joined the National Security Agency in 1952 and served there for more than forty years, rising to the rank of the organization's Chief Information Officer (CIO.)

Mr. Cotter studied gaps in the cybersecurity protection regime for the Bulk Power System. He submitted to the Federal Energy Regulatory Commission (FERC) five (5) "Motions to Intervene" (MTIs) on various dockets. His research required study of four industry compliance audits of either CIP Standards or a parallel massive, independent set of Engineering Standards. The latter, in existence long before CIP, were essential to industry management of power flows between eight separated Grid regions. FERC and NERC Regulators structured CIP standards so they would not interfere with those "Operations", directly violating the law (Federal Power Act as amended 2005) which legislated CIP Standards. **These five MTIs have not been responded to by FERC in any related 2020 orders and notices**.

We summarize each MTI below and provide a hyperlink to the actual document and include the following excerpts :

> "**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."**

Mr. Cotter also provided the following "Exposure Summary":

> **"[E]xperts in the five or six critical infrastructures, including…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 [Russian] Federation out of deference to other industry priorities."**

Mr. Cotter provided a succinct history of the evolution of Critical Infrastructure Protection (CIP) standards:

> "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 [and the Federal Power Act] 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

"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. 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), 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."

Mr. Cotter's Five Motions to Intervene were submitted between April and November 2020. Their main thrust was to document inadequacy of cybersecurity protection for the Bulk Power System, the core of the power supplied to the State-regulated Distribution Systems.

Summaries are below:

1st MTI on Docket No. EL20-46-000

This Docket covered an associate's complaint focused 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. The MTI added to the complaint Supply Chain vulnerabilities, and more importantly, documents 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. As one example of two totally independent Engineering and CIP standards, the MTI contains a table summarizing over 476 pages of critical ***"operational"*** protection systems standards, whose cyber assets are absolutely devoid of cybersecurity wrappings.

Link:
https://securethegrid.com/wp-content/uploads/2021/02/GeorgeCotter-1stMotion-FERC-11Jun20.pdf

2nd MTI on Dockets Nos. EL20-46-000, RM20-12-000 and AD20-19-000

This MTI focuses on a FERC Staff paper proposing increased Tariff incentives for utilities voluntary cybersecurity investments; an absurd initiative given documented avoidance of CIP Standards. The MTI challenges FERC to show what Operational facilities are covered by CIP Standards, to identify actual cybersecurity CIP linkages to the independent Engineering Standards, and identify CIP measures to protect **Synchrophasor** networks, (Map provided). FERC did not respond, simply because they couldn't address these documented shortcomings. The MTI contains documentary evidence of a Duke Energy CIP Compliance Audit which challenges FERC to show how 127 separate CIP violations could be found with complete absence of linkages to the non-CIP Engineering Standards involved.

Link:
https://securethegrid.com/wp-content/uploads/2021/02/GeorgeCotter-2ndMotion-FERC-25Jun20.pdf

3rd MTI on Dockets Nos. EL20-46-000, RM20-12-000 and AD20-19-000

Building on a recent joint Cybersecurity Advisory titled ***"NSA and CISA Recommend Immediate Actions to Reduce Exposure Across all Operational Technologies and Control Systems"*** that focused on OT and Control Systems known to be vulnerable to malware attacks, this joint guidance issuance had the BES OT and Control Systems directly in its gunsights. This MTI contains a succinct description of the conflict FERC found itself in at the inception of CIP Standards in dealing with eight separate Reliability Regions insisting on absolute protections for regional variances from CIP Standards interference. It summarizes the convolutions NERC went through to structure CIP Standards around the Engineering Standards. The MTI contains yet another detailed study of a non-CiP Engineering Standards audit that documented avoidance of Operations and Real Time Power Flows, two no-no's in industry efforts to maintain tight control from FERC on inter-regional Grid relationships.

Link:
https://securethegrid.com/wp-content/uploads/2021/02/GeorgeCotter-3rdMotion-FERC-7Aug20.pdf

4th MTI on Dockets Nos. EL20-46-000, RM20-12-000, AD20-19-000, and RM18-20-000

This MTI deals with a number of issues, some raised in previous MTIs. It does include a detailed examination of a non-CIP compliance audit of CAISO, one of the largest Independent Systems Organizations in the US, consisting of over one hundred separate utilities. The purpose of the audit is not revealed but is believed to have been necessary due to a shift in Regional Entity responsibility back from PEAK Reliability to the WECC. IT appears to have been "pro forma", checking a box. But it does reveal what had been seen in previous assessments, little or no action on anything related to Operations or Real Time Power Flows. Also discussed is a decade-long debate between FERC and NERC over need for CIP Standards governing Control Center to Control Center communications; NERC was holding the bag on resisting, due to direct conflict with the identical issue embodied in non-CIP Engineering Standards, all in FERC Order no. 866.

Link:
https://securethegrid.com/wp-content/uploads/2021/02/GeorgeCotter-4thMotion-FERC-14Sept20.pdf

5th MTI on Dockets Nos. EL20-46-000, RM20-12-000, AD20-19-000, and RM18-20-000

This MTI reveals direct couplings between Transmission and Distribution systems in Interconnection Regions that are essential for Grid operations, modernization and reliability, but impossible to justify on CIP Standards grounds; i.e., the interconnection of "CIP-protected" BES facilities with non-CIP Distribution systems, notably **Synchrophasor** networks, without cybersecurity interface protections**. Synchrophasors** are a major engineering innovation that has completely muddled the CIP, non-CIP picture; consequently NERC and FERC religiously avoid their citation. Evidence from Dominion Energy, CAISO, So. California Edison, NEISO, Bonneville Power Association, and TVA of this conflict is presented. A "Forced Oscillation Event" is described that demonstrates the criticality of **Synchrophasors.**

Link:
https://securethegrid.com/wp-content/uploads/2021/02/GeorgeCotter-5thMotion-FERC-18Nov20.pdf

(5) Re-addressing Concerns Voiced to the Trump Administration but Not Apparently Actioned:

We also share concerns voiced to the Trump Administration after the issuance of EO13920 in response to a DOE Request for Information (RFI) which included the following recommendations:

(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 Foreign and Domestic Lobbying for "Business as Usual" Approaches to Grid Security; and

(4) Demand Trusted Personnel & Organizations to Immediately Cease Ties With Foreign Adversaries.

These four requests could help the Biden Administration strengthen EO 13920 and its implementation.

Our 2020 letter can be found at the link below:

https://securethegrid.com/wp-content/uploads/2021/02/STG-Coalition-Comments-on-DOE-RFI-24-Aug-2020.pdf