Foundation for Resilient Societies
24 Front Street, Suite 203
Exeter NH 03833
855-688-2430

August 24, 2020

Mr. Charles P. Kosak
Deputy Assistant Secretary
Transmission Permitting and Technical Assistance Division
OE-20, Office of Electricity
U.S. Department of Energy
1000 Independence Avenue, S.W.
Washington, D.C. 20585

Email: bulkpowersystemEO@hq.doe.gov

Subject: Request for Information for Bulk-Power System Executive Order

Dear Mr. Kosak:

The Foundation for Resilient Societies, Inc., a 501 (c)(3) non-profit engaged over the past eight years in research and education to strengthen the resilience of the critical infrastructures, appreciates the opportunity to respond briefly to the Request for Information in support of Executive Order 13920,

President Trump's Executive Order 13920, "Securing the United States Bulk-Power System," issued May 1, 2020, provides a broad array of opportunities to increase the protection, adaptability, and recovery of the bulk power from foreign adversaries. This Executive Order can facilitate improved supply chain procurement, supply-chain risk management, and operational countermeasures against adversaries who may seek to threaten, destroy, or leverage control of electric grid assets to impair the grid itself and other critical infrastructures.

We appreciate the work of the U.S. Department of Energy (DOE) and other organizations that assisted the President in developing this Executive Order.

The broad context for assessing and modeling electric grid resilience

Before responding to specific requests for information, we wish to provide contextual information on why the federal government and other public and private enterprises need to support a base of competing suppliers manufacturing equipment in the United States and allied nations. Such a supplier base will be important to ensure provide reliable and resilient critical infrastructures.

The National Academies Press recently published a set of Workshop Proceedings, *Models to Inform Planning for the Future of Electric Power in the United States*. Jason Fuller of Pacific Northwest Laboratories observed:

> *"It's not just the grid anymore," he said. "As power engineers, we have a tendency to think about transmission lines and power lines and transformers. … But our system is becoming something that's much more intertwined with the fabric of society. It's becoming tied into communications and other elements of the system."* [1]

Executive Order 13920 concentrates on specific types of equipment within the bulk power system, which is appropriate, especially because if this equipment is damaged, destroyed, or compromised by foreign adversaries, the risks to human life, public health, the economy, and the national security could be immense.

When a foreign adversary compromises even a few bulk power system assets, the ensuing knowledge derived from experimentation risks catastrophic attack at a time of the adversary's choosing.

How many bulk power substations are subject to Executive Order 13920; and does it matter if only a small share operate transformers supplied from manufacturers in adversary nations?

EO 13920 covers only the bulk power system, defined as including transmission systems and equipment of 69 kV and higher, and excluding equipment operating at lower voltages. How many transformers operate with a high-end voltage of 69 kV or higher? Available data for the North American Electric Reliability Corporation regions excludes Alaska and Hawaii. For U.S. jurisdictions, as of July 2020, an available database (from Oak Ridge National Laboratory via the U.S. Department of Homeland Security) indicates there were 74,923 electric substations in the U.S. portion of the database, with 53,827 of them operating at 69 kV or higher, 3,063 operating below 69kV, and 18,033 with high voltage tap data unavailable.[2]

Most substations have at least two transformers on-site. What can DOE infer from the historical record documented by the U.S. International Trade Commission that China has supplied 200 high voltage transformers to U.S. customers in the period 2008 through 2017? This is an approximate average of 20 per year. Assuming the same rate of imports of Chinese manufactured transformers imported into the U.S. electric grid for the period 2018-2020, a total of about 260 Chinese-manufactured transformers would constitute approximately one half of one percent of the total transformers now deployed in the Continental U.S. (CONUS).

Three observations are provided:

> First, if the government of China can operate a laboratory for experimentation within the U.S. bulk power system that consists of less than one percent of operating transformers, through communications and remote observation, this is still a significant hazard to the U.S. electric grid, the economy, and the national security.

[1] *Models to Inform Planning for the Future of Electric Power in the United States,* National Academies Press, 2020, pp. 41-42.

[2] *Homeland Infrastructure Foundation-Level Data (HIFLD) for Electric Substations*, U.S. Department of Homeland Security, July 8, 2020.

Second, because Executive Order 13920 takes effect at a time when only a small fraction of U.S. substations now contain Chinese-manufactured transformers, plus other grid equipment that is not currently eligible for "whitelisting," this Executive Order is timely in identifying and containing risks of foreign control of the U.S. bulk power system at a relatively early stage of evolving hazards.

Third, there is a strong rationale for the definition of "bulk-power system electric equipment" in EO 13920 because loss or compromise of this equipment can cause cascading electric grid collapse, impede electric grid restoration, and damage customer premises equipment. Moreover, much of this equipment is specific to electric grids, has long procurement lead times, and is logistically difficult to transport or install. A particularly problematic category, substation transformers, often has designs unique to a particular grid location and is constructed of electrical steel, a commodity difficult to source within the U.S. See Attachment 1 to this letter, "Bulk-Power System Electric Equipment in Executive Order 13920; Rationale for Inclusion in Order Definitions."

Recommendation that the Energy Information Administration (EIA), a sister agency within DOE, commence publishing time series on imports by year of critical grid equipment manufactured abroad.

We write in support of the Recommendations by David Jonas Bardin to the Energy Information Administrator, urging the Energy Information Administrator to utilize historic databases of the U.S. International Trade Commission to publish time series on the import trends for electric grid equipment for the U.S. bulk power system as well as the distribution grid. Better understanding of the sources of grid equipment would be helpful to improve grid supply chain risk management (SCRM).

Answers to Specific Requests for Information by DOE – July 8, 2020:

(A-3) Are non-standard incentives or changes to established standard development organizations' SCRM standards (including NIST 800 series, ISA/IEC 62443, NERC-CIP, and other Cyber Risk Maturity Model evaluations/practices) necessary to build capacity to protect source code, establish a secure software and firmware development lifecycle, and maintain software integrity? How are benchmarks documented and tracked, including:
a. The ability to provide software, firmware, and hardware "bill of materials" (*e.g.* NTIA Software Component Transparency [see *https://www.ntia.doc.gov/SoftwareTransparency*] or equivalent industry norm) and track supply chain provenance and white-labeling;
b. authentication practices that prevent tampering, unauthorized production, and counterfeits; and
c. monitoring and tracking sub-tier supplier's adherence to security requirements as part of the SCRM?

Please see the Filing of Resilient Societies on August 17, 2020, in FERC Docket AD20-19-000 which is attached as an Appendix.

In summary, the bulk-power system electric equipment covered in Executive Order 13920 is critical to the security of the U.S. electric grid. Protection of the supply chain for this equipment from compromise by foreign adversaries will be an important step forward.

Respectfully submitted by:

William R. Harris, Director Emeritus

Thomas S. Popik, Chairman and President

Attachments:

1. Matrix titled “Bulk-Power System Electric Equipment in Executive Order 13920”
2. Filing of Resilient Societies on August 17, 2020 in FERC Docket AD20-19-000

Bulk-Power System Electric Equipment in Executive Order 13920

Rationale for Inclusion in Order Definitions

Category	Loss or Compromise Risks Electric Grid Collapse	Loss or Compromise Impedes Grid Restoration	Compromise Risks Damage To Customer Premises Equipment	Equipment Is Specific To Electric Grids	Long Lead Time to Replace	Logistic or Installation Issues for Replacement	Supply of Electrical Steel Is Constrained	Unique Designs Are Common
Reactors	✓	✓	✓	✓			✓	
Capacitors	✓	✓	✓	✓				
Substation Transformers	✓	✓	✓	✓	✓	✓	✓	✓
Large Generators	✓	✓		✓	✓	✓	✓	
Backup Generators		✓						
Substation Voltage Regulators	✓	✓	✓	✓				
Shunt Capacitor Equipment	✓	✓	✓	✓				
Automatic Circuit Reclosers	✓	✓	✓	✓				
Instrument Transformers	✓	✓	✓	✓			✓	
Coupling Capacity Voltage Transformers	✓	✓	✓	✓				
Protective Relaying	✓	✓	✓	✓				
Metering Equipment	✓	✓		✓				
High Voltage Circuit Breakers	✓	✓	✓	✓	✓			
Generation Turbines	✓	✓		✓	✓	✓		
Industrial Control Systems	✓	✓	✓					
Distributed Control Systems	✓	✓	✓					
Safety Instrumented Systems	✓	✓						

Source: Foundation for Resilient Societies www.resilientsocieties.org
August 24, 2020

UNITED STATES OF AMERICA

BEFORE THE FEDERAL ENERGY REGULATORY COMMISSION

Comments on the Cybersecurity Incentives)
White Paper of the FERC Staff issued June 18, 2020) FERC Docket No. AD20-19-000

Comments of the Foundation for Resilient Societies, Inc. (submitted August 17, 2020)

The Foundation for Resilient Societies, Inc. (hereafter "Resilient Societies"), a 501(c)(3) non-profit research and education organization, commends the Federal Energy Regulatory Commission (hereafter "FERC" or "the Commission") and its Staff for the June 18, 2020 Staff White Paper proposing alternative frameworks and financial incentives to improve cybersecurity of the electric grid.[1] We provide brief comments below:

Question 1: Should the Commission consider adopting one or both of the CIP Reliability Standards and NIST Framework approaches? Describe any other possible approach in detail.

Resilient Societies supports a transition to adoption of the National Institute of Standards and Technology (NIST) Framework as the primary risk-based and mandatory framework for cyber protection of the bulk electric system. We concur in assessments of the Bureau of Reclamation ("Reclamation") filed on August 14, 2020 that the Critical Infrastructure Protection (CIP) standards utilize inconsistent definitions, and we favor adoption of the NIST Framework in place of CIP reliability standards. Our assessment is based in part on the exclusion from "high" or "medium" risk assets of many elements of the bulk power system that are vulnerable to and targeted by foreign cyber adversaries. We also ask the Commission to take notice of the multiple filings in this Docket (and others) by the former Chief Scientist of the National Security Agency, George R. Cotter. Mr. Cotter's detailed analyses demonstrate that electric power flows are generally excluded from CIP reliability standards, while they are a primary target of foreign adversaries. Due to challenges to assure compatibility of the phases, frequencies and voltages of the power grid across regions, CIP standards have excluded tools such as synchrophasors from mandatory encryption or other CIP protections. A shift to 'best practices" incentives within the NIST Framework could facilitate a broader scope for cyber protections, including the protection of cross-regional power flows and the protection of business systems that are target of cyber adversaries.

Question 2: Are the methods for granting incentives based on CIP Reliability Standards adequate?

Resilient Societies does not support financial incentives for CIP Reliability Standards compliance, because we assess the CIP standards to exclude critical assets, including so-called "Low Impact" assets

[1] See Notice of White Paper. Cybersecurity Incentives White Paper. Docket AD20-19-000, issued June 18, 2020.

that are targeted by foreign adversaries, including distribution system assets and vendor-managed software and firmware that can enable cyber adversary takeover of critical grid assets. Resilient Societies could support risk-based cyber incentives across a broader set of grid assets. We also encourage the Commission to consider the proposal of ITC and its subsidiaries, in comments of August 17, 2020, to allow capitalization of some cybersecurity investments, in lieu of a higher rate of return (so-called "adders" to allowable Commission rates) to provide alternative incentives for return on transmission system cybersecurity investments.

Question 3: Should the Commission provide a rebuttable presumption of the reasonableness and applicability of incentives for [CIP Reliability Standard] investments?

Resilient Societies does not support presumptions for rate of return adders based on CIP reliability standards that, overall, do not provide adequate protections from adversary cyber-attack capabilities. Incentives should be based on discernable performance metrics that can be empirically tested, without any presumptions that CIP standard compliance merits rate of return enhancements.

Question 4: Is the proposed approach for granting incentives based on the NIST Framework adequate?

Resilient Societies supports granting incentives based on the NIST Framework, with open ended opportunities for financial incentive if demonstrated on a case by case basis. We also support financial incentives for registered entities that voluntarily report recent cyber incidents and ongoing cyber-attacks to the U.S. government on a near-real-timed basis, for the purposes of supporting (a) cyber deterrence capabilities of the United States, and (b) prompt disruption of cyber-attacks upon electric grid assets, and (c) adoption of sanctions against cyber adversaries and their sponsors.

Question 5: Answer: Any components of the NIST framework should be eligible for cyber protection incentives if demonstrated in cases brought before FERC.

Question 6: Answer: Resilient Societies supports incentives to protect corporate systems, and distribution assets outside the bulk power system, and financial aid to state utility commissions to strengthen cyber protection of the distribution grid.

Federal legislation to aid states' cybersecurity protection, cybersecurity training, and coordination with federal cybersecurity initiative could be beneficial but is beyond the scope of FERC authorities.

Question 11: Answer: A sunset date at some future date might be appropriate to limit consumer charges for existing or future cybersecurity incentives that become obsolete.

Comments are Respectfully Submitted by:

/s/ William R. Harris

William R. Harris,
Director-Emeritus and Attorney
For the Foundation for Resilient Societies, Inc.
24 Front Street
Exeter, NH 03833
www.resilientsocieties.org