UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Equipment and Services Produced
or Provided by Certain Entities Identified as Risks to National Security — Docket No. RM20-19-000

NOTICE OF INTERVENTION AND RESPONSE OF THE ELECTRICITY CONSUMERS RESOURCE COUNCIL

On September 17, 2020, the Federal Energy Regulatory Commission (FERC or Commission) issued a Notice of Inquiry (NOI) seeking comments on the potential risks to the bulk electric system (BES) posed by using equipment and services produced or provided by entities identified as risks to national security.[1] Pursuant to 18 C.F.R. § 385.211 (2019) and 18 C.F.R. § 385.214 (2019), the Electricity Consumers Resource Council (ELCON) hereby submits comments and provides timely notice of intervention in the above-captioned proceeding.

I. STATEMENT OF INTEREST

ELCON is the national association representing large industrial consumers of electricity. ELCON member companies produce a wide range of products and services from virtually every segment of the industrial community. ELCON members own and operate hundreds of major facilities and are consumers of electricity in the footprints of all organized markets and other regions throughout the United States. Reliable electricity supply at just and reasonable rates is essential to our members' operations. ELCON has a direct interest in this proceeding both on behalf of its members and on behalf of the organization. Further, ELCON's interests are not adequately represented by any other party to this proceeding.

ELCON staff has participated in many proceedings led by the North American Electric Reliability Corporation (NERC). For example, ELCON staff was on the

[1] *Equipment and Services Produced or Provided by Certain Entities Identified as Risks to National Security*, September 17, 2020 (172 FERC ¶ 61,224).

Standards Drafting Team that was established to lead the response to FERC Order Nos. 743 and 743-A, which directed NERC to revise the definition of the BES. ELCON staff continues to be closely involved at NERC, with staff now serving on NERC's Reliability and Security Technical Committee. Additionally, some of ELCON members' major facilities are NERC registered entities and thus subject to FERC-approved mandatory reliability standards.

II. BACKGROUND

On May 1, 2020, President Trump issued Executive Order (EO) 13920, "Securing the U.S. Bulk-Power System."[2] On July 8, 2020, the Department of Energy (DOE) issued a Request for Information (RFI) regarding EO 13920 "seeking information to understand the energy industry's current practices to identify and mitigate vulnerabilities in the supply chain for components of the bulk-power system (BPS)."[3]

ELCON submitted a timely response to the RFI on August 24, 2020, and ELCON's response is appended to these comments. ELCON's RFI responses focused on the scope of EO 13920, which we viewed as problematic, and urged DOE to tailor the scope of its implementation to the existing definition of the BES. ELCON argued that restricting the reach of EO 13920 to the BES would provide much-needed regulatory certainty and better integrate implementation of the EO with existing NERC standards.

FERC noted in the NOI that EO 13920 and several other legislative and executive actions "raise concerns over the potential risks to bulk electric system reliability posed by the use of equipment and services provided by Huawei, ZTE, and other entities identified as risks to national security."[4] Those actions include the Federal Communications Commission's determination that the companies "Huawei and ZTE pose a national security threat to the integrity of communications networks and the communications supply chain due to their close ties to the Chinese government" and

[2] *See* https://www.whitehouse.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/
[3] *See* https://www.federalregister.gov/documents/2020/07/08/2020-14668/securing-the-united-states-bulk-power-system
[4] NOI at P 15.

present "profound risks to the security of affected communications networks."[5] Additionally, the Commission cited the Covered Companies defined in section 889(f)(3) of the National Defense Authorization Act for Fiscal Year 2019 and posed a series of questions regarding Covered Companies.[6]

III. RESPONSE TO THE NOI

At the outset, we note that ELCON members have every incentive to ensure the security and reliability of their own assets. ELCON members operate both non-BES and BES assets, all of which are designated to be low impact by NERC. In all cases, however, ELCON members are diligent in their efforts to mitigate the risks posed by Covered Companies and other security threats—even those risks that might emerge from sub-tier suppliers—and continuously assess their posture with respect to all sensitive equipment, whether provided by domestic suppliers, Covered Companies, or others.

Q1. To what extent is the equipment (including components) and services provided by Covered Companies used in the operation of the bulk electric system?

A1. NERC's 2020 State of Reliability Report notes that, based on responses to a 2019 NERC Alert, its analysis suggests there is "minimal exposure of the BPS through branded products from the named Chinese telecommunications and video surveillance manufacturers…."[7] ELCON agrees with NERC's analysis.

Q2. Describe the risks to bulk electric system reliability and security posed by the use of equipment and services provided by Covered Companies?

---

[5] NOI at P 12.

[6] *See* NOI at P 11. "Section 889(f)(3) of the 2019 NDAA defines 'covered telecommunications equipment or services' as: (1) telecommunications equipment produced by Huawei or ZTE or any subsidiary or affiliate of such entities; (2) video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company or any subsidiary or affiliate of such entities; (3) telecommunications or video surveillance services provided by such entities or using such equipment; or (4) telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense . . . reasonably believes to be an entity owned or controlled by, or otherwise connected to, the . . . People's Republic of China."

[7] NERC 2020 State of Reliability Report at p. 4. *See* https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_SOR_2020.pdf

A2. ELCON members fully appreciate the risks involved with the use of equipment and services provided by Covered Companies in the operation of BES assets and have taken significant steps to address those risks, even though all BES assets operated by member companies are designated by NERC to be low impact. Many ELCON members screen restricted parties and perform due diligence inquiries as part of the acquisitions process. Further, the business standard clause in typical acquisition agreements ensures suppliers comply with local laws and do not source from restricted countries. ELCON asserts that the current acquisition practices used by our members adequately address risks to the bulk electric system posed by equipment and services provided by Covered Companies. As mentioned above, ELCON members have every incentive to ensure the security and reliability of their own assets.

Q3. Discuss the effectiveness of the current CIP [Critical Infrastructure Protection] Reliability Standards in mitigating the risks posed by equipment and services provided by Covered Companies used in the operation of the bulk electric system.

A3. ELCON believes the risks to the BES are effectively addressed by the current standards and are appropriately reflected in an asset's risk designation. Particularly for low-risk BES assets, ELCON is skeptical that modifications to CIP standards such as limiting purchase options (as through a blacklist or other prohibition) would provide significant net benefits. Rather, such a limit on purchase options could raise costs substantially for industrial consumers and reduce their competitiveness with the same foreign adversaries identified in this NOI.

Q4. Describe any strategies, in addition to compliance with the CIP Reliability Standards, entities have implemented or plan to implement to mitigate the risks associated with use of equipment and services provided by Covered Companies.

A4. Some ELCON members mitigate risks posed by Covered Companies by sourcing assets exclusively from within the U.S., while others take special precautions when sourcing assets from abroad. As mentioned above, many ELCON members screen restricted parties and perform due diligence inquiries as part of the acquisitions process.

ELCON members also conduct enterprise risk assessments on a regular basis. IT systems are evaluated on a periodic basis using C2M2 and other models. Cyber security risks for industrial control systems are managed and evaluated through an operations and integrity management framework, risk assessments, and cyber measures guided by industry standards. However, ELCON believes monitoring and tracking benchmarks for every sub-tier supplier for every asset under a company's ownership is unnecessary and would be unduly burdensome.

Q5. What other methods could the Commission employ outside the CIP Reliability Standards, whether through regulatory action or through voluntary collaboration with industry and government, to further address the risks to bulk electric system reliability and security posed by the use of equipment and services provided by Covered Companies? For example, raising awareness about the risks identified in response to the previous questions, identifying potential solutions, and assisting with mitigating actions (including the facilitating information sharing)?

A5. ELCON encourages the Commission to work collaboratively on a voluntary basis with ELCON members and other industry representatives to identify and address concerns about reliability and security risks posed by Covered Companies. Collaborative, voluntary efforts have proven to be an efficient and effective way for the industry to address risks to reliability and security and to share information in a timely manner. To that end, ELCON greatly values its regular communications with Commission staff and looks forward to continuing to work collaboratively with FERC and NERC on these important issues.

Respectfully submitted,

Travis Fisher
President & CEO
Electricity Consumers Resource Council
1101 K Street NW, Suite 700

Washington, DC 20005
Email: tfisher@elcon.org
Phone: 202-682-1390

Dated: November 23, 2020

CERTIFICATE OF SERVICE

I hereby certify that I have this day caused to be served the foregoing document upon each person designated on the official service list compiled by the Secretary of this proceeding.

Dated at Washington, D.C.: November 23, 2020

Travis Fisher
President & CEO
Electricity Consumers Resource Council

Appendix: Response to DOE's RFI

August 24, 2020

Deputy Assistant Secretary Charles Kosak
U.S. Department of Energy, Office of Electricity
Transmission Permitting and Technical Assistance Division

Re: Request for Information [DOE-HQ-2020-0028]

Dear Mr. Kosak,

The Electricity Consumers Resource Council (ELCON) submits these comments in response to the Department of Energy's (DOE) request for information (RFI) [DOE-HQ-2020-0028] relating to Executive Order 13920 (Securing the United States Bulk-Power System). ELCON is the national association representing large industrial consumers of electricity. Reliable electricity supply at just and reasonable rates is essential to our members' operations.

ELCON strives to enhance the DOE's implementation of E.O. 13920, particularly on the crucial question of the scope of the Notice of Proposed Rulemaking. We feel strongly that DOE and electricity consumers would benefit if DOE were to tailor the scope of its implementation of E.O. 13920 to the existing and well-defined Bulk Electric System (BES). Restricting the reach of E.O. 13920 to the BES as defined by the North American Electric Reliability Corporation (NERC) would provide much-needed regulatory certainty and better integrate implementation of E.O. 13920 with existing NERC standards.

ELCON responds below to each question posed in the RFI. We sincerely appreciate the ability to comment on the DOE's implementation of E.O. 13920. We also thank the DOE for extending the comment period, as ELCON and other trade associations requested in a July 13, 2020 letter (appended to this submission below ELCON's RFI responses).

Thank you for considering the enclosed comments. Please contact me anytime if I can be of assistance in DOE's implementation of E.O. 13920.

Sincerely,

Travis S. Fisher
President & CEO
Electricity Consumers Resource Council
1101 K Street NW, Suite 700
Washington, DC 20005

Email: tfisher@elcon.org

Responses of the Electricity Consumers Resource Council (ELCON) to the Request for Information from the Department of Energy regarding Executive Order 13920

(A-1) Do energy sector asset owners and/or vendors conduct enterprise risk assessments, including a cyber maturity model evaluation on a periodic basis? Provide an explanation or description of an assessment program if it addresses the mitigation of risks associated with FOCI with respect to foreign adversaries (see *https://www.dcsa.mil/mc/ctp/foci/*).

Yes. ELCON members conduct enterprise risk assessments on a regular basis. IT systems are evaluated on a periodic basis using C2M2 and other models. Industrial control systems cyber security risks are managed and evaluated through an operations and integrity management framework, risk assessments, and cyber measures guided by industry standards such as ISA/IEC 62443 and NIST 800-82rev2.

In response to this question and elsewhere, ELCON asks that the DOE distinguish between assets identified as part of the Bulk Electric System (BES) and non-BES assets. For ELCON members that own and operate BES assets, all such assets comply with mandatory North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards regarding cybersecurity. Importantly, all BES assets owned by ELCON members are designated as low impact according to NERC. For non-BES assets, while the risks to the bulk power system are even lower than for low-risk BES assets, ELCON members still have a direct economic incentive – the threat of ineffective equipment, lost business, and lost revenue – to protect assets from risks, foreign and domestic, tied to hardware and software acquisitions.

ELCON urges the DOE to tailor its implementation of E.O. 13920 to focus not only on NERC registered entities listed under the present definition of the BES, but, further, on the narrow subset of the BES that is deemed to be defense-critical infrastructure.

To the extent the DOE considers it necessary to revisit or circumvent NERC designations (BES vs non-BES, high impact vs medium or low impact, etc.), ELCON asks that DOE give existing designations a high degree of deference and prioritize leveraging the appropriate channels and stakeholder processes to attempt to modify those well-defined designations. ELCON members and other stakeholders were closely involved in the definition of the BES that the Federal Energy Regulatory Commission (FERC) approved in 2014 – ELCON is concerned given the scope of E.O. 13920 that the DOE will create regulatory confusion by blurring the bright lines established by NERC and FERC in defining the BES.[8]

(A-2) Do energy sector asset owners and/or vendors identify, evaluate, and/or mitigate the following:

a. FOCI with respect to foreign adversaries with respect to access to company and utility data, product development, and source code (including research partnerships);

[8] See https://www.nerc.com/pa/RAPA/Pages/BES.aspx

Yes. Some ELCON members mitigate FOCI risks by sourcing assets exclusively from within the U.S., while others take special precautions when sourcing assets from abroad. Further, some ELCON members leverage company access controls to physically limit access to equipment. As a general rule, ELCON members have a strong and direct incentive to protect assets from risks and to continuously assess their cybersecurity posture with respect to FOCI-related threats.

b. potential supply chain risks from sub-tier suppliers, recognizing that some sub-tier supply chain manufacturers could have FOCI with respect to foreign adversaries; and

Yes. ELCON members have a direct incentive to protect assets from risks and to continuously assess their cybersecurity posture – even those risks that might emerge from sub-tier suppliers. For example, some ELCON members perform restricted party screenings and due diligence inquiries of primary contracts as part of the acquisitions process. The business standard clause in many acquisition agreements requires that suppliers and sub-suppliers do not supply from restricted countries and comply with local laws. Further, any supplier that is contracted to perform services on site is subject to background checks and audits.

c. assets and services critical risk tolerance regarding protecting these assets and services from FOCI?

Yes. As mentioned above, ELCON members have a direct incentive to protect assets from risks and to continuously assess their cybersecurity posture. That includes enterprise-wide assessments of FOCI-related risks as well as the development of company-specific risk tolerances tailored to the nature of each company's lines of business and exposure to FOCI-related risks, taking into account specific cost-benefit analysis appropriate for each company.

(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?

ELCON believes that any effort by DOE and FERC to expand transmission incentives to cybersecurity should be done in consultation with Congress. As ELCON noted in its recent comments on FERC's proposed implementation of Section 219 of the Federal Power Act (FPA), any incentives granted by FERC should follow the letter of the statute approved by Congress.[9] *With the Energy Policy Act of 2005, Congress explicitly granted FERC the authority to create incentives for transmission development pursuant to FPA Section 219. The same act of Congress created Section 215 of the FPA, which governs the creation of an Electric Reliability Organization (ERO) to develop and enforce mandatory reliability standards. Notably, Section 215 does not authorize FERC or the ERO to use incentives as part of*

[9] See https://elcon.org/comments-of-the-electricity-consumers-resource-council-elcon-american-chemistry-council-acc-and-american-forest-paper-association-afpa-docket-no-rm20-10-000-electric-transmission-incenti/

securing the reliability of the bulk power system. To be clear, cybersecurity incentives should not be promulgated as part of the DOE's implementation of E.O. 13920.

FERC acknowledged in its white paper in Docket No. AD20-19 that "additional transmission incentives are not necessary to maintain an adequate level of reliability. However, transmission incentives to counter the evolving and increasing threats to the cybersecurity of the electric grid may be warranted."[10] In our view, determining whether or not cybersecurity incentives are warranted is the role of Congress. ELCON disagrees that it is the role of FERC staff or Commissioners to mix and match statutory obligations to suit the needs of the day. If Congress had intended FERC to use incentives as part of its FPA Section 215 obligations, it would have authorized incentives in that section as it did with Section 219.

Further, incentives pancaked on top of the standards development and enforcement process for BES assets would needlessly complicate compliance and add significant administrative burdens to processes that are working well under the status quo, such as NERC CIP standards.

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;

Each ELCON member company tailors its internal processes for assessing software, firmware, and hardware purchases to the specific needs of the company and the equipment. ELCON members believe any risks to the bulk power system are effectively addressed by company standards and are also reflected in a given asset's designation as BES or non-BES. Particularly for non-BES assets, ELCON is skeptical that limiting purchase options (as through a blacklist or other prohibition) would provide net benefits given that NERC has already deemed non-BES assets to be low-risk. Such a limit on purchase options could raise costs substantially for industrial consumers and reduce their competitiveness with the very foreign adversaries identified in this request for information.

b. authentication practices that prevent tampering, unauthorized production, and counterfeits; and

Because ELCON members are asset owners and not vendors, this question does not seem to be applicable.

c. monitoring and tracking sub-tier supplier's adherence to security requirements as part of the SCRM?

For many ELCON members, screening of restricted parties and due diligence inquiries are done as part of the acquisitions process. Further, the business standard clause in acquisition agreements ensures suppliers comply with local laws and do not source from restricted countries. But again, monitoring and

[10] *Cybersecurity Incentives Policy White Paper*, June 2020, at pp 2-3. See https://elibrary.ferc.gov/idmws/common/OpenNat.asp?fileID=15561319

tracking benchmarks for every sub-tier supplier for every asset under a company's ownership seems to be unnecessary, particularly when all ELCON members' assets are deemed to be low risk by NERC and ELCON members comply with applicable NERC requirements for such BES assets. Consequently, a requirement to monitor and track every sub-tier supplier for every asset would be costly and would not provide bulk power system security benefits above or commensurate with costs.

(A-4) What information is available concerning the following: BPS electric equipment cyber vulnerability testing standards, analyses of vulnerabilities, and information on compromises of BPS electric equipment over the last five years, including results of independent BPS electric equipment testing and penetration testing of enterprise systems for vulnerabilities (including methodology for discovery and remediation)?

a. What process does the energy sector have to share information with utilities regarding vulnerabilities and vice versa? Are contingency plans in place? How is the effectiveness of vulnerability testing and mitigation efforts monitored, tracked, and audited?

The E-ISAC is one example of a successful existing program to share electricity sector information among industry members. NERC states: "The E-ISAC offers products and services that give timely, relevant, and actionable situational awareness and analysis to asset owners and operators as well as cross-sector and government partners. As the threat landscape continues to evolve, the E-ISAC fulfills its role as a trusted leader and source of security information within the electricity industry in collaboration with the Department of Energy, the Department of Homeland Security, and the Electricity Subsector Coordinating Council."[11]

b. Is a record of an analysis of component vulnerabilities and any compromises of components and systems maintained for a specific period of time (*e.g.*, five years)? If yes, are the results of independent component testing and penetration testing of enterprise systems for vulnerabilities (including timeline for discovery and remediation) also maintained?

A requirement to monitor and track every sub-tier supplier for every asset would be costly and impose significant administrative burdens without providing substantial added bulk power system security benefits. Retaining such information for an extended period of time would likewise not provide added bulk power system security benefits.

c. How are the results of independent component testing and penetration testing of enterprise systems for vulnerabilities (including timeline for discovery and remediation) maintained?

Based upon the assessed risk, ELCON members may identify vulnerabilities as a high value learning incident/event and have specific mitigating controls designated for gap closure and tracked globally.

d. How are vulnerabilities identified by external entities addressed? How is the distribution of information regarding patching security vulnerabilities in the supply chain facilitated?

[11] See https://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx

Vulnerabilities identified by external entities may not be applicable to asset owners' risk mitigation strategies at all times. These may be evaluated, analyzed, then processed with integrity considerations as required to maintain not only cybersecurity but reliability.

e. What insecure by design/vulnerable communication protocols exist today that should be retired or cannot be disabled or mitigated from BPS electric equipment (examples of protocols include Distributed Network Protocol 3 [DNP3], File Transfer Protocol [FTP], Telnet, or Modbus)?

Insecure protocols in the environment are managed using risk assessments to identify additional controls if needed and mitigate risks to acceptable levels. However, ELCON understands based on feedback from DOE that E.O. 13920 does not create a "rip and replace" regime, and we encourage any retirement of equipment to be handled on a voluntary basis.

(A-5) What governance of sub-tier vendors do energy sector asset owners and/or vendors have in place? Is contract language for Supply Chain Security included in procurement contracts? Are metrics for supply chain security, along with cost, schedule, and performance maintained? What specific guidance should be developed for Integrator/Installer/Maintenance Service provider activities?

Many ELCON member companies perform restricted party screening and due diligence inquiries as part of the acquisitions process. Furthermore, the business standard clause in supply agreements requires that suppliers and sub-suppliers comply with local laws and do not supply from restricted countries. Any supplier that is contracted to perform services on site is subject to background checks and audits as standard practice.

For non-BES assets, such guidance regarding procurement contract language, etc., should be voluntary or left to the individual company to tailor to its own needs. Non-BES assets, by definition, do not pose a risk to the reliable operation of the BES.

(A-6) Can energy sector asset owners and/or vendors document the level of engagement in information sharing and testing programs that identify threats and vulnerabilities and incorporation of indicators of compromise (*e.g.*, Information Sharing and Analysis Center, Information Sharing and Analysis Organization)? Does the energy sector participate in a community for sharing supply chain risks? Does the energy sector encourage security related information exchange with external entities, including the Federal government?

ELCON members participate in several trade associations and communities of practice such as E-ISAC, InfraGard, ONG-ISAC, NERC, ICS-CERT, API, etc. ELCON members also actively engage and participate with Federal partners, including NCCIC Threat Intel events, speaking engagements, and assistance with cyber investigations.

(A-7) What physical and logistical role-based access control policies have been developed to monitor and restrict access during installation when a foreign adversary, or associated foreign-owned, foreign-controlled, or foreign-influenced person is installing BPS electric equipment at a

BPS site in the U.S.? What policies and practices exist to ensure installers/integrators effectively protect the systems and components during installation and commissioning? What policies and practices are in place to ensure that service providers (including those providing remote monitoring and management of systems) effectively maintain the security protections of the systems and components they are monitoring? Does an insider threat program exist?

In order for suppliers to come on site, each supplier must have a background check exhibit included in its agreement. Appropriate network control points exist between the service providers and the in-scope equipment to prevent interactive remote access.

(A-8) Are there critical mineral or supply chain materials, and if so, what are they? Specify if any of these critical inputs rely on foreign sources, and the cause for that reliance, such as lack of domestic capability or quality factors. Per Executive Order 13817, the Department of Interior prepared *The Final List of Critical Materials 2018*, see: *https://www.federalregister.gov/documents/2018/05/18/2018-10667/final-list-of-critical-minerals-2018*.

ELCON recognizes that the supply of some critical materials (such as the rare earth minerals used in the U.S. electricity system) depends on foreign sources. However, ELCON does not believe top-down federal planning is a productive way to deal with critical materials issues. Rather, voluntary trade between willing partners is the appropriate response to resource shortages or quality concerns.[12] *Additionally, ELCON believes top-down initiatives by national governments to relieve scarcity rarely work as designed. Finally, ELCON believes this question is beyond the scope of E.O. 13920.*

(B-1) Within the E.O. 13920 definition of BPS electric equipment, what are the estimated one-time and recurring costs of developing, implementing, and periodically revising compliance plans and procedures associated with the Executive Order, including but not limited to:

a. Evaluating requirements.

The record does not contain enough information for ELCON to estimate compliance costs. The cost of developing plans and procedures is one consideration – ELCON members already have procedures in place to mitigate cybersecurity and other threats posed by FOCI. However, if the cost of compliance includes the higher cost of new or replacement equipment caused by the DOE's blacklisting of certain equipment or vendors, then compliance costs could reach into millions of dollars per industrial site. That would be an entirely separate and more serious consideration. As a practical matter, increased costs could render industrial facilities owned by ELCON members – such as oil refineries, auto manufacturing facilities, or chemical plants – less competitive with sites owned or influenced by foreign adversaries. In

[12] As resource economist Julian Simon wrote in his book *The Ultimate Resource 2*, "our supplies of natural resources are not finite in any economic sense. Nor does past experience give reason to expect natural resources to become any more scarce. Rather, if history is any guide, natural resources will progressively become less costly, hence less scarce, and will constitute a smaller proportion of our expenses in future years." Julian Simon, *The Ultimate Resource 2*, page 6. See: http://www.juliansimon.com/writings/Ultimate_Resource/

other words, E.O. 13920 could paradoxically improve foreign adversaries' competitiveness by increasing costs to domestic manufacturing operations.

Further, the scope of E.O. 13920 remains unclear, and ELCON insists that the DOE and electricity consumers would be best served by DOE tailoring its implementation of E.O. 13920 to the existing and well-defined BES. Restricting the reach of E.O. 13920 to the BES, as defined by NERC (with all relevant inclusions and exclusions), would eliminate the large uncertainties involved in estimating compliance costs and would better integrate implementation of E.O. 13920 with existing NERC standards.

b. Developing compliance plans and frameworks: Supply chain documentation, foreign involvement evaluations, risk assessments, and process reviews.

Feedback submitted by ELCON members indicates that the cost of developing compliance plans is not the driving concern in this proceeding. However, if ELCON members are asked to develop detailed compliance plans for all assets that fall under the wide purview of E.O. 13920, especially for assets that are presently defined as non-BES, many of those plans would represent unanticipated costs with little to no benefit to the security of the electric grid. ELCON members are most directly concerned with running their main lines of business, which are industrial processes that require large amounts of electricity. ELCON members comply with NERC requirements in order to get electrical and thermal energy into their manufacturing processes efficiently and cost-effectively. Additional compliance costs imposed on ELCON members would encumber our main lines of business.

c. Implementing plans: New supplier processes and contractual provisions; and supplier audits.

Without knowing whether or not ELCON members' existing supply chains will be affected by E.O. 13920, or to what degree, it is impossible to accurately estimate the cost of implementation. But to reiterate our central concern, if low-cost suppliers of non-BES equipment (which, by definition, has already been deemed to be low risk) are blacklisted or otherwise prohibited under the implementation of E.O. 13920, ELCON members would face large cost increases with no commensurate benefit to overall grid security.

d. Supporting transaction reviews: Records retention and responding to information inquiries.

ELCON members do not believe that record-keeping by itself will pose an immediate or high cost to industrial consumers of electricity. ELCON's main focus is that the scope of E.O. 13920 be limited to those facilities that have already been deemed to have some direct nexus to grid security, which are the facilities that are registered with NERC and included in the definition of the BES. Tailoring the scope of the E.O. appropriately will help mitigate unintended consequences related to the costs and burdens of E.O. 13920.

e. Negotiating agreements to mitigate concerns raised in connection with transactions.

Renegotiating agreements that have already been finalized would be costly for ELCON members. Putting in place new terms for new agreements may be less costly, depending on the terms. As stated elsewhere in this response, ELCON members believe it is imperative that the DOE narrow the incredibly broad

applicability of E.O. 13920 and tailor its implementation to focus not only on NERC registered entities but, further, on the subset of the BES that is deemed to be defense-critical infrastructure. In other words, certainly not all industrial facilities rated at or above 69kV are defense-critical.

f. Other compliance costs.

Again, if the cost of compliance includes the higher cost of new or replacement equipment that will be prohibited by DOE going forward, then compliance costs could reach into millions of dollars per industrial site. ELCON members reiterate that such costs would have the perverse effect of rendering domestically owned industrial facilities – such as oil refineries, auto manufacturing facilities, or chemical plants – less competitive with sites owned or influenced by foreign adversaries.

We encourage the Administration to adapt the scope of E.O. 13920 to ensure it does not create precisely the type of regulatory burden and regulatory uncertainty that prior executive orders by the Administration have attempted to reduce. For example, Section 1 of Executive Order 13771, "Reducing Regulation and Controlling Regulatory Costs," January 30, 2017, reads:

> It is the policy of the executive branch to be prudent and financially responsible in the expenditure of funds, from both public and private sources. In addition to the management of the direct expenditure of taxpayer dollars through the budgeting process, **it is essential to manage the costs associated with the governmental imposition of private expenditures required to comply with Federal regulations.** Toward that end, it is important that for every one new regulation issued, at least two prior regulations be identified for elimination, and that the cost of planned regulations be prudently managed and controlled through a budgeting process.[13] (emphasis added)

Section 1 of Executive Order 13777, "Enforcing the Regulatory Reform Agenda," February 24, 2017, reads:

> *Policy.* It is the policy of the United States to alleviate unnecessary regulatory burdens placed on the American people.[14]

ELCON urges the DOE to follow the policy laid out the above executive orders, particularly the guidance in E.O. 13771 that emphasizes the need "to manage the costs associated with the governmental imposition of private expenditures required to comply with Federal regulations." One simple way to do that with respect to E.O. 13920 is to sharpen DOE's implementation to focus on NERC registered entities and, further, on the narrow subset of the BES that is deemed to be defense-critical infrastructure.

As ELCON stated in our comments sent to the comment collection email address (bulkpowersystemEO@hq.doe.gov), ELCON members are highly sensitive to regulatory compliance costs as well as delays in ongoing work such as repairs and replacements of existing equipment, upgrades of

[13] See https://www.govinfo.gov/content/pkg/FR-2017-02-03/pdf/2017-02451.pdf
[14] See https://www.govinfo.gov/content/pkg/FR-2017-03-01/pdf/2017-04107.pdf

existing equipment, and new facilities that are being designed or already under construction. E.O. 13920 represents a potentially large regulatory burden and imposes massive regulatory uncertainty on ELCON members and the electricity industry generally. ELCON believes that, to the extent E.O. 13920 ultimately applies to non-BES equipment and burdens American manufacturing with increased regulatory uncertainty and increased compliance costs, it would be inconsistent with E.O. 13771 and E.O. 13777 as discussed above. Further, E.O. 13920 makes no attempt to identify two prior regulations for elimination, as E.O. 13771 requires.

(B-2) Within the E.O. 13920 definition of BPS electric equipment, are there categories of BPS electric equipment that are more reliant on vendors likely to become the subject of transaction reviews, and if so, what are they? What are the sourcing challenges and cost impacts for companies facing prohibited transactions for those BPS electric equipment categories?

Without knowing which transactions will be prohibited, we have no way of answering questions about the costs of any forthcoming prohibitions. In the event a supplier has to change its sourcing and manufacturing strategy to be compliant with the E.O. 13920, there would likely be cost and schedule impacts to ELCON members' projects. Further, in certain instances replacement equipment may not be available.

(B-3) Does the energy sector have a procedure to identify services, components, and/or systems which are or should be covered by E.O. 13920? If yes, list the services, components, and systems and provide the reasoning regarding why they should or should not be covered by E.O. 13920.

Yes. There already exists a framework for determining which facilities might pose a risk to grid security – the existing definition of the BES and its specific inclusions and exclusions. The scope of E.O. 13920 would likely be addressed by the NERC CIP Standards.

(B-4) What unique challenges could E.O. 13920 present to small businesses?

The challenges of E.O. 13920 are similar to other instances of red tape and regulatory uncertainty that ELCON members face every day. Typically, smaller companies struggle (relative to multinational corporations) to satisfy legal requirements or stay informed of developments in federal policy. However, no matter the size of the company, E.O. 13920 creates regulatory burdens that run contrary to prior executive orders by the Administration and pose substantial risks to ELCON members' international competitiveness.

ELCON members are left with many of the same questions we asked in our prior comments, which the DOE treated as premature because the NOPR was not yet finalized. We ask again that the DOE consider our questions as it drafts the NOPR. To reiterate, those questions were:

1) *How is DOE coordinating with NERC and FERC?*
2) *How will DOE protect CEII?*
3) *Has the DOE limited the scope of the EO to the BES, as defined by NERC?*
4) *Has the DOE limited the scope of the EO further to the defense-critical subset of the BES?*
5) *Will the DOE undertake its own estimate of the cost of compliance with the EO?*

6) *Will the DOE commit in the NOPR that it will not "rip and replace" any existing equipment?*
7) *Will industrial equipment such as cogeneration facilities – which contribute no or de minimis quantities of power – be excluded from compliance with the EO?*

Document Content(s)