

CHAMBER OF COMMERCE
OF THE
UNITED STATES OF AMERICA

June 7, 2021

Mr. Michael Coe
Director
Energy Resilience Division
Office of Electricity
U.S. Department of Energy
Mailstop OE-20, Room 8H-033
1000 Independence Avenue, SW
Washington, DC 20585

RE: RFI on Ensuring the Continued Security of the United States Critical Electric Infrastructure

Dear Director Coe:

The U.S. Chamber of Commerce (“the Chamber”) appreciates the opportunity to submit these comments in response to the Request for Information (“RFI”) issued on April 20, 2021, by the Office of Electricity, Department of Energy (“DOE”).¹ The RFI, entitled “Ensuring the Continued Security of the United States Critical Electric Infrastructure,” was issued to seek stakeholder input to inform the next steps from DOE and the Administration as they consider the potential issuance of a new executive order to replace Executive Order 13920, “Executive Order on Securing the United States Bulk-Power System” (the “BPS EO”), which was issued by the prior administration on May 1, 2020.²

Consistent with the Chamber’s previous comments on and communications with DOE regarding bulk electric system supply chain security, these comments leverage the broad knowledge base and real-world experiences of the Chamber’s working group representing the majority of the primary participants in the electric sector supply chain for the United States bulk electric system (the “Supply Chain Working Group”). Through its interactions with other stakeholder groups, DOE, and the broader Administration, the Supply Chain Working Group intends for its efforts to supplement the contributions of electric utility interests providing feedback *via* the Electricity Subsector Coordinating Council. The working group also aims to ensure that DOE has a robust understanding of the indispensable stakeholders and associated interests that are directly impacted by, and will be required to achieve compliance with, any forthcoming directives

¹ Notice of Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure, 86 Fed. Reg. 21,309 (April 22, 2021).

² 85 Fed. Reg. 26,595 (May 4, 2020).

or orders relevant to the bulk electric system supply chain. The comments below reflect the extensive collaboration and agreement of these bulk electric system supply chain participants, while simultaneously attempting not to oppose or otherwise be adverse to the views held by the other key stakeholders to the bulk electric system.

I. Background

The enhanced, high-level governmental focus on the bulk electric system supply chain reached new heights with the May 1, 2020, issuance of the prior administration’s “Executive Order on Securing the United States Bulk-Power System” or the BPS EO. The BPS EO declared a national emergency with respect to the potential for foreign entities to infiltrate and threaten the operations of the United States power grid and effectively halted the installation of bulk power system equipment “designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary.” The BPS EO was promoted as an effort to protect against infiltration and operational threats to the U.S. power grid emanating from “foreign adversaries.” However, the lack of advance stakeholder engagement and ambiguous scope of that order fomented industry uncertainty that served to halt or delay the nationwide installation, operations, and maintenance of a wide variety of critical bulk electric system equipment. This was during a time of multi-faceted challenges, including the continued provision of reliable and affordable electric service during a pandemic and the economic and regulatory uncertainty resulting therefrom.

On July 8, 2020, DOE’s Office of Electricity issued a “Request for Information,” which sought mostly technical information related to the electric utility industry’s current practices to identify and mitigate perceived supply chain vulnerabilities.³ The Chamber, leveraging the engagement of its Supply Chain Working Group, submitted a comprehensive response to the 2020 RFI on August 24, 2020.⁴ Rather than make the recommended BPS EO amendments to reflect this and other stakeholder feedback, DOE moved forward with the issuance of its “Prohibition Order Securing Critical Defense Facilities,” on December 17, 2020.⁵ The Prohibition Order, along with the quickly identified ambiguities and inconsistencies therein, further exacerbated the predictable commercial and regulatory confusion generated by the BPS EO. The combination of the BPS EO and the Prohibition Order put all electric sector supply chain manufacturers and their customers in the untenable position of attempting to abide by regulations that were, in many instances, impossible to accommodate.

Given the unsustainable nature of the situation, the Chamber welcomed President Biden’s Executive Order 13990, “Executive Order on Protecting Public Health and the Environment and Restoring Science to Tackle the Climate Crisis,” which specifically suspended the BPS EO and, pursuant to subsequent guidance from DOE, the Prohibition Order.⁶ While contemporaneous DOE guidance did not eliminate all ambiguity with respect to the applicability of the Prohibition Order to bulk electric system component transactions, the Suspension EO provided encouragement that a more measured approach to bulk electric system supply chain security would emerge from DOE’s reassessment of its supply chain activities. Moreover, the current Administration’s goals

³ Securing the United States Bulk-Power System, 85 Fed. Reg. 41,023 (July 8, 2020) (the “2020 RFI”).

⁴ https://www.uschamber.com/sites/default/files/uscc_comments_on_doe_bps_eo_rfi.pdf.

⁵ 86 Fed. Reg. 533 (January 6, 2021) (the “Prohibition Order”).

⁶ 86 Fed. Reg. 7,037 (January 25, 2021) (the “Suspension EO”).

to decarbonize the power sector and dramatically expand the electric transmission grid to support an unprecedented influx of renewable generation resources will necessarily place significant demand pressures on what had become, pursuant to the BPS EO and the Prohibition Order, an artificially-constrained supply chain. Further, many of the above activities occurred in the wake of the October 2020 commencement of mandatory compliance obligations associated with NERC CIP-013, which was developed and implemented to specifically strengthen the security of electric sector supply chain generation and transmission systems.

On April 20, 2021, DOE announced its 100 day plan among DOE, the electricity industry, and the Cybersecurity and Infrastructure Security Agency (“CISA”) to enhance the cybersecurity of electric utility industrial control systems and secure the electric sector supply chain.⁷ In another welcome move, DOE separately issued an order revoking its previously issued Prohibition Order.⁸ Contemporaneously, DOE issued the RFI to which these comments now respond.

II. The Chamber and its Members Support the Shared Goal of a Secure Bulk Electric System Supply Chain

From the outset, it is important to emphasize that the Chamber and its Supply Chain Working Group strongly support the goal of securing our nation’s bulk electric system from all threats – physical and cyber – including those emanating from private actors or nation-states. We believe that this shared goal is best met by clearly aligning the scope, requirements, and effective date of any future DOE rulemaking activities with substantial preexisting and robust industry-led standards, including NERC CIP-013. To the extent that additional risks are identified that are not captured by existing standards in systems operating below 100 kV, these vulnerabilities should be carefully studied with an eye towards whether the relevant distribution facilities also require inclusion in either future standards-setting processes or rulemaking procedures.

Unclear mandates and orders drafted without sufficient stakeholder engagement and buy-in will reprise the confusion and uncertainty resulting from the BPS EO and Prohibition Order. Companies across the entire electric sector manufacturing supply chain, along with other equipment users (*e.g.*, the oil and natural gas industry, large industrial users, critical manufacturing, information communications and technology sector, etc.), will be unsure of how to proceed with needed infrastructure projects. Collaboration among government, the electric utility sector, and the relevant supply chain manufacturers should be a primary focus of DOE activities moving forward. The BPS EO contained a broad, undefined scope, with unclear application to individual bulk electric system components and a wide-ranging lack of clarity with respect to its ultimate implementation details. The Chamber asks that this past experience be a “lesson-learned” as DOE considers its next actions in this space.

The entirety of the Chamber’s membership recognizes the critical national security importance of a domestic bulk electric system that is secure and resilient from sabotage, manipulation, or exploitation by nation-states or other bad actors. As such, the Chamber shares the goals of DOE and the Administration to ensure grid security. Moreover, the Supply Chain

⁷ <https://www.energy.gov/articles/biden-administration-takes-bold-action-protect-electricity-operations-increasing-cyber-0>.

⁸ Revocation of Prohibition Order Securing Critical Defense Facilities, 86 Fed. Reg. 21,308 (April 22, 2021).

Working Group fully supports the full implementation of NERC CIP-013, *Cyber Security - Supply Chain Risk Management*, which squarely targets the security of the bulk electric system supply chain. The Chamber can support additional, industry-accepted best practices designed to harden the supply chain, including its upstream and downstream segments. These measures will ensure that products comply with heightened expectations of security concomitant to the critical nature of the nation's bulk electric system and the many other critical sectors reliant upon it. The working group also supports the concurrent best-practices development efforts by the North American Transmission Forum ("NATF"), which is likewise focused on protecting the cybersecurity of components and equipment that are manufactured for and integrated into the nation's bulk electric system. It is essential that these preexisting programs and efforts be leveraged, rather than overwritten, as DOE evaluates its available options for further action affecting the electric sector supply chain.

The Chamber and its Supply Chain Working Group continue to strongly support the work of the Department of Homeland Security ("DHS") Information and Communications Technology ("ICT") Supply Chain Risk Management ("SCRM") Task Force and believes that task force is a valuable instrument in collaborating on the analysis and development of operational and policy recommendations for the ICT Supply Chain. The Chamber continues to ask that DOE establish a task force similar to the SCRM Task Force to represent and collaborate with the electric sector supply chain and other bulk electric system stakeholders, including entities responsible for oil, natural gas, and related ICT infrastructure. For reference, members of the ICT SCRM include 40 major information technology and communications companies, along with 20 federal agencies. The ICT SCRM Task Force's four working groups relate to: (1) information sharing, (2) threat assessments, (3) qualified bidders and qualified manufacturing lists, and (4) counterfeit products. The ICT SCRM Task Force offers a useful multi-stakeholder model for coordinated industry and government supply chain risk management work – a model that could prove quite useful as DOE formulates its future supply chain focused activities.

The Chamber and its Supply Chain Working Group are committed to working with DOE as this process moves forward. As seen recently with the ransomware attack on the Colonial Pipeline, energy infrastructure is critical to the functioning of our society and serves as the foundation for our economy. Heightened security standards – similar to those in place today across the electric sector – are warranted to ensure that this vital infrastructure operates reliably and is resilient to disturbances, whether natural, man-made, or otherwise. Nevertheless, DOE should weigh any future rules or regulations against a risk-based, cost/benefit screen. This would ensure that any such actions are of reasonable scope and application, and would protect critical bulk electric system operations. In addition, this approach would avoid an overly broad scope or outsized impact on electric customer rates. Moreover, DOE's efforts should seek to minimize or eliminate stranded asset costs associated with otherwise unclear gains in grid security.

III. Supply Chain Working Group Response to the RFI

The Chamber appreciates the issuance of the RFI and concurrent acknowledgement by DOE that additional stakeholder engagement is necessary to develop fully the suite of options and opportunities available to DOE and the Administration as they look to bolster the security of the bulk electric system. As the BPS EO and Prohibition Order demonstrated, rushed regulations developed without sufficient stakeholder engagement can be both counterproductive to electric

grid security objectives while also undermining this Administration’s clean energy – and associated transmission grid expansion – goals. Thoughtfully developed and clearly delineated rules, containing defined and achievable obligations, can instead support a stronger bulk electric system supply chain while advancing the modernization and decarbonization of our energy system.

A. Development of a Long-Term Strategy

DOE should focus on the development of a durable supply chain strategy that primarily leverages beneficial, preexisting supply chain risk management and security practices with select enhancements that merit the support of the applicable bulk electric system stakeholders. Most importantly, future regulatory actions in this space should be risk-based, with the encouragement of threat awareness and risk mitigation programs specifically tailored to guard against the associated risks they are designed to counter. Broad prohibition orders applicable to specific product lines or countries of origin can be counterproductive, as security risks may take many different forms and can originate from diverse geographic locations. Likewise, the adherence of an electric supply chain manufacturer to certain controls, guidelines, and protections should alleviate the concerns attendant to supply chains sourcing from countries with otherwise questionable labor and/or cybersecurity practices.

Moreover, any additional standards and/or regulations applicable to the electric utility sector and the associated supply chain should be national and uniform in nature. Certain states are experimenting with the development of their own cyber rules and initiatives, but piecemeal and inconsistent regulation of superregional electric grids would unavoidably be counterproductive. Electrons do not stop at state lines, and thus state-by-state cybersecurity or supply chain standards would have little practical benefit while simultaneously imposing an inconsistent regulatory structure that would be impossible for utilities or manufacturers to manage. Electric sector manufacturers operating on a global scale cannot reasonably be expected to tailor domestically-bound products to fifty different sets of state-level standards. In addition, such a diversity of requirements would divert finite resources from the development and production of the most secure components possible – forced to focus instead on variable standards rather than a proactive, broad-based, internal supply chain risk management program. States and local government entities can play a productive role by ensuring that investor-owned utilities have ratemaking and tariff structures in place that provide incentives for cybersecurity and software upgrade investments, however. Therefore, any future DOE actions should clarify (at a minimum with respect to all facilities subject to federal jurisdiction), that nationally-applicable standards, requirements, and guidelines supersede any state entreaties to regulate within the electric sector supply chain space.

A performance-based approach to cybersecurity and supply chain regulation, which leverages existing standards and best practices, remains the most effective mechanism to ensuring the security of the bulk electric system. In addition to specific, preexisting sector-specific efforts, such as NERC CIP-013, technical standards and reports (*e.g.*, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27402 (in development), ISO 17800, ISA/IEC 62443, NIST SP 800-53, NIST SP 800-161, NIST SP 800-82, NIST SP 800-193, NISTIR 8259A), controls, and certifications (*e.g.*, the Department of Defense Cybersecurity Maturity Model Certification), and cross-sectoral efforts such as those being led by the NATF, DOE could encourage the adoption of supply chain best practices by bulk electric sector suppliers, thereby facilitating a belt-and-suspenders approach to supply chain security.

The Chamber is a proponent of the NATF’s goal of “a streamlined, effective, and efficient industry-accepted approach for entities to assess supplier cyber security practices [that], if applied widely, will reduce the burden on suppliers so their efforts with purchasers can be prioritized and entities can be provided with more information effectively and efficiently.”⁹ DOE could facilitate responsible and effective procurement practices by taking a similar position to NATF’s, albeit with more direct authority: by facilitating one or more working groups between utilities and vendors in a particular industry space, taking specific information security topics relevant to supply chain security (e.g. background checks of vendor employees, proactive and reactive vulnerability disclosure, incident response, etc.). DOE can also work with vendors and utilities to produce a small set of DOE/FERC/NERC endorsed guidance or methods that have been developed and mutually agreed upon by the working group. Such efforts could achieve responsible and effective supply chain risk management for the bulk electric grid.

The Supply Chain Working Group also supports the build-out of the capabilities of DOE’s CyTRICS (Cyber Testing for Resilient Industrial Control Systems) program. Select members of the Chamber’s working group have indeed volunteered to partner with DOE on this effort. The prequalification of critical bulk electric system equipment and software, using 3rd party testing tools and DOE testing programs such as CyTRICS, and expedited review capabilities can all be employed to mitigate the potential risks facing sensitive bulk electric system equipment. However, the sheer magnitude of the products, components, software, and firmware integrated into the bulk electric system, combined with the finite evaluation capacity of the CyTRICS program, require that overarching best practices also be available to empower suppliers to self-verify product security. This is where documents such as the recently-released “Supply Chain Best Practices” developed by the National Electrical Manufacturers Association (NEMA) can be quite informative.¹⁰

Consistent with NEMA’s guidelines, electric sector supply chain manufacturers and their respective products could be cleared for purchase and use within the bulk electric system. These individual suppliers must follow certain common-sense but robust practices that are implemented during and throughout product development, production, and deployment. Such risk-based practices would be designed to minimize the potential for viruses, bugs, malware, or other anomalies to be exploited by adversaries to negatively impact an individual product’s operation and/or its interaction with other electric grid equipment. The four key phases of internal controls, which could form the foundation for external acceptance of the covered electric grid components, could be comprised as follows:

- 1) **A holistic analysis of the manufacturing and design process** to detect and eliminate any anomalies (malware, maliciously tainted, counterfeit, etc.) in the embedded components of a product’s supply chain. This would include monitoring and certification of upstream supplier practices, a documentable, repeatable, and measurable formal design process, renewed evaluations of new component versions, the inclusion of code signing (when technically feasible),

⁹ <https://www.natf.net/industry-initiatives/supply-chain-industry-coordination>.

¹⁰ NEMA Guideline Document CPSP 1-2021, available at: <https://www.nema.org/standards/view/supply-chain-best-practices>.

and the enforcement of a documented purchasing process that gives preference to original component manufacturers and their authorized suppliers.

- 2) **Tamper-proofing of products** to ensure that their manufactured configuration has not been altered between the production line and the ultimate operating environment. These efforts could include the use of tamper-resistant microprocessors, controls that protect software against reverse engineering or modification, hardening of the security of data storage devices, the implementation of secure channels of communications – and disabling of non-secure channels – linked to such products, and the utilization of tamper-resistant coatings and seals.
- 3) **Tools that facilitate an asset owner's ability to comply** with security requirements and the other demands of their regulated environment with respect to the manufactured device. These tools could include internal configuration management practices, asset management technologies, quality assurance audits, a thorough understanding and consideration of the risk environment in which the product will operate, product testing regimes inclusive of penetration testing, and comprehensive incident management plans.
- 4) **An active decommissioning and revocation process** that is designed to prevent obsolete or comprised devices from being leveraged to access or disrupt otherwise secure networks. These efforts could include the protection or disposal of legacy data, the physical destruction of outdated/vulnerable equipment, and the complete removal of any and all communications pathways such devices previously used to interact with a linked industrial control network.

The above procedures and internal structures, along with other more individualized processes that hold stakeholder support, could form a strong foundation for a non-punitive program. This program would recognize the merits and benefits of procuring bulk electric system components from a manufacturer that has implemented specific yet flexible guidelines and controls to harden the security of their products and their devices' respective componentry, software, and firmware. While compelling the reshoring of supply chain manufacturing capacity to the United States may be viewed by some as a simple solution to reduce supply chain vulnerabilities, it is important to recognize that such actions would potentially violate World Trade Organization commitments. Regardless, it would still likely lead to retaliatory steps against U.S. products by other nations, while also imposing added cost and disruption upon the significant domestic manufacturing base of bulk electric system equipment and software. Thus, efforts to compel the movement and reconfiguration of critical bulk electric system supply chains should be avoided.

B. Prohibition Authority

At the outset, DOE should not limit its options to the development and issuance of a new prohibition order applicable to the bulk electric system supply chain. Instead, DOE should develop an objective and transparent framework that continuously monitors and assesses bulk electric

system threats while, when necessary, issuing appropriate and actionable mitigation procedures. While this effort could include the future issuance of a prohibition order, it could instead model the operational directives now issued by CISA consistent with its statutory authorities.

The Prohibition Order issued in December 2020 by DOE, under the auspices of the authority provided by the BPS EO, should provide some “lessons learned” on a regulatory path to avoid moving forward. This Prohibition Order appeared to be issued in a vacuum, without consideration of the comprehensive stakeholder input provided to DOE through formal comments and as otherwise submitted to the agency in the wake of the BPS EO and the 2020 RFI. Basic internal inconsistencies and misconceptions regarding the commercial viability of certain directives and sought certifications undercut the workability of that order and fostered greater uncertainty and distrust between utility customers and supply chain manufacturers. Transparency was not the Prohibition Order’s hallmark, and efforts to facilitate transparency should be emphasized as DOE contemplates and develops its next steps.

Relying on a single approach to security, such as one based on the national origin of equipment or components in the supply chain, can result in a false sense of security and corresponding single point of failure. While the Supply Chain Working Group does not take a position on whether a successive prohibition order is the optimal mechanism to address bulk electric system supply chain vulnerabilities, the Supply Chain Working Group strongly believes that a risk-based approach is preferable to bright-line exclusions, such as those centered on a national-origin-based approach, which can be exploited and/or avoided by our adversaries. However, the working group does suggest certain guiding factors that should be considered by DOE in the development and/or implementation of any new prohibition order. Factors DOE should consider include, but are not limited to, the following:

- 1) **A Targeted Approach, Following Normal Rulemaking Order.** Any future prohibition order should be more surgical in its guidance. Any order should be developed as part of a transparent process, with clear reasoning, and ideally issued as a Notice of Proposed Rulemaking to allow for further industry comment. Care should be taken to not issue an order with unclear origins, justifications, or mandates, as such shortfalls would undermine its credibility and viability.
- 2) **A Risk-Based Approach.** The contemporaneous adherence to a risk-based approach targeting actual security risk, rather than less impactful ancillary factors, should also be a foundational component of any new prohibition order. The Prohibition Order focused on a discrete set of bulk electric grid facilities, which was beneficial for targeting the scope of components impacted. However, that order also flagged grid components solely on the basis of their country of origin, rather than on any more qualitative measurement of risk or potential vulnerability. A risk-based approach should focus on many factors, with consideration for the offsetting impacts of thorough internal supply chain controls that are implemented by the relevant electric grid component manufacturers.

- 3) **Adherence to Common Industry-Accepted Terms.** The December Prohibition Order mixed standard industry terminology with other terms of ambiguous meaning, such as “programmable components,” “digital components,” “associated control and protection systems,” and “persons owned by, controlled by, or subject to the jurisdiction of.” Any future prohibition order should adopt NERC-recognized and other industry-standardized terms in order to improve the clarity of such prohibition order and protect impacted stakeholders from having to make determinations that go beyond what is under their control or expertise. In addition, accompanying guidance documentation should also be issued so that all impacted stakeholders may implement the rules under the order in a consistent and appropriate manner and may interact with one another with a common understanding of such rules.
- 4) **Applicable Only to Finished Products.** Covered products should be limited to finished products and not sub-assemblies. Instead, DOE should rely on suppliers to secure supply chains for sub-assemblies (*e.g.* through testing to ensure no tampering; code quality and cyber penetration checks; and re-writing/loading software outside of countries of concern). In addition, any prohibition order should provide an exemption for open-source software and for information technology equipment and software with significant uses outside the bulk electric system. Appropriate forms of exemption should also be considered for software developed and compiled by multinational companies that are not under the control of countries of concern but whose global teams collaborating on the development of software may include some collaborators physically located in countries of concern.
- 5) **Any Prohibition Order Should Default to Mitigation, Rather than Replacement.** The bulk electric system is comprised of countless devices, components, and systems of firmware and software that have been installed and recovered in electric customer rates over a span of decades. While vulnerabilities may exist in some of this installed utility plant, mitigation can often provide a more rapid and cost-effective reduction of the associated risk. As such, mitigation strategies should be evaluated and exhausted before any “rip-and-replace” mandate is implemented. DOE could consider developing a mitigation/cure roadmap for existing hardware and software that may otherwise be subject to a future prohibition order.
- 6) **A Reasonable Compliance Timeframe.** Any prohibition order should recognize the complexity and scope of the bulk electric sector supply chain. Thus, advance guidance and ample opportunity to comply with any new directives or mandates should be afforded to supply chain stakeholders and regulated utilities before any prohibition order affecting particular devices, geographic installations, countries of origin, or other subset of bulk electric system components is deemed effective. A phased-in implementation of at least two (2) years will allow supply chains for bulk electric system equipment to be moved, as necessary, and impacted utilities should be directed to not prematurely enforce any prohibition order’s mandates.

With respect to the scope of any potential new prohibition order, the Chamber cautions against tiered levels of criticality. The initial Prohibition Order’s applicability to Defense Critical Electric Infrastructure (DCEI) was satisfactorily defined and logical, given the importance of the identified facilities and their associated electric grid infrastructure to national security. However, practical implementation of that order demonstrated that utilities do not prefer to run two separate supply chains. Instead, the DCEI supply chain security specifications became *de facto* standards for the entire bulk electric system.

The expansion of a future prohibition order to other critical infrastructure sectors should be evaluated on a cost/benefit basis. Will the exponential expansion of the application of such a prohibition order to other critical sectors outweigh the associated costs? In the case of a forward-looking application, the integration of prudent risk-based controls within supply chain manufacturers’ design and build processes could be cost-effective as compared to the adverse impacts that could result from a prolonged power interruption. However, if a new prohibition order were to also require extensive mitigation and device replacement directives, the case for an expanded scope will likely favor a limitation that the prohibition order apply to the most critical subsectors of critical infrastructure. The utilization of NERC “bright-line criteria” would enable utilities and vendors to sufficiently identify the critical infrastructures within their service territories that are serviced by such impacted equipment.

Likewise, the expansion of a prohibition order’s scope to “National Critical Functions,” as defined in Executive Order 13865 “Coordinating National Resilience to Electromagnetic Pulses,”¹¹ would require a similar balancing of costs versus benefits. The adoption by manufacturers of reasonable and practicable risk-based internal controls to minimize the opportunity for newly installed devices, software, or firmware to serve as a conduit to perpetrate physical or cyber-attacks may be cost-effective on a broad basis. However, the imposition of elevated controls or blanket prohibitions against products of certain geographic origin or with particular sensitive functions, with such bans applying both prospectively and retroactively, would likely see the costs and associated customer rate impacts outweigh the benefits of a super-hardened electric grid to serve those National Critical Functions.

The preceding explanations can be condensed into the essential request that DOE undertake significant stakeholder engagement before the issuance of any new prohibition order. Only through comprehensive and open-minded discussions with all impacted bulk electric system stakeholders, inclusive of electric utilities, relevant municipal and cooperative utility providers, electric sector supply chain manufacturers, and any other entities that may be required to substantially alter their practices, procedures, and/or equipment to achieve compliance with any such prohibition order, can the true costs and benefits of any particular proposal be thoroughly evaluated and measured in light of the associated impact on national security, other critical infrastructure sectors, and/or National Critical Functions.

¹¹ 84 Fed. Reg. 12,041 (March 29, 2019).

IV. Principles for Sustainable Policies to Secure Bulk Electric System Supply Chains

In the immediate aftermath of the prior administration’s issuance of the BPS EO, the Chamber gathered together an informal group representing the majority of the primary participants in the electric sector supply chain for the United States bulk electric system. This group, the Supply Chain Working Group, met numerous times and exchanged ideas virtually to ultimately develop a comprehensive “Principles” document to assist DOE in its ultimate implementation of the BPS EO. This Principles document is included as Attachment A to this RFI response.

While these Principles were developed by the Chamber and its Supply Chain Working Group to support the electric sector supply chain’s response to the BPS EO, the majority of the included 22 Principles remain equally applicable as DOE sets forth on a new path to evaluate and strengthen the security of the bulk electric system supply chain. The attached Principles seek to expand upon the DOE’s understanding of the potential impacts of supply-chain focused regulatory activities beyond merely the owners and operators of the bulk electric system. Given that the companies that comprise the Supply Chain Working Group, and others, will be relied upon to defend, revise, and/or otherwise restructure their associated manufacturing and supply chains to support electric utility compliance with any rules or regulations forthcoming from DOE, it is imperative that the views and realities facing electric sector component manufacturers are fully considered by DOE *before* the agency moves forward with additional actions in this area.

The DOE’s consideration and integration of these attached Principles will not only reflect that the electric sector supply chain has been heard by DOE, but it will also ensure that any final rule sets forth a workable framework that is enduring and consistent with existing regulatory and other programs. Any such rule will also be mindful of the unnecessary costs and adverse security impacts that could result from a final rule that conflicts with the electric sector supply chain’s strong commitment to the security of the United States bulk electric system.

V. Conclusion

The Chamber and its Supply Chain Working Group support DOE’s effort to reevaluate and enhance the security of the bulk electric system and the internal controls, design, and manufacturing processes of the entities that supply the grid’s critical products and components. The bulk electric system is critical to our national security and our everyday lives. Concomitantly, the grid’s security, reliability, and resilience is essential to preserving our way of life. While many of the core components that comprise the electric grid have not significantly changed in their design or function for decades, the threat matrix facing the bulk electric system and other critical infrastructure sectors has significantly increased in frequency and complexity. As such, the hardening of the electric grid from all threats – both physical and cyber – is more important than ever.

The growing cyber hazards facing the bulk electric system and its associated information technology and operational technology platforms justify the enhanced public/private collaboration addressing threat indicators and supply chain controls. NERC CIP-013 is one of many powerful tools in this space. Therefore, it is extremely important that DOE, as it considers further actions impacting the bulk electric system supply chain, first leans into the existing programs, procedures,

and controls that are aimed at the same security concerns targeted by the May 1, 2020 BPS EO. Only after DOE undertakes a comprehensive inventory of existing bulk electric system protections can DOE effectively and efficiently fill-in any perceived gaps.

The Chamber sincerely appreciates the opportunity to comment on the RFI. If you have any questions or need additional information, please contact Heath Nakmuhs, Vice President and Policy Counsel, Global Energy Institute, at hnakmuhs@uschamber.com, or Vince Voci, Director, Policy, Cyber, Intelligence, and Security Division, at vvoci@uschamber.com.

Sincerely,



Marty Durbin
President
Global Energy Institute



Christopher Roberti
Senior Vice President
Cyber, Intelligence, and
Supply Chain Security Policy

Attachment A

Principles for Engagement of the Electric Sector Supply Chain on the Bulk-Power System Executive Order

In order to support the DOE's development of the any rules, orders, or regulations applicable to the bulk electric system supply chain, and to assist the DOE's understanding of the potential impacts of Executive Order 13920, "Executive Order on Securing the United States Bulk-Power System" (the "Grid Order"), beyond the directly-regulated owners and operators of the bulk electric system, an informal group representing the majority of the primary participants in the electric sector supply chain for the United States bulk electric system has developed the following "Principles" to assist the DOE in its future activities aimed at hardening the supply chain for bulk electric system equipment.

WHEREAS, the electric sector manufacturing supply chain (the "Supply Chain") recognizes the critical national security importance of a domestic bulk power system that is secure and resilient from sabotage by nation-states and/or other bad actors;

WHEREAS, the Supply Chain fully supports the full implementation of NERC CIP-13 and concurrent efforts of the North American Transmission Forum that each focus on protecting the cybersecurity of the components and equipment that are manufactured for and integrated into the bulk power system;

WHEREAS, the Chamber supports the work of the DHS Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force and believes it is a valuable instrument in collaborating on analysis and developing operational and policy recommendations for the ICT Supply Chain through the collaborative efforts of its membership;

WHEREAS, DOE should establish a task force similar to the SCRM Task Force to represent and collaborate with the Supply Chain and other bulk power system stakeholders (e.g., oil, natural gas, and related infrastructure). For reference, members of the SCRM include 40 major information technology (IT) and communications companies, along with 20 federal agencies. The SCRM task force's four working groups relate to: (1) information sharing, (2) threat assessments, (3) qualified bidders and qualified manufacturing lists, and (4) counterfeit products. The SCRM Task Force offers a useful multi-stakeholder model for coordinated industry and government supply chain risk management work; and

WHEREAS, the Supply Chain is committed to working with DOE on Rules of reasonable scope and application, which would serve to protect critical bulk power system operations while avoiding an overly broad scope or unduly impacting electric customer rates and seeking to minimize stranded asset costs associated with unclear gains in grid security.

The Supply Chain Principles (subject to addition) are as follows:

1. During the Rules development process, DOE should consult with and implement the feedback of all impacted sectors within the bulk power system ecosystem, including electric

utilities, independent generation providers, transmission companies, affected grid customers, and the Supply Chain (collectively, “Impacted Entities”).

2. Immediate guidance should be issued by DOE to clarify the interim responsibilities and legal obligations of all Impacted Entities with respect to potentially covered bulk power system equipment that was under contract or pending contract as of May 1, 2020, whether such contract is for the acquisition, importation, transfer, or installation of such equipment. Parties to these contracts fear penalty and seek clarifying guidance on their immediate responsibilities and legal obligations prior to the issuance of final Rules. Such guidance should clarify the effective date of the Grid Order and which transactions may continue, without penalty for non-compliance, until the Rules are finalized.
3. Prior to the publication of Rules, all impacted entities should be entitled the opportunity to review, comment on and provide suggestions for the improvement of draft Rules for a period of at least sixty (60) days, with sufficient time thereafter for DOE to integrate such feedback into the Rules.
4. The Rules should be focused exclusively on maintaining the security and resilience of the domestic bulk power system and/or critical facilities therein; the U.S. power grid is stronger and more advanced because of its access to international markets and the global supply chain, which contributes to the reliability and security of that grid. Further, the Rules should be appropriately and explicitly limited to bulk power system electric equipment and not expanded to include functions outside the scope of the Grid Order. For example, industrial controls systems, distributed control systems, and safety instrumented systems serve numerous functions outside of bulk power systems. The Rules should underscore that nothing in the Grid Order shall be construed by another federal agency to promulgate additional regulations or standards relating to such equipment. If clearly defined proper safeguards and mitigation measures are in place, technologies should be exempted from the Rules. In addition, the DOE should identify clear mitigation measures and standards that allow technologies to be exempt.
5. Prior to the finalization of Rules, the DOE should perform an analysis to ensure that: (1) Such Rules provide a clear understanding of applicability to Impacted Entities (*e.g.*, an MOU between those parties); and (2) Requirements of the Grid Order neither overlap nor are inconsistent with existing regulations already in place for the Impacted Entities.
6. The Rules on bulk power systems electrical equipment should, to the maximum extent practical, integrate and rely upon preexisting sector-specific efforts, technical standards (*e.g.*, ISO/IEC 27001, ISO 17800, ISA 62443, NIST SP 800-161, NIST SP 800-82, NISTIR 8259A), controls, and certifications (*e.g.*, the Department of Defense Cybersecurity Maturity Model Certification). These and other preexisting activities should be leveraged to ensure the most efficient compliance with the Rules and to prevent unintended conflicts between the Rules and such efforts, technical standards, controls, and certifications. The Office of Management and Budget should use its existing authorities to streamline the supply chain regulatory framework and create reciprocity between federal programs.

7. To the maximum extent possible, the Rules should clearly set forth their geographic application (*e.g.* if the Rules are aimed at Defense Critical Electric Infrastructure (DCEI), or some larger or smaller subset of the domestic bulk power system, the Rules should unequivocally so state).
8. To the maximum extent possible, the Rules should clearly identify criteria that need to be met, as well as the specific products and components within their purview, while also specifying the products and components which will not be subject to DOE's Grid Order oversight. This identification need not identify products from particular suppliers, but rather should list well-defined categories of products utilized within the bulk power system.
9. The Rules should more specifically define "foreign adversary" and how DOE interprets "persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary." To provide additional clarity, we suggest that DOE refer to existing lists for export trade compliance. Many Supply Chain entities have global networks, many with headquarters in countries that have robust trade and defense agreements with the U.S.
10. The Rules should clearly identify the depth of DOE's analysis of individual grid components (*e.g.* does a non-critical imported microchip within a complex power component otherwise domestically manufactured and assembled potentially render the entire component non-conforming?), and how DOE will address current global transformation laws and country of origin calculations.
11. The Rules should establish a carve out or simplified process for Commercial Off-the-Shelf (COTS) components and other generic systems that are not purpose built for the bulk power industry.
12. The Rules should explore a framework for how DOE and industry can more effectively share actionable supply chain risk information. While DOE, and other government agencies, routinely share cyber threat information (*e.g.*, signatures and indicators of compromise), this information is structured and formatted whereas information on vendor- or product-based risk (*e.g.*, the insertion of malicious code and/or other forms of compromise or exploitation) is not widely available to the Supply Chain. For example, the Electricity Information Sharing and Analysis Center (E-ISAC) membership does not include equipment manufacturers. The Rules should seek to answer the following questions: (1) What supply chain information would be most valuable for the government and industry to mitigate the risk of sabotage? (2) Does such information exist in a public or private body or sharing platform that allows it to be accessible across the supply chain for risk management purposes? (3) How will DOE share targeted intelligence and involve relevant suppliers in the assessment of risks to specific products? (4) What legal or policy barriers to bi-directional information sharing exist, including from substantial countervailing risks of IP loss and inadvertent dissemination of security vulnerabilities?
13. The prequalification program should be set forth with specificity, and to the maximum extent practical, integrate and rely upon preexisting sector-specific efforts, technical standards, controls, and certifications, while avoiding sole reliance on government funded laboratories in accordance with [OMB Circular No. A-119](#) (Federal Participation in the

Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities). Considering the risk, it may be appropriate in limited circumstances for the prequalification program to be managed by a national laboratory. How will this program operate, how will it be funded, and how will it combat the potential for lengthy delays in issuing accreditations for bulk power system components? Also, to what extent will the prequalification program involve physical testing of products or on-site assessments of vendor supply chains?

14. The Rules should clearly articulate how DOE will assess and incorporate into its decision-making the potential market impacts, including an economic impact or cost-benefit analysis, of its prohibition or prequalification of certain products or components, including the potential for supply disruptions, decreased competition, and increasing prices associated with diminished production capacity, and declining international competitiveness of U.S. manufactured products.
15. DOE should establish an appeal process for those Supply Chain entities whose bulk power system electric equipment is prohibited, as determined by the Secretary of Energy. At a minimum the Rules should provide an appeal process for those notified of an adverse decision to provide an impacted entity the opportunity to respond and mitigate that decision.
16. The Rules that address installed equipment should consider the replacement costs or monitoring and risk mitigation investments related to installed equipment.
17. The Supply Chain should be made financially whole with respect to impacted bulk power system components and equipment ordered, manufactured, contracted (or governed by contracts) before May 1, 2020, or installed, through targeted Congressional appropriation or otherwise, provided that the Supply Chain shall use good faith to mitigate any costs reasonably avoidable pursuant to DOE interim implementation guidance, consistent with existing contractual commitments.
18. The recommendation for the isolation and monitoring of identified equipment should be set forth with specificity and shall be based on objective facts with evidence of a national security threat, be technology-neutral, risk-based, and consider defense in depth strategies. Industry-leading solutions that are commercially available that might be appropriate for risk management use include passive vulnerability scanning, continuous diagnostics and mitigation, and intrusion detection systems. Deployment of these technologies is specific to the environment into which they are deployed, the threats which are to be managed, and the layers of security deployed by the enterprise. Determining appropriate risk management controls, technical standards, and technology is a shared responsibility between the government, utilities, the Supply Chain, and managed service providers.
19. The Rules should encourage, to the maximum extent possible, the broadest stakeholder participation in ongoing risk management activities and supply chain risk information sharing, while mitigating the substantial countervailing risks of IP loss and inadvertent dissemination of security vulnerabilities. Similar to DOE's ongoing collaboration with the Electricity Subsector Coordinating Council, DOE should consider establishing a critical

infrastructure subsector coordinating council to collaborate with the bulk power system Supply Chain.

20. In considering the membership and charter of the Task Force created under the Grid Order, DOE should consider: (1) adding to the list of members of the Task Force the critical manufacturing subsector coordinating council or other industry body representing the Supply Chain; and (2) ensuring the Task Force coordinates with the Federal Acquisition Security Council (FASC) to ensure consistency and reduce the potential for duplication and/or conflict related to preexisting Federal government supply chain security policy and decisions.
21. DOE should define penalties for non-compliance and should establish a safe harbor provision such that companies that can demonstrate sound systems to determine the country of origin of the items they import should be afforded a presumption of innocence should a non-qualifying item evade such controls, resulting in a mitigation of whatever penalty might apply.
22. After implementation, DOE should undertake periodic, formal review of the effectiveness of the Rules in achieving the policy objectives of the Grid Order while maintaining an efficient, competitive market for bulk power system equipment. This review should provide Impacted Entities with the opportunity to provide suggestions for the improvement of the Rules.