CHAMBER OF COMMERCE
OF THE
UNITED STATES OF AMERICA

August 24, 2020

Mr. Charles Kosak
Deputy Assistant Secretary
Transmission Permitting and Technical Assistance Division
Office of Electricity
Department of Energy
Mailstop OE-20, Room 8G-024
1000 Independence Avenue, SW
Washington, DC 20585

RE: Bulk Power System EO RFI (DOE-HQ-2020-0028)

Dear Deputy Assistant Secretary Kosak:

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 July 8, 2020, by the Office of Electricity, Department of Energy ("DOE").[1] The RFI, entitled "Securing the United States Bulk-Power System," was issued to seek information related to the energy industry's current practices to identify and mitigate perceived vulnerabilities in the supply chain for bulk-power system components. DOE is soliciting comments pursuant to the RFI in order to inform its efforts to implement the directives set forth in Executive Order 13920 (the "BPS EO"), issued on May 1, 2020.[2]

In order to assist DOE with its development of a notice of proposed rulemaking or other implementing guidance responsive to the BPS EO, the Chamber immediately convened an informal working group representing the majority of the primary participants in the electric sector supply chain for the United States bulk power system (the "Supply Chain Working Group"). 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, or otherwise, to ensure that DOE has a robust understanding of the full breadth of stakeholders and associated interests that are impacted by, and will be required to achieve compliance with, the BPS EO. The comments below reflect the extensive collaboration and agreement of these bulk power system supply chain participants.

[1] Securing the United States Bulk-Power System, 85 Fed. Reg. 41,023 (July 8, 2020).
[2] Executive Order on Securing the United States Bulk-Power System, 85 Fed. Reg. 26,595 (May 4, 2020).

I. Background

On May 1, 2020, the President issued the "Executive Order on Securing the United States Bulk-Power System" or the BPS EO. The BPS EO declares a state of emergency with respect to the potential for foreign entities to infiltrate and threaten the operations of the United States power grid and essentially halts 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 has been promoted as an effort to protect against infiltration and operational threats to the U.S. power grid by "foreign adversaries," yet the undefined scope of the order could halt or delay the nationwide installation, operations, and maintenance of a wide variety of critical bulk power system equipment during a time of multi-faceted challenges. The electric power sector is challenged with the continued provision of reliable and affordable electric service, economic challenges (including regulatory uncertainty), and challenges regarding the uncertainty of ongoing trade disputes. Moreover, the industry is already working toward near-term compliance with NERC CIP-13, which specifically targets the security of the electric sector supply chain generation and transmission systems.

The implementation of the BPS EO and these pre-existing grid security obligations could either supplement or contradict the shared goal of a bulk electric power system that is secure and resilient from foreign or otherwise adverse influence or intrusion – during peacetime, periods of conflict, or otherwise. For example, we note that NERC CIP-13 establishes security targets for Bulk Electric Systems (BES) performing transmission or generation functions at 100kV or higher. The BPS EO introduces some potential ambiguity, by both introducing a new term "Bulk-Power Systems," which on the one hand includes systems as low as 69 kV, but then explicitly excludes electricity distribution systems.

The Chamber strongly supports the goal of achieving improved security for our nation's bulk-power systems, and believes this shared goal is best met by clearly aligning the scope, requirements, and effective date of any future DOE rulemaking under the BPS EO to preexisting and robust industry-led standards, including NERC CIP-13. To the extent that additional risks are identified that are not captured by these 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.

Affected companies – within the electric utility sector, across the entire electric sector manufacturing supply chain, and other equipment users (*e.g.*, the oil and natural gas industry, large industrial users, critical manufacturing, information communications and technology sector, etc.) – are now unsure of how to proceed with infrastructure projects – and the associated design, manufacture, and commissioning of necessary bulk power system components – given that the BPS EO was deemed immediately effective on May 1, 2020. Meanwhile, the codification of guidelines, rules, or regulations implementing the BPS EO are not due to be finalized by DOE until September 2020, or later. The significant uncertainty borne by stakeholders is due to the broad scope of the BPS EO, the unclear application of the BPS EO to individual bulk power system

components, and the wide-ranging lack of clarity with respect to the ultimate implementation details of the BPS EO.

II. The Electric Sector Supply Chain Shares the Goal of a Cyber-Secure Bulk Power System

From the outset, it is important to emphasize that the Chamber and its Supply Chain Working Group strongly recognize the critical national security importance of a domestic bulk power system that is secure and resilient from sabotage, manipulation, or exploitation by nation-states and/or other bad actors. As such, the Chamber's working group shares the goals of DOE and the BPS EO to ensure grid security. Moreover, the Supply Chain Working Group fully supports the full implementation of NERC CIP-13, *Cyber Security - Supply Chain Risk Management*, which squarely targets the security of the bulk power system supply chain. The working group also supports the concurrent efforts of the North American Transmission Forum, which is likewise focused on protecting the cybersecurity of components and equipment that are manufactured for and integrated into the nation's bulk power system. These preexisting programs and efforts should be leveraged, rather than overwritten, as the DOE develops its NOPR implementing the BPS EO.

The Chamber and its Supply Chain Working Group also 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 it is a valuable instrument in collaborating on the analysis and development of operational and policy recommendations for the ICT Supply Chain through the collaborative efforts of that group's membership. The Chamber would 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 power 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 the DOE formulates the implementation of the BPS EO.

The Chamber and its Supply Chain Working Group are committed to working with DOE to develop a NOPR and subsequent final rule 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. Moreover, DOE's efforts should seek to minimize or eliminate stranded asset costs associated with otherwise unclear gains in grid security.

III. Principles for the Sustainable Implementation of the BPS EO[3]

In order to respond to the RFI and to support the DOE's development of a NOPR and final rule, the Chamber and its Supply Chain Working Group collaborated to develop a set of "Principles" to support the electric sector supply chain's response to the BPS EO. These Principles seek to expand upon the DOE's understanding of the potential impacts of the BPS EO and its implementation beyond merely the owners and operators of the bulk power 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 the BPS EO, it is imperative that the views and realities facing electric sector component manufacturers are fully considered by DOE as it moves forward with the implementation of the BPS EO.

The Chamber's Supply Chain Working Group's Principles are as follows:

1. During the NOPR and final rule 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 electric sector supply chain (collectively, "Impacted Entities").

2. Without additional undue delay, DOE should issue guidance 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 a NOPR or final rule. Such guidance should clarify the legal effective date of the BPS EO and should identify the types of transactions that may continue, without penalty for non-compliance, until the DOE finalizes its implementation rule.

3. Prior to the publication of a final rule, all Impacted Entities should be entitled the opportunity to review, comment on, and provide suggestions for the improvement of a publicly-issued NOPR for a period of at least sixty (60) days, with sufficient time thereafter for DOE to integrate such feedback into its final rule.

4. In any rulemaking pursuant to the BPS EO, DOE should explicitly clarify that the BPS EO and resulting rule are intended to align with the NERC CIP definition of "Bulk Electric Systems" transmission and generation systems above 100 kV. Such alignment should pertain to the scope, requirements, and effective dates of any such rulemaking. Therefore, consistent with the BPS EO, DOE should clearly exclude electricity

[3] These comments assume, consistent with the Administrative Procedure Act, that DOE will next proceed with the issuance of a Notice of Proposed Rulemaking, or NOPR, which will thereafter be subject to public comment, in order to solicit feedback on its proposed implementation of the BPS EO. In the event that DOE takes a different path toward the finalization of rules implementing the BPS EO, these comments apply equally to any such alternative pathway to facilitate industry compliance with the directives within the BPS EO, including any final rule resulting therefrom.

distribution systems from the scope of its forthcoming rule, pending further study. The BPS EO demonstrates a clear intent to avoid the inclusion of distribution systems in its definition of "Bulk-Power Systems."[4] To the extent there are non-distribution systems in the range between the threshold of 69 kV referenced in the BPS EO and the 100 kV referenced in NERC CIP-013-1, the question of whether and how to address security risks should be further studied with an eye towards whether existing standards should be expanded to address them – or whether a parallel standard should be developed by NERC to address cybersecurity and supply chain risk management for such systems. Moreover, to alleviate unnecessary confusion between efforts to comply with NERC standards and any future rules developed pursuant to the BPS EO, DOE should make every effort to align both the requirements and the timing of any rules it promulgates with both the contents and the effective date of related NERC standards.

5. The DOE final rule 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 final rule should be appropriately and explicitly limited to bulk power system electric equipment and not expanded to include functions outside the scope of the BPS EO. For example, industrial controls systems, distributed control systems, and safety instrumented systems serve numerous functions outside of bulk power systems. DOE's final rule should underscore that nothing in the BPS EO 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 scope of the final rule. In addition, the DOE should identify clear mitigation measures and standards that allow technologies to be exempt from the final rule.

6. Prior to the finalization of a final rule, the DOE should perform an analysis to ensure that: (1) The rule provides a clear understanding of applicability to Impacted Entities (*e.g.*, an MOU between those parties); and (2) Requirements of the BPS EO neither overlap nor are inconsistent with existing or pending regulations already in place for the bulk power system and Impacted Entities.

7. DOE's final rule, as applied to bulk power system electrical equipment should, to the maximum extent practical, integrate and rely upon preexisting sector-specific efforts (*e.g.* NERC CIP-13), 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

[4] The BPS EO only references "bulk-power system" in contrast with the term "Bulk Electrical System" used by NERC. The BPS EO defines "bulk-power system" to mean "(i) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and (ii) electric energy from generation facilities needed to maintain transmission reliability. For the purpose of this order, this definition includes transmission lines rated at 69,000 volts (69 kV) or more, but does not include facilities used in the local distribution of electric energy." DOE can resolve this apparent ambiguity by clearly stating that the EO intended to exclude all distribution systems, including those in the range of 69-100 kV.

Certification). As noted above, DOE should parallel the scope of its rule to the greatest extent possible to that of NERC CIP-13. NERC CIP provides clear standards and compliance documentation to ensure the security and reliable operation of the Bulk Electric System. These standards explicitly spell out the functional entities, applicable systems and requirements, as well as the appropriate measures to satisfy standards. BPS utilities and entities understand how to comply with NERC CIP and NERC/FERC understand how to audit. These and other preexisting activities should be leveraged to ensure that the final rule supports an efficient compliance architecture and prevents unintended conflicts between that final rule and already applicable efforts, technical standards, controls, and certifications. In the development of the final rule, the Office of Management and Budget should utilize its existing authorities to streamline the supply chain regulatory framework and create reciprocity between applicable federal programs.

8. To the maximum extent possible, the final rule implementing the BPS EO should clearly set forth its geographic application. In other words, if the final rule is focused at Defense Critical Electric Infrastructure (DCEI), or some larger or smaller subset of the domestic bulk power system, the rule should unequivocally so state.

9. To the maximum extent possible, the final rule 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 the final rule implementing the BPS EO. The DOE's specification and identification need not identify products from particular suppliers, but rather should list well-defined categories of products utilized within the bulk power system.

10. The final rule should more specifically define "foreign adversary" in a more predictable manner than the contemporaneous listing of such nation-states provided within the RFI. In addition, the final rule should specifically identify 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 electric sector supply chain manufacturers have global networks, and many have headquarters in countries that have robust trade and defense agreements with the United States.

11. The final rule should clearly delineate the depth of DOE's analysis of individual grid equipment. For example, would a non-critical imported microchip within a complex power product otherwise domestically manufactured and assembled potentially render the entire product non-conforming with such final rule? In addition, the final rule should identify how DOE will address current global transformation laws and country of origin calculations.

12. The final rule should establish a carve out or simplified clearance process for Commercial Off-the-Shelf (COTS) components, products and other generic systems that are not purpose built for the bulk power industry. In addition, the final rule should exempt COTS components and products that don't include any programmable logic.

For example, if the only reasonable source for screws or power bricks utilized in networking gear boxes is from a "foreign adversary", such items without any programmable elements should still be available for use in COTS components and products. Otherwise, the final rule's application to COTS components, products and their makeup could serve to severely constrict the supply chain without any appreciable benefit to bulk power system security.

13. The final rule should establish a framework for DOE and industry to 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, such as the insertion of malicious code and/or other forms of compromise or exploitation, is not widely available to the electric sector supply chain. Specifically, the Electricity Information Sharing and Analysis Center (E-ISAC) membership does not include equipment manufacturers. The final rule should answer the following questions:

    a. What supply chain information would be most valuable for the government and industry to mitigate the risk of sabotage, manipulation, or exploitation?
    b. 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?
    c. How will DOE share targeted intelligence and involve relevant suppliers in the assessment of risks to specific products? Enhanced government participation in such an information-sharing program would be mutually beneficial.
    d. 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? The Chamber suggests using existing ISAC's which have matured methods for bi-directional sharing. These have proven to be effective at secure, multi-directional threat intelligence processing and dissemination.

14. The final rule should set forth with specificity the BPS EO pillar two prequalification program 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, however, it may be appropriate in limited circumstances for the prequalification program to be managed by a national laboratory. The final rule should detail the operation of the prequalification program, how it will be funded, and how it will provide for the timely issuance of accreditations for bulk power system equipment. In addition, the final rule should identify the extent to which the prequalification program will involve physical testing of products or on-site assessments of vendor supply chains. The final rule should consider the establishment of a safe harbor for equipment that has been approved as part of the prequalification program.

15. To further mitigate unintended ambiguity, DOE's final rule should provide an expedited mechanism whereby parties to negotiated contracts may seek pre-clearance from DOE before proceeding with a transaction that does not include pre-qualified vendors or equipment. Parties using this mechanism would provide advance notification of the intent to proceed with a transaction. The parties to the deal should be able to rely on a heightened burden of proof should DOE elect to oppose the deal or elements of the deal after receiving advance notice and allowing the pre-clearance notice window to lapse without raising objections.

16. The final rule should clearly articulate how DOE will assess and incorporate into its decision-making the potential market impacts stemming from the implementation of the BPS EO, including an economic impact or cost-benefit analysis of its prohibition or prequalification of certain products or components. In its development of a final rule, the DOE should also take into account the potential for supply disruptions, decreased competition, and increasing prices associated with diminished production capacity, as well as the potential impairment of international competitiveness for domestically manufactured products.

17. The final rule should establish an appeal process for any supply chain entities whose bulk power system electric equipment is prohibited, as determined by the Secretary of Energy under the authority of the BPS EO. At a minimum, DOE should provide an appeal process for those notified of an adverse decision to provide an Impacted Entity the opportunity to respond and potentially mitigate that adverse decision.

18. The final rule's implementation of BPS EO pillar three, regarding the identification, isolation, monitoring, or replacement of installed bulk power system equipment, should consider the replacement costs or monitoring and risk mitigation investments related to installed equipment. Rules regarding the isolation of equipment should be narrowly focused and used only in the highest risk cases. The concern here is that isolation permanently reduces efficiencies in financial and environmental cases and may be at counter purposes with years of progress.

19. Concurrent with the its finalization of the rules implementing the BPS EO, DOE should seek, through targeted Congressional appropriation or otherwise, the resources to make Impacted Entities whole with respect to impacted bulk power system components and equipment ordered, manufactured, contracted (or governed by contracts), or installed before May 1, 2020. However, such financial indemnification is rightly subject to such Impacted Entity's use of good faith to mitigate any costs reasonably avoidable consistent with any forthcoming interim implementation guidance from DOE, consistent with existing contractual commitments.

20. Under BPS EO pillar three, any 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 and 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. The final rule should recognize that the determination of appropriate risk management controls, technical standards, and associated technology is a shared responsibility between the government, electric utilities, electric sector supply chain entities, and managed service providers.

21. Within its final rule, the DOE 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 intellectual property loss and the inadvertent dissemination of security vulnerabilities. Similar to DOE's ongoing collaboration with the Electricity Subsector Coordinating Council, the DOE should consider establishing a critical infrastructure subsector coordinating council to collaborate with the bulk power system supply chain.

22. In considering the membership and charter of the Task Force created under pillar four of the BPS EO, DOE should consider: (1) adding to the list of members of the Task Force the critical manufacturing subsector coordinating council or another industry body representing electric sector supply chain entities; 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.

23. The final rule should clearly set forth the 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. In such instances, a mitigated level of whatever penalty might otherwise apply should be available.

24. Following the issuance of the final rule implementing the BPS EO, and on a periodic basis thereafter, DOE should undertake regular, formal reviews of the effectiveness of the final rule in achieving the policy objectives of the BPS EO while maintaining an efficient, competitive market for bulk power system equipment. This formal review should provide Impacted Entities with the opportunity to provide suggestions for the improvement of the DOE's BPS EO implementing regulations.

The DOE's consideration and integration of the above Principles into its formulation of a NOPR – and ultimate finalization of regulations responsive to the BPS EO – will not only reflect that the electric sector supply chain has been heard by DOE, but it will also ensure that the final rule sets forth a workable framework that is enduring and consistent with existing regulatory and other programs, while being mindful of the unnecessary costs and adverse security impacts that could result from a final rule that conflicts with – rather than builds upon – the electric sector supply chain's strong commitment to the security of the United States bulk power system.

IV. The Economic Impacts of a DOE Final Rule are Currently Incalculable, But Likely Significant

The second half of the RFI solicits feedback from stakeholders on the potential one-time and recurring costs associated with the development, implementation, and periodic revision of compliance plans responsive to the DOE's implementation of the BPS EO. While the Chamber and its Supply Chain Working Group appreciate and welcome this inquiry, far too little is known about the ultimate breadth and scope of the BPS EO's ultimate intention, implementation, and application to the bulk power system.

Quite simply, no reasonable approximation of costs can be deduced from what is currently known about the BPS EO. Though it is ostensibly focused on the bulk power system, it remains unclear as to whether the BPS EO might also apply to equipment similar or identical to bulk power system products that are instead installed in locations and within facilities not owned or controlled by the owners and operators of the bulk power system. Similarly, too little is known regarding the potential depth of DOE's analysis into bulk power system componentry and its underlying hardware or software. Will non-critical componentry of minimal or no security risk nevertheless be subject to a blanket ban based solely upon its country of origin? The answer to this question and others will have a significant impact on the compliance costs associated with the BPS EO. Therefore, in order to avoid unintended and unnecessary costs that do not yield measurable security benefits, DOE should avoid misalignment of any rule it promulgates under the BPS EO with existing cybersecurity or supply chain risk management efforts.

While the RFI's economic inquiry is primarily limited to the administrative and contracting costs associated with compliance activities resulting from the BPS EO, this constricted inquiry fails to capture the very significant potential costs of BPS EO implementation. For example, many supply chain manufacturers have invested considerable time, resources, and money in the establishment of notionally secure supply chains subject to extensive controls, oversight and audit. While this preexisting enterprise architecture might ultimately support security levels consistent with those sought by the BPS EO, they could be at risk of falling short, on paper, with the requirements set forth in DOE's final rule.

Moreover, the cost of the bulk power system equipment subject to potential regulation under the BPS EO is significant – both individually and collectively. Multi-million dollar transformers are commonplace throughout the bulk power system. If even one type of transformer from one electric sector supplier is deemed unacceptable, the isolation and/or replacement costs associated with such a determination would be extraordinary. Thus, the DOE's economic analysis must also consider the very real potential costs on industry (both utilities and the supply chain) as well as on all electric consumers, if the DOE's final rule leads to a widespread "rip and replace" regime that seeks to reconstitute a significant portion of the domestic bulk power system.[5]

[5] Along the same lines, the Office of Management and Budget's consideration of whether this DOE rulemaking is considered "significant" for the purposes of its obligation to review the same should also consider the significant potential costs (both administrative and otherwise) resulting from the actual application of DOE's proposed implementing regulations on the owners, users, and operators of the bulk power system and the significant sunk investments therein.

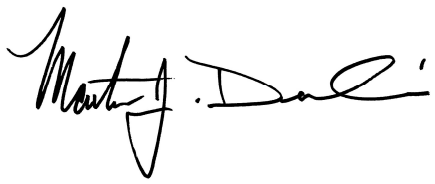
V. Conclusion

The Chamber and its Supply Chain Working Group support the initiative of the BPS EO to evaluate and improve the security of the bulk power system and the controls and processes of the entities that manufacture and supply its critical products and components. The bulk power system is critical to our national security and our everyday lives; thus, its security is essential to maintaining 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 power system and its owners and operators has significantly increased in frequency and complexity. As such, the cybersecurity of the electric grid and its equipment is more important than ever.

The increasing cyber challenges facing the bulk power system are why the associated industries and government have enhanced their collaboration with respect to threat indicators and supply chain controls – with some such controls merely in their infancy, such as NERC CIP-13. Therefore, it is extremely important that DOE, in its development of a NOPR and final rule, lean into the existing programs, procedures, and controls that are aimed at the same security concerns targeted by the BPS EO. Only through a comprehensive inventory of existing bulk power system protections can the DOE effectively and efficiently implement its obligations under the BPS EO.

The Chamber appreciates the opportunity to comment on the RFI. If you have any questions or need additional information, please contact Heath Knakmuhs, Vice President and Policy Counsel, Global Energy Institute, at hknakmuhs@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