

CHAMBER OF COMMERCE
OF THE
UNITED STATES OF AMERICA

November 23, 2020

Ms. Kimberly Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, NE
Washington, D.C. 20426

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

Dear Secretary Bose:

The U.S. Chamber of Commerce (“the Chamber”) appreciates the opportunity to submit these comments in response to the Notice of Inquiry (“NOI”) issued on September 17, 2020, by the Federal Energy Regulatory Commission (“FERC” or “Commission”).¹ The NOI, entitled “Equipment and Services Produced or Provided by Certain Entities Identified as Risks to National Security,” was issued by FERC to seek comments on the potential risks to the bulk electric system posed by the power sector’s use of equipment and services produced or provided by entities identified as risks to national security. FERC has chosen to solicit comments from industry on this topic in the wake of, among other things, Presidential Executive Order 13920, issued on May 1, 2020.²

In the immediate wake of the issuance of the Bulk-Power System Executive Order (the “BPS EO”), and in order to provide comprehensive feedback and guidance with respect to its implementation, 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 electric 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 with respect to perceived electric sector supply chain vulnerabilities – and the rectification thereof – *via* the Electricity Subsector Coordinating Council, the Edison Electric Institute, or otherwise. As a subgroup of the Chamber, however, the Supply Chain Working Group has also welcomed input from members operating in other industry sectors, such as those within the oil and gas industry. The Supply Chain Working Group seeks to ensure that the Department of Energy (“DOE”), and now FERC, have a robust understanding of the full breadth of stakeholders and associated interests

¹ 172 FERC ¶ 61,224 (2020).

² Presidential Executive Order No. 13920, Securing the United States Bulk-Power System, 85 Fed. Reg. 26,595 (May 4, 2020) (the “BPS EO”).

that are impacted by, and would be required to achieve compliance with, any regulatory or rulemaking activities relating to the vast range of components manufactured for and integrated within the bulk electric system. The comments set forth herein reflect the extensive collaboration and agreement of these bulk electric system supply chain entities and other impacted industry participants.

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 promotes uncertainty across the sector that has halted or delayed the nationwide installation, operations, and maintenance of a wide variety of critical bulk power system equipment during a time of multi-faceted challenges. As the Commission is well aware, the electric power sector is challenged with the continued provision of reliable and affordable electric service, economic challenges (including regulatory uncertainty), and supply challenges regarding the undulating nature of ongoing trade disputes. Moreover, FERC and industry have recently commenced compliance activities with respect to NERC CIP-013-1, *Cyber Security – Supply Chain Risk Management*, which specifically focuses upon the security of electric sector supply chain generation and transmission systems.

At its monthly open meeting held on September 17, 2020, FERC released the NOI that solicits the comments set forth herein. The NOI leverages upon the BPS EO, a separate Presidential executive order targeted at the supply chain for information and communications technology,³ telecom-focused provisions included within the two most recently-passed National Defense Authorization Acts (“NDAAs”),⁴ and related activities by the Federal Communications Commission addressing the national security threats posed by specific suppliers within that agency’s regulated industry. The NOI specifically seeks input from stakeholders on the potential exposure of the bulk electric system – and specifically substations, generating stations, and control rooms – to equipment manufactured or otherwise sourced by the entities identified as risks to national security within the NDAA’s.⁵ FERC’s NOI seeks comment on the current practices utilized by its regulated electric industries to identify and mitigate perceived vulnerabilities in the bulk electric system supply chain. As such, the NOI closely mirrors much of the feedback

³ Presidential Executive Order No. 13873, Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 22,689 (May 17, 2019) (the “ICTS EO”).

⁴ National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, § 1656 (2017); John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 889(f)(3) (2018).

⁵ It is imperative to note that none of the suspect entities specifically identified within the 2019 NDAA have participated in the Chamber’s Supply Chain Working Group. However, it is unclear whether any of the Supply Chain Working Group’s participants utilize or integrate within their products specific components or technologies manufactured by such entities.

requested by the Request for Information issued by DOE to inform its compliance activities, and a potential rulemaking responsive to, the BPS EO.⁶

The as yet uncertain implementation of the BPS EO and any potential additional FERC activities resulting from the NOI, if layered on top of 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-013-1 establishes security targets for “Bulk Electric Systems” performing transmission or generation functions at 100kV or higher. Meanwhile, 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 excluding electricity distribution systems. The NOI appears to focus on the facilities included within the “Bulk Electric Systems” definition, though clarification in this regard would be helpful.

The Chamber strongly supports the Commission’s goal of both understanding bulk electric system vulnerabilities and ensuring that any such vulnerabilities are mitigated or eliminated to the greatest extent possible. This shared goal is best met by clearly aligning the scope, requirements, and effective date of any future supply chain rulemaking activities – either by DOE or FERC – with preexisting and robust industry-led standards, including NERC CIP-013-1. 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.), currently remain unsure of how to proceed with infrastructure projects – and the associated design, manufacture, and commissioning of necessary bulk electric system components – given the multiple rulemakings and inquiries currently underway to evaluate the bulk electric system supply chain, both at DOE and now before FERC. Meanwhile, the codification of guidelines, rules, or regulations implementing the BPS EO are currently overdue, without current guidance on when such additional information will be forthcoming. The significant uncertainty borne by stakeholders is due to the broad scope of the BPS EO, the unclear application of the BPS EO and related inquiries to individual bulk electric system components, and the wide-ranging lack of clarity with respect to the ultimate implementation details of the BPS EO and any additional activities by FERC to address supply chain security.

II. The Electric Sector Supply Chain Shares the Goal of a Cyber-Secure Bulk Electric 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 electric system that is secure and resilient from sabotage, manipulation, or exploitation by nation-

⁶ Securing the United States Bulk-Power System, 85 Fed. Reg. 41,023 (July 8, 2020).

states and/or other bad actors. As such, the Chamber's working group shares the goals of FERC and DOE to ensure grid security. Moreover, the Supply Chain Working Group fully supports the full implementation of NERC CIP-013-1. 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 electric system. These preexisting programs and efforts should be leveraged, rather than overwritten, as FERC and DOE respond to the concerns raised by the ICTS EO, the BPS EO, and otherwise.

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. In a manner consistent with the SCRM Task Force, the Chamber asks that the Commission consults and collaborates with the electric sector supply chain and other bulk electric system stakeholders, including entities responsible for oil, natural gas, and related ICT infrastructure, as it evaluates future actions and activities relating to the security of the bulk electric system supply chain. 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 FERC and DOE consider additional activities in this space.

The Chamber and its Supply Chain Working Group are committed to working with FERC, DOE, and other relevant government entities in the development of any additional rules or regulations deemed necessary to protect critical bulk electric system operations while avoiding an overly broad scope or unduly impacting electric customer rates. Moreover, any additional initiatives should be tailored to minimize or eliminate stranded asset costs associated with otherwise unclear gains in grid security.

III. Principles to Guide the Enhancement of Supply Chain Security

In order to respond to the NOI and to support the Commission's consideration of any perceived vulnerabilities and mitigation measures currently in place, 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 related supply chain security concerns. These Principles seek to expand upon the Commission's understanding of the potential impacts of regulatory structures such as CIP-013-1 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 regulatory structures directed at securing the bulk electric system supply chain, it is imperative that the views and realities facing these impacted manufacturers are fully considered as FERC considers whether additional supply chain security actions are necessary beyond CIP-013-1.

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

1. As it considers whether additional actions are necessary to secure the bulk electric sector supply chain, FERC should consult with and implement the feedback of all impacted sectors within the bulk electric system ecosystem, including electric utilities, independent generation providers, transmission companies, major industrial producer-consumers (including oil and gas), other affected grid customers, and the electric sector supply chain (collectively, "Impacted Entities").
2. Without additional undue delay, FERC should work with DOE to provide guidance to clarify the interim responsibilities and legal obligations of all Impacted Entities with respect to potentially impacted bulk electric system equipment that was under contract or pending contract as of May 1, 2020 (the issuance date for the BPS EO), 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 further guidance from DOE, FERC, or otherwise. Such guidance should clarify the legal effective date of the BPS EO and any interrelated FERC activities, and should identify the types of transactions that may continue, without penalty, until additional guidance is issued from DOE and/or FERC.
3. In the event that FERC moves to propose additional standards or regulations that directly or indirectly impact electric sector supply chain entities, all such stakeholders should be entitled the opportunity to review, comment on, and provide suggestions for the improvement of such standards or regulations over a period of at least sixty (60) days.
4. In any subsequent action applicable either directly or indirectly to the electric sector supply chain, FERC should reaffirm the NERC CIP definition of "Bulk Electric Systems" to transmission and generation systems above 100 kV. Therefore, FERC should continue to exclude electricity distribution systems from the scope of any additional regulatory activity. FERC should seek to work with NERC, to the greatest extent possible, in light of NERC's mandate and mission of ensuring the reliability of the North American bulk power system.
5. Any additional FERC actions purporting to regulate, either directly or indirectly, the electric sector supply chain should be focused exclusively on maintaining the security and resilience of the domestic bulk electric 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. Any related regulatory actions should be appropriately and explicitly limited to bulk electric system electric equipment and not expanded to include other functions beyond that scope. For example, industrial controls systems, distributed control systems, and safety instrumented systems serve numerous functions outside of bulk electric systems. Any subsequent order resulting from the NOI should underscore that nothing therein shall be construed to promulgate additional regulations or standards relating to such equipment. If clearly defined proper safeguards and mitigation

measures are in place, such technologies should be exempted from FERC's limited authority over the reliability of the bulk electric system.

6. Any further Commission action in this proceeding should ensure that: (1) It provides a clear understanding of its applicability to Impacted Entities; and (2) Any additional requirements resulting therefrom neither overlap nor are inconsistent with existing or pending regulations already in place for the bulk electric system and Impacted Entities.
7. Any Commission action resulting from this NOI, as applied to bulk electric system equipment should, to the maximum extent practical, integrate and rely upon preexisting sector-specific efforts (*e.g.* NERC CIP-013-1), 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). NERC CIP-013-1 already 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. These and other preexisting activities should be leveraged to ensure that any additional regulatory activities support an efficient compliance architecture and prevent unintended conflicts with already applicable efforts, technical standards, controls, and certifications.
8. To the maximum extent possible, if FERC chooses to tailor any directive(s) resulting from this NOI to some larger or smaller subset of the domestic bulk electric system, such directive(s) should unequivocally so state.
9. In initiating additional action applicable to the electric sector supply chain the Commission should, to the maximum extent possible, clearly identify criteria that need to be met, as well as the specific products and components within such action's purview, while also specifying the products and components which will not be subject to such additional action. FERC's specification and identification need not identify products from particular suppliers, but rather should list well-defined categories of products utilized within the bulk electric system.
10. In taking any additional action applicable to electric sector supply chain security, FERC should utilize a definition of "foreign adversary" that is more durable and predictable than the contemporaneous listing of such nation-states provided within DOE's RFI or within the NDAAs referenced by the NOI. To provide clarity here, we suggest that FERC 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. Any Commission action resulting from the NOI should clearly delineate the depth of its application to individual grid equipment. For example, would a non-critical imported microchip within a complex power product otherwise domestically

manufactured and assembled potentially render an entire product non-conforming? In addition, FERC should identify how it will address current global transformation laws and country of origin calculations.

12. FERC should establish a carve out for Commercial Off-the-Shelf (COTS) components, products and other generic systems that are not purpose built for the bulk power industry. In addition, FERC 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" or similarly screened origin, such items without any programmable elements should still be available for use in COTS components and products. Otherwise, the application of additional rules or regulations to COTS components, products, and their makeup could serve to severely constrict the supply chain without any appreciable benefit to bulk electric system security.
13. FERC should advocate for a more effective framework for sharing actionable supply chain risk information among government and industry actors. 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. Thus, a truly effective information sharing framework 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 government agencies 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. If a FERC response to the NOI announces a plan to establish or rely upon a pre-existing prequalification program (*via* DOE or otherwise), to the maximum extent practical, such effort should 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 any prequalification program to be managed by a DOE national laboratory. Any prequalification program should detail such program's operations, how it will be funded, and how it will provide for the timely issuance of accreditations for bulk electric system equipment. In addition, such prequalification program should identify the extent to which it will involve physical testing of products or on-site assessments of vendor supply chains. Any FERC action should consider the establishment of a safe harbor for equipment that has been approved as part of such prequalification program.

15. If FERC seeks to restrict access to particular supply chain components based on country of origin, the Commission should provide an expedited mechanism whereby parties to negotiated contracts may seek FERC's pre-clearance for such transaction when it does not include otherwise 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 FERC 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. Any FERC action to restrict access to the electric sector supply chain should clearly articulate how the Commission will assess and incorporate into its decision-making the potential market impacts stemming from the implementation of such action, including an economic impact or cost-benefit analysis of any prohibition or prequalification requirement for certain products or components. FERC 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. Consistent with the Administrative Procedure Act, any FERC action that serves to place a limitation upon the electric sector supply chain should be subject to a rehearing process for any supply chain entities whose bulk electric system equipment is prohibited by a Commission decision or other binding action. Unless otherwise provided before a specific decision is rendered, any Impacted Entity should be provided with a meaningful opportunity to respond and potentially mitigate an adverse decision.
18. In the event that FERC moves forward with any requirement regarding the identification, isolation, monitoring, or replacement of installed bulk electric system equipment, the Commission should consider the replacement costs or monitoring and risk mitigation investments related to such installed equipment. Any action 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 imposition of any additional requirement(s) upon the electric sector supply chain, the Commission should seek, through targeted Congressional appropriation or otherwise, the resources to make Impacted Entities whole with respect to impacted bulk electric system components and equipment ordered, manufactured, contracted (or governed by contracts), or installed before the effective day of such requirement(s). Such financial indemnification could be conditioned upon such Impacted Entity's use of good faith to mitigate any costs reasonably avoidable consistent with existing contractual commitments.
20. Consistent with Principle 18, any FERC recommendation or requirement for the isolation and monitoring of bulk electric system 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 Commission 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. Concomitant with its authority over bulk electric system reliability, FERC 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. In recognition of the beneficial current activities of the Electricity Subsector Coordinating Council, the Commission should support the establishment of a critical infrastructure subsector coordinating council to collaborate with the bulk electric system supply chain.
22. In its consideration of additional rules or regulations applicable to the security of the supply chain for the bulk electric system, FERC should consult and coordinate with the critical manufacturing subsector coordinating council (or another industry body representing electric sector supply chain entities), and 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. In the event that FERC proposes to establish penalties for non-compliance that would purport to be applicable to electric sector supply chain entities, the Commission should set those forth with specificity and reference the authority upon which such an assertion of jurisdiction is premised.⁷ Any penalty provisions – such as those applied to regulated

⁷ The Supply Chain Working Group maintains that FERC lacks any jurisdiction to directly regulate or impose penalties upon the entities that manufacture equipment and/or components supplied for or integrated within the bulk

electric utilities consistent with FERC's jurisdiction – should include a safe harbor provision such that supply chain entities can demonstrate sound systems to determine the country of origin of the items they import. Such due diligence procedures 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. As it should undertake with respect to all mandatory electric reliability standards, FERC should periodically review the effectiveness of its activities relating to the bulk electric sector supply chain in achieving their sought security enhancement objectives while maintaining an efficient, competitive market for bulk electric system equipment. This formal review should provide Impacted Entities with the opportunity to provide suggestions for the improvement of FERC's activities relating to the bulk electric system supply chain.

The Commission's consideration and integration of the above Principles into its consideration of next steps relating to the NOI would not only reflect that the electric sector supply chain has been heard by FERC, but it would also ensure that any new Commission rules or regulations set 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 regulatory activities that conflict with – rather than build upon – the electric sector supply chain's strong commitment to the security of the United States bulk electric system.

IV. Conclusion

The Chamber and its Supply Chain Working Group support the intent of both FERC and DOE to evaluate and improve the security of the bulk electric system and the controls and processes of the entities that manufacture and supply its critical products and components. The bulk electric 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 electric 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.

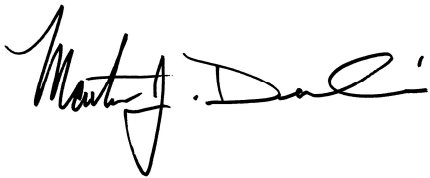
The increasing cyber challenges facing the bulk electric system are why the associated industries and government have enhanced their collaboration with respect to threat indicators and supply chain controls – with some such controls merely in their infancy, such as NERC CIP-013-1. Therefore, it is extremely important that FERC, as it considers additional actions in this space, lean into the existing programs, procedures, and controls that are aimed at the same security concerns referenced within the NOI. Only through a comprehensive inventory of existing bulk

electric system unless such entity is otherwise subject to FERC's jurisdiction as a result of its separate provision of interstate electric transmission services or participation in interstate wholesale power markets. Even in that case, however, such entity's manufacturing activities would presumably reside beyond FERC jurisdiction.

electric system protections can FERC and other government agencies effectively and efficiently manage the security of the bulk electric system.

The Chamber appreciates the opportunity to provide these comments responsive to the NOI. 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