



October 9, 2026

Mr. Andrew McClure
Director
Office of Cybersecurity, Energy Security, and Emergency Response
U.S. Department of Energy
1000 Independence Avenue SW
Washington, DC 20585

Re: Bulk Power System Executive Order; Docket No. DOE-HQ-2026-1123

Dear Director McClure:

The U.S. Chamber of Commerce (“the Chamber”) appreciates the opportunity to submit these comments in response to the Department of Energy’s (“DOE” or “the Department”) September 9, 2026, Request for Information (“RFI”) regarding the bulk power system supply chain.¹ The Department is soliciting comments through the RFI to inform its efforts to implement the directives set forth in Executive Order 14421 (the “BPS EO”), issued on August 26, 2026.²

The Chamber strongly supports the Department’s focus on strengthening the security, reliability, and resilience of the bulk power system. America’s electric infrastructure is foundational to economic growth, public safety, national security, advanced manufacturing, artificial intelligence, and the competitiveness of every region of the country. As electricity demand continues to grow, we must be able to expand, modernize, and secure the grid at the same time – these are not conflicting but are rather complementary goals. But this effort requires a practical, risk-based approach that protects the bulk power system without delaying needed investment, disrupting existing supply chains, or unintentionally increasing costs for consumers and businesses.

¹ Securing the United States Bulk-Power System, 91 Fed. Reg. 57,322 (September 9, 2026).

² Executive Order on Declaring a National Emergency to Secure the United States Bulk-Power System, 91 Fed. Reg. 55,995 (August 31, 2026).

Following the issuance of Executive Order 13920 in 2020, the Chamber convened an informal “Supply Chain Working Group” representing a broad range of a significant percentage of the participants across the supply chain for the bulk power system. That effort was designed to supplement the contributions of electric utility stakeholders and ensure that DOE had a full understanding of the entities that manufacture, procure, integrate, install, operate, and service the complex equipment that supports the country’s bulk power system.

The same basic guiding principle remains essential today as the Supply Chain Working Group submits these comments responsive to the RFI and the BPS EO: durable policy to secure the grid must be developed in close partnership with the private sector and must reflect the operational realities of the full energy sector supply chain.

A Proposed Framework for DOE’s Implementation of the BPS EO

The Chamber encourages DOE to adopt a framework that is targeted, workable, technology-neutral, and coordinated across the Federal Government. At a high level, DOE should:

1. Prioritize risk-based supply chain security measures focused on the most consequential threats and the most critical components;
2. Avoid broad prohibitions, duplicative compliance regimes, or retroactive requirements that could disrupt grid reliability or delay modernization;
3. Strengthen public-private collaboration and confidential information sharing, with appropriate protections for sensitive business information;
4. Coordinate with FERC, NERC, CISA, and other relevant Federal entities to avoid conflicting obligations;
5. Promote supply chain diversification through domestic capacity, trusted allies, and reliable trading partners;
6. Pair any new security expectations with clear definitions and realistic implementation requirements and timelines;
7. Stress security outcomes over prescriptive technology choices; and
8. Recognize that infrastructure deployment is critical to enhancing security.

I. DOE Should Implement a Risk-Based, Targeted Approach

The Chamber supports the objective of reducing unacceptable supply chain risks to the bulk power system. However, effective policy must distinguish between theoretical exposure and material risk. Not every foreign-sourced component, vendor relationship, software update, service provider, or subcomponent presents the same level of concern. Restrictions should be targeted toward identified cybersecurity risks and high-risk suppliers rather than broadly applied across entire equipment classes or technologies. Overly broad restrictions could capture equipment that poses little or no cybersecurity risk. A one-size-fits-all approach would strain limited industry and government resources while potentially delaying – or preventing – the deployment of equipment that is necessary to maintain reliability and meet the electricity demands concomitant with achieving global leadership in artificial intelligence.

DOE should focus its implementation of the BPS EO on clearly identified risks to the bulk power system, using transparent criteria and a structured risk assessment process. That process should consider, at a minimum:

- The function of the equipment or service within the bulk power system;
- The potential consequence of compromise or disruption;
- The degree of remote access, data visibility, or operational control involved;
- The availability of alternative suppliers;
- Existing utility, vendor, and industry cybersecurity controls;
- Whether mitigation is possible short of replacement or exclusion; and
- The operational impact of removal, substitution, or delayed procurement.

A risk-based approach will allow DOE to focus on the highest-priority threats while preserving the flexibility needed to maintain and expand the grid.

II. DOE Should Avoid Undermining Reliability or Ongoing Grid Modernization

The Chamber urges DOE to avoid policy approaches that could unintentionally create reliability risks. The bulk power system depends on long planning horizons, specialized manufacturing, complex engineering standards, and coordinated

procurement. Many critical components are not readily substitutable, and sudden restrictions on suppliers or equipment categories could produce cascading delays.

America's electricity grid is undergoing a period of significant growth. The expansion of domestic manufacturing, data centers, advanced technologies, electrification, and broader economic growth are increasing the need for reliable and affordable power. Meeting that demand requires more infrastructure, faster deployment, and regulatory certainty. Bulk power system supply chain security rules should be designed to support these goals, not frustrate them. As such, DOE should avoid retroactive requirements that mandate removal or replacement absent a specific, demonstrated risk and not develop blanket restrictions that fail to account for component function, system architecture, or available mitigation options. Further, duplicative reviews can delay urgent reliability projects, as can requirements that conflict with FERC, NERC, or other established reliability obligations.

In instances where DOE identifies a need for mitigation, the Department should provide affected entities with sufficient time, flexibility, and technical guidance to implement practical solutions without compromising reliability. Compliance timelines must reflect real-world project development cycles, customer approval processes, equipment lead times, and supply chain realities.

III. Public-Private Collaboration Is the Foundation of Any Durable Framework

The Chamber and its Supply Chain Working Group strongly support a collaborative model between the Federal Government and the owners, operators, manufacturers, vendors, and service providers that support the bulk power system. The private sector has deep technical expertise and direct visibility into procurement practices, equipment specifications, software integration, lifecycle management, and operational constraints. As such, the Department should leverage that expertise as it develops its implementation plan for the BPS EO and thereafter.

The Department should formalize engagement with the entire electric sector supply chain, including utilities, relevant infrastructure owners and operators, original equipment manufacturers, component suppliers, software providers, integrators, logistics companies, engineering firms, and other affected stakeholders. DOE should

also maintain strong coordination with the Electricity Subsector Coordinating Council and other established channels for government-industry engagement.

As part of its implementation process, DOE should promote structured opportunities for industry input before new obligations are proposed, while maintaining mechanisms for the confidential submission of sensitive technical and commercial information, as necessary. The Department should also provide stakeholders with a clear understanding of how DOE evaluates risk and should continue such engagement throughout the implementation of the BPS EO, as specialized supply chain companies possess technical knowledge that may be critical to understanding the operational impacts of DOE's implementation plan.

In addition, any supply chain review will necessarily involve sensitive commercial, technical, cybersecurity, and national security information. DOE should provide strong protections for information submitted by industry, including procurement data, vendor relationships, network architecture, software details, component-level information, vulnerability data, and mitigation plans. The Chamber urges the Department to clearly explain how submitted information will be protected, used, retained, and shared. Without the establishment of robust safeguards, relevant stakeholders may be reluctant to provide the level of detail necessary for DOE to make informed judgments. In addition, DOE should avoid public disclosure of information that could expose vulnerabilities, reveal proprietary business arrangements, or inadvertently create new security risks.

IV. DOE Should Coordinate Across the Federal Government

Supply chain security for the bulk power system cannot be addressed through fragmented agency action. DOE should ensure that any approach is coordinated with FERC, CISA, the Department of Commerce, the Department of Homeland Security, the Department of War, the intelligence community, and other relevant governmental partners, such as NERC. Coordination among these entities is especially important because the electric sector already operates under extensive reliability, cybersecurity, procurement, and operational obligations and regulations. New requirements resulting from the BPS EO should complement, rather than duplicate or conflict with, existing standards and processes. As such, DOE should work closely with FERC and NERC to ensure that any new supply chain security measures are aligned with existing reliability requirements.

V. Promote Diversification, Domestic Capacity, and Trusted Partners

The Chamber and its Supply Chain Working Group support efforts to strengthen domestic manufacturing and reduce overreliance on high-risk supply chains. However, supply chain resilience cannot be achieved through domestic production alone. The bulk power system relies on complex global supply chains, and many components require specialized materials, manufacturing processes, and technical expertise. DOE should pursue a balanced strategy that expands domestic capacity while deepening cooperation with trusted allies and trading partners.

This diversified approach, which places grid reliability and resilience first, should focus on the following: (1) Permitting reform for energy, manufacturing, mining, processing, and infrastructure projects; (2) Support for domestic production of critical grid components and materials where commercially viable; (3) Coordination with allied and partner nations to improve supply availability; (4) Policies that encourage investment in manufacturing capacity and workforce development; (5) Avoidance of punitive import and/or tariff restrictions on trusted partners where such actions worsen shortages or increase costs; and (6) Clear transition periods for any procurement-related policy changes. A resilient supply chain is one that is secure, diverse, flexible, and capable of supporting rapid grid expansion.

VI. Clear Definitions and Workable Compliance Expectations are Needed to Support Rising Electricity Demand

As the Department proceeds with an implementation rule or related regulatory action, enhanced clarity will be essential. Ambiguous definitions could create uncertainty for utilities and suppliers and will discourage investment. DOE should define key terms carefully, including the universe of “bulk-power system electric equipment” and the precise scope of the “bulk-power system” for the purposes of compliance with the BPS EO and the Department’s resulting regulations. All stakeholders should have a clear view as to what constitutes covered equipment, covered services, covered vendors, foreign ownership or control, remote access, critical components, and prohibited or restricted transactions.

DOE should also distinguish among equipment, software, firmware, services, data access, maintenance, and support functions. These categories present different risk profiles and should not be treated identically. DOE should also avoid imposing

obligations on suppliers that are impossible to satisfy because of limited visibility into upstream subcomponents or proprietary third-party systems. DOE's implementation requirements should be practical, auditable, and aligned with commercially available information.

VII. DOE Should Encourage Cybersecurity and Supply Chain Risk Management Without Mandating Prescriptive Technology Choices

The Chamber and its Supply Chain Working Group support strong cybersecurity and supply chain risk management practices. At the same time, DOE should avoid prescriptive requirements that lock in particular technologies, vendors, architectures, or compliance checklists. The threat environment changes quickly, and industry must retain the flexibility to adopt new tools, architectures, and mitigation techniques to maximize the security of our critical infrastructure.

DOE's implementing regulations should encourage outcome-based approaches that allow entities to demonstrate effective risk management through recognized practices, including vendor due diligence, secure procurement, software integrity, access controls, vulnerability management, incident response planning, component traceability (where feasible), and lifecycle management. Existing installed assets and related lifecycle support activities should receive clear treatment under the BPS EO to avoid unintended impacts to reliability, maintenance, modernization, and emergency response efforts. DOE should also recognize that different entities and equipment classes will require different controls. An outcome-based framework will produce better security results than a rigid compliance model that will become outdated or fail to account for operational realities.

VIII. DOE Should Recognize the Relationship Between Supply Chain Security, Permitting, and Infrastructure Deployment

Supply chain resilience is inseparable from the ability to build. Domestic manufacturing, mineral production, processing capacity, transmission infrastructure, generation resources, and grid modernization projects all depend on timely permitting and regulatory approvals. If projects cannot be approved and constructed on predictable timelines, the nation's electric grid will remain dependent on constrained or less secure supply chains.

The Chamber encourages DOE to use this RFI process to identify federal permitting and regulatory barriers that impede the development of secure domestic and allied supply chains. DOE should work across the Administration and with Congress to advance reforms that enable faster deployment of energy infrastructure, manufacturing capacity, and critical materials projects. Quite succinctly, security policy should be paired with policies that make secure supply possible.

Principles for the Sustainable Implementation of the BPS EO³

To respond to the RFI and to support the Department's development of a final rule and/or regulations implementing EO 14421, 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 across all stakeholders with equities in the operation, maintenance, and expansion 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 sector-wide compliance with the BPS EO, it is imperative that the views and realities facing electric sector component manufacturers, contractors, system integrators, and other entities responsible for specifying, procuring, integrating, installing, testing, and commissioning such equipment are fully considered by DOE as it moves forward with further actions, as directed by the BPS EO.

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

1. During the rules and regulations 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

³ The Chamber requests, consistent with the Administrative Procedure Act, that DOE next proceed with the issuance of proposed rules and/or regulations that will thereafter be subject to public comment, to solicit more specific feedback on the DOE's proposed implementation of the BPS EO. If DOE takes a different path toward the finalization of rules implementing the BPS EO, these comments and Principles apply equally to any such alternative pathway to facilitate industry compliance with the directives within the BPS EO, including any final rule or regulations resulting therefrom.

providers, transmission companies, affected grid customers, contractors, system integrators, and the electric sector supply chain (collectively, “Impacted Entities”).

2. Without additional undue delay, DOE should issue guidance⁴ 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 August 26, 2026, whether such contract is for the acquisition, importation, transfer, engineering, integration, installation, testing or commissioning of such equipment, software, firmware, digital and/or maintenance services, or other impacted items physical or virtual. Parties to these contracts fear penalty and seek clarifying guidance on their immediate responsibilities and legal obligations prior to the issuance of rules or regulations. 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 of the BPS EO. Notwithstanding the interim period, there should also be an adequate phase-in period to account for equipment lead times and supply chain realities.
3. Prior to the publication of a final rule, all Impacted Entities should be provided the opportunity to review, comment on, and provide suggestions for the improvement of publicly-issued draft and/or proposed rules for a period of at least sixty (60) days, with sufficient time thereafter for DOE to integrate such feedback into its final rule and regulations.
4. Within its resulting rule or regulations, DOE should align the implementation of the BPS EO with applicable NERC Reliability Standards to the maximum extent practicable, including 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 rule. Therefore, consistent with the BPS EO, DOE should clearly exclude electricity distribution systems from the scope of its forthcoming rule. The BPS EO demonstrates a clear intent to avoid the inclusion of distribution

⁴ Such guidance should address equipment and services subject to purchase orders, subcontracts, approved vendor lists, engineering specifications, fabrication commitments, and other binding project commitments entered into before the applicable restriction became effective.

systems in its definition of “Bulk-Power Systems.”⁵ 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-013-2, 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 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, DOE’s rule or regulations 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, programmable logical controllers, safety instrumented systems, protective relays, network infrastructure, cybersecurity appliances, and other operational technology (OT) 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 specific equipment, software, firmware, digital service, maintenance service, or remote-access capability unless it falls within the expressly defined scope of the BPS EO and presents the risk addressed by the rule. If clearly defined proper safeguards and mitigation measures are in place, technologies should be exempted from the scope of

⁵ 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 electric system 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.

the final rule. In addition, the DOE should identify clear mitigation measures and standards that allow technologies to be exempt from a final implementing rule or regulations.

6. Prior to the finalization of a rule, the DOE should perform an analysis to ensure that: (1) The rule provides a clear understanding of its 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. DOE should specifically ensure that compliance responsibilities are clearly allocated among owners/operators, contractors, original equipment manufacturers, system integrators, and lower tier suppliers based upon the information reasonably available to and controlled by each party.
7. DOE's 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-013), technical standards and reports (*e.g.*, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27402, 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). As noted above, DOE should parallel the scope of its rule to the greatest extent possible to that of NERC CIP-013. 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 any new DOE rule and already applicable efforts, technical standards, controls, and certifications. In the development of its rule or regulations, DOE's compliance mechanisms should permit reliance upon equivalent or substantially comparable industry recognized cybersecurity and supply chain assurance frameworks and should avoid requiring duplicative audits, certifications, or supplier assessments.

8. To the maximum extent possible, DOE's 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. Further, DOE should clearly state that implementing regulations do not apply to operations outside the United States (*i.e.*, in Mexico, Canada or elsewhere) for companies otherwise subject to DOE's jurisdiction and the rules and regulations resulting from the BPS EO.
9. To the maximum extent possible, DOE's resulting rule or regulations 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 publish a table indicating what equipment, software, etc., is included within its purview, and what is excluded from coverage, using well-defined voltage and asset types. Covered product definitions should be sufficiently specific to permit applicability determinations during engineering and procurement and should identify whether associated embedded software, firmware, communications modules, remote access capabilities, spare parts, and replacement components are included.
10. The final rule should more specifically define "Covered Foreign Entity" in a more predictable manner than the uncertain and potentially changing qualification of such nation-states provided within the BPS EO. 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 government of a foreign country." 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, DOE should identify how its rule or regulations will address current global transformation laws and country of origin calculations. Further, integrator attestations should be leveraged to avoid the unnecessary audit of sub-components.

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 (inclusive of facility-owner maintenance, repair, and operations (MRO), spares, and field-replacement orders) 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 "Covered Foreign Entity", such items without any programmable elements should still be available for use in COTS components and products. A simplified clearance process should also be available for commercially available components with programmable functionality where such functionality cannot reasonably create the security, remote access, sabotage, manipulation, or supply disruption risks addressed by the BPS EO. 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. DOE's rule or regulations 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. Accordingly, DOE's implementation 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 process, timing, and channels should suppliers use to notify DOE, customers, and any other stakeholders of incidents, known exploited vulnerabilities, material supplier-risk changes, software or firmware integrity concerns, or other conditions affecting equipment or associated services?
 - e. 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 ISACs 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 DOE's rule or regulations should set forth with specificity the BPS EO Section 2(e) 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 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 rule should identify the extent to which the prequalification program will involve physical testing of products or on-site assessments of vendor supply chains. DOE should also consider

the establishment of a safe harbor for equipment that has been approved as part of the prequalification program.⁶

15. To further mitigate unintended ambiguity, DOE's 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 implementing rule or regulations 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, project delays, procurement lead time increases, redesign costs, equipment substitution costs, construction impacts, commissioning delays, warranty impacts, spare parts availability, lifecycle support limitations, and increasing prices associated with diminished production capacity, as well as the potential impairment of international competitiveness for domestically manufactured products.
17. DOE's 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.

⁶ Prequalification should attach to clearly identified equipment configurations or product families and should identify what changes to hardware, firmware, software, manufacturing location, component sourcing, or ownership require requalification.

18. The rule's implementation of BPS EO Section 2(b), 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 isolation 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. Further, DOE should also consider impacts on plant safety, reliability, warranties, equipment certification, interoperability, commissioning status, long-term service agreements, spare parts strategies, and contractual performance guarantees before requiring isolation or replacement.
19. Concurrent with the finalization of the rule or regulations 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 August 26, 2026. 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 interim implementation guidance from DOE, consistent with existing contractual commitments.
20. Under BPS EO Section 2(b), 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, but DOE should define required security outcomes rather than prescribe specific cybersecurity technologies, recognizing that appropriate controls depend upon system architecture, operating environment, threat, consequence, and defense-in-depth measures. The suitability of particular 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. These deployment considerations should also account for vendor and

integrator provided remote monitoring, diagnostic, and firmware updating capabilities that are frequently required by contract and that support reliability and restoration. Any requirement addressing such supplier access should align with the vendor remote access controls of NERC CIP-005-7 R2 rather than establish parallel obligations. DOE's 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. DOE's implementing rule 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 (ESCC), the DOE should consider establishing a critical infrastructure subsector coordinating council to collaborate with the bulk power system supply chain and related engineering, procurement, and construction (EPC) contractors.
22. DOE should publish model contract clauses that facility owners, EPC contractors, and suppliers can utilize to reduce the potential for specific projects to impose differing and/or conflicting versions of DOE's rules and regulations implementing the BPS EO.
23. DOE's implementing 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 its rule or regulations implementing the BPS EO, and on a periodic basis thereafter, DOE should undertake regular, formal reviews of the effectiveness of its implementing rule in achieving the policy objectives of the BPS EO while maintaining an efficient, competitive market for bulk power system equipment. This formal review, which can be integrated

within the BPS EO's Section 6 congressional reporting requirement, should provide Impacted Entities with the opportunity to provide suggestions for the improvement of the DOE's implementation of the BPS EO.

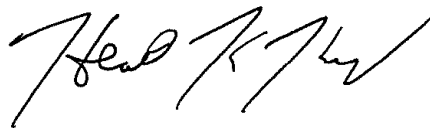
The DOE's consideration and integration of the above Principles into its formulation of its rule or regulations implementing the BPS EO will both ensure that the electric sector supply chain has been heard by DOE, but will also set forth a workable framework that is enduring and consistent with existing regulatory and other programs, while being mindful of the unnecessary costs and adverse security impacts that could result from 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.

Conclusion

The Chamber and its Supply Chain Working Group appreciate the Department's attention to the security and resilience of the bulk power system supply chain. The United States must protect critical energy infrastructure while also building the grid capacity necessary to support economic growth, technological leadership, and national security. These goals are mutually reinforcing when policy is practical, targeted, and developed in partnership with the private sector.

We look forward to working with DOE to develop sound bulk power system supply chain security measures that strengthen national security, preserve reliability, support affordability, and enable the expansion and modernization of America's electric infrastructure. If you have any questions or need additional information, please contact me at hknakmuhs@uschamber.com.

Sincerely,

A handwritten signature in black ink, appearing to read "Heath K. Knakmuhs", with a stylized flourish at the end.

Heath K. Knakmuhs
Vice President and Policy Counsel
Global Energy Institute
U.S. Chamber of Commerce