

October 9, 2026

SUBMITTED ELECTRONICALLY

Mr. Eric Rollison
Assistant Director, Technology Development
Office of Cybersecurity, Energy Security, and Emergency Response
U.S. Department of Energy
1000 Independence Avenue SW
Washington, D.C. 20585-0121
Email: BulkPowerEO@doe.gov
Telephone: 202-586-1769

RE: Bulk-Power System Executive Order RFI (Docket No. DOE-HQ-2026-1123)

Dear Mr. Rollison,

ACORE appreciates the opportunity to submit the following comments in response to the U.S. Department of Energy's ("the Department") Request for Information re: Docket No. DOE-HQ-2026-1123 ("the RFI"), which seeks public comment on recommendations for the implementation of Executive Order ("E.O.") 14421: *Declaring a National Emergency to Secure the United States Bulk-Power System*,¹ signed August 26, 2026.

ACORE² is a nonpartisan, nonprofit organization that operates at the intersection of affordability, reliability, and clean energy deployment. Our work is focused on stabilizing energy prices, strengthening the electric grid, and driving investment in cost-effective technologies to ensure that clean energy delivers for people, businesses, and the U.S. economy. ACORE's membership includes clean energy investors, developers, energy buyers, power generators, manufacturers, and energy providers.

ACORE's comment provides its view of the current threat landscape, the opportunities a connected grid presents for security and resiliency, and a brief overview of the existing regulatory foundation that the Department can align with and build from. ACORE then provides

¹ Executive Order 14421, "Declaring a National Emergency to Secure the United States Bulk-Power System" Federal Register 91, no. 167 (August 31, 2026): 55995-55999, <https://www.govinfo.gov/content/pkg/FR-2026-08-31/pdf/2026-17843.pdf>.

² "ACORE: Powering Investment in American Clean Energy," accessed August 25, 2026, <https://acore.org/>.

general recommendations for a future-focused regulatory regime, and specific responses to the categories of questions presented by the RFI.

Cyber Threats to American Critical Infrastructure and Society Continue to Evolve

In the early 2000s, cyber threats to critical infrastructure were primarily associated with independent hackers, cybercriminals seeking financial gain, and terrorist concerns. Since then, the digital evolution, made possible by more efficient internet connectivity and the expansion of commercially available connected technologies, has led to numerous innovations and advancements that benefit consumers, businesses of all sizes, and our national security enterprise. However, this same connectivity has increased the importance of cybersecurity across industry sectors and government, particularly as techniques and capabilities of foreign nation-state actors have grown.

The 2026 Annual Threat Assessment of the Intelligence Community,³ and 2025 Homeland Threat Assessments,⁴ as well as recent private-sector analysis by the Council on Foreign Relations,⁵ all highlight the risk to critical infrastructure of the active, well-resourced, and persistent efforts of nation-state actors to probe, infiltrate, and pre-position cyber exploitation and attack capabilities across U.S. critical infrastructure. These risks are real and present challenges for nearly every segment of society and the economy, not just the electricity sector. As the most recent internet crime report from the Federal Bureau of Investigation (“FBI”) makes clear, data breaches and ransomware are an issue across critical sectors, with the health care, critical manufacturing, financial services, government, and information technology sectors being the most significant targets.⁶

In the future, advances in technologies such as artificial intelligence (“AI”) and quantum computing present additional challenges that require thoughtful response now. Responding effectively to growing cyber and supply chain risks is a whole-of-government and whole-of-society challenge. ACORE’s members support the development of a thoughtful, durable regulatory regime to secure and strengthen the bulk power system (“BPS”), and other critical infrastructure for the future.

Connectivity and Digitization Create New Options for Strengthening the Grid

³ “2026 Annual Threat Assessment of the U.S. Intelligence Community,” ODNI, March 2026, <https://archive.dni.gov/files/ODNI/documents/assessments/ATA-2026-Unclassified-Report.pdf>.

⁴ “Homeland Threat Assessment 2025,” DHS I&A, October 2025, https://www.dhs.gov/sites/default/files/2024-10/24_0930_ia_24-320-ia-publication-2025-hta-final-30sep24-508.pdf.

⁵ Matthew Ferren, Adam Segal and Rush Doshi, “The Cyber Gap: How to Counter China’s Threat to America’s Critical Networks,” Council on Foreign Relations, September 2026, <https://www.cfr.org/reports/the-cyber-gap>.

⁶ “Federal Bureau of Investigation Internet Crime Report 2025,” FBI, 2025, https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf.

The BPS serves as the backbone that provides the electricity to support the U.S. economy, national defense, vital emergency services, and critical infrastructure. E.O. 14421, *Declaring a National Emergency to Secure the United States Bulk-Power System*, finds that U.S. dependence on affordable, reliable, and secure electricity has increased rapidly with the growth of vehicle and building electrification, advanced manufacturing, and AI.

After two decades of flat growth, U.S. electricity demand growth is forecasted to rise by 166 gigawatts (“GW”) through 2030—15x the peak load of New York City—according to utility forecasts submitted to the Federal Energy Regulatory Commission (“FERC”). Data center demand represents 55% of this forecast, with manufacturing, fossil fuel production and mining, and other sources of electricity demand making up the remaining 45%.⁷

This increase in electricity demand is placing severe upward pressure on key electricity sector equipment. According to recent analysis from McKinsey, the global supply backlog for transformers is expected to grow from approximately 1,000 gigavolt-amperes (“GVA”) in 2024 to 1,690 GVA by 2030, and the demand shortfall is only expected to compound.⁸ Lead times for switchgears have increased to 35-80 weeks (depending on size), well above historical averages.⁹ U.S. industry is actively working to address these and other supply constraints, with over \$185 billion invested in expanding domestic electric equipment manufacturing since 2018.¹⁰ The Department should be mindful of these constraints as it considers appropriate measures for implementing E.O. 14421 while maintaining a reliable, secure, and affordable electricity supply.

These developments represent a catalytic moment for investing in needed upgrades to the grid to advance security, reliability, and affordability of our electricity supply. For example, digital connectivity can provide advantages in performance and security. Software systems can be monitored, patched, and provide necessary real-time feedback when disrupted or attacked to allow for effective response and mitigation.¹¹ There are also performance benefits that allow for more effective utilization of transmission assets through better sensing that allows grid operators to better see and manage the system.¹² In addition, the application of these technologies and

⁷ John D. Wilson, et al., “Power Demand Forecasts Revised for Third Year Running, Led by Data Centers,” GridStrategies, November 2025, p 3, <https://gridstrategiesllc.com/wp-content/uploads/Grid-Strategies-National-Load-Growth-Report-2025.pdf>.

⁸ Carsten Hirschberg, Eike Reus and Thorsten Schleyer, “The transformer supercycle: Why demand is outrunning supply,” McKinsey & Company, September 18, 2026, <https://www.mckinsey.com/industries/electric-power-and-natural-gas/our-insights/the-transformer-supercycle-why-demand-is-outrunning-supply>.

⁹ “Electrical Switchgear Shortage: Supply Chain Impact & Solutions,” DEI Power Solutions, May 6, 2026 <https://feeds.deipower.com/blog/electrical-switchgear-shortage>.

¹⁰ Zach Gilbert, Don Leavens and Steve Wilcox, “2025 Guide to the Electroindustry,” NEMA, June 2025, https://www.makeitelectric.org/wp-content/uploads/Documents/Site_Pages/2025-Guide-to-the-Electroindustry.pdf.

¹¹ Phoebe Benich, Emma Stewart and Harry Krejas, “Electrotech Moneyball: An Industrial Strategy for Ranking Risk and Opportunity in Energy & AI Supply Chains,” Carnegie Mellon Institute for Strategy and Technology, <https://www.cmu.edu/cmist/tech-and-policy/electrotech-moneyball/electrotech-moneyball-cmist-white-paper-may-2026.pdf>.

¹² “Modernising Grids in the Age of Electricity: Scaling digital technologies and AI for better use of existing networks,” IEA, September 2026, <https://iea.blob.core.windows.net/assets/ebd98036-db76-4347-b498-4b18d73fe305/ModernisingGridsintheAgeofElectricity.pdf>.

systems is enhancing the capacity and resiliency of the grid, regardless of the type of generation: nuclear and gas plants, hydropower facilities, as well as solar, wind, and battery storage.¹³

Providing a clear, stable regulatory framework to align public and private tools will help support necessary investments in innovation in digital services, expanding the secure and domestic production capacity and workforce for equipment, and related activities.

Established Regulatory Frameworks Provide a Basis for E.O. 14421 to Build From

In recent years, cybersecurity and the supply chain for physical information communications technology (“ICT”) equipment have become more prominent areas of concern. As a result, numerous federal policies have been implemented to address each. The Department should seek to build on existing research, analysis, and requirements when implementing E.O. 14421. While not an exhaustive list of all public and private-led policies and initiatives, the following existing policies present existing structures and requirements that the Department should consider seeking to build off or align with.

Existing Cyber Security Regulations and Resources

The Government Accountability Office (“GAO”) has identified over one hundred federal cybersecurity regulations across 37 federal agencies and nine critical infrastructure sectors. Existing regulations include requirements to report cybersecurity incidents, report cybersecurity plans or other technical information, or conduct reviews, audits, or assessments.¹⁴ In addition to federal regulations, the Department has directed resources toward several initiatives that it should consider reviewing and building on as part of E.O. 14421 implementation, including:

- **Existing Cyber and Supply Chain Risk Management Standards:** Section 215 of the Federal Power Act of 1920¹⁵ requires mandatory and enforceable reliability standards to protect the reliability and security of the BPS, certifying the North American Energy Reliability Corporation (“NERC”) as the designated electric reliability organization (“ERO”). Of the rules assessed by GAO, 19 are applicable to the energy sector under either the Department or FERC, which include the Critical Infrastructure Protection (“CIP”) standards promulgated by NERC and implemented by FERC.¹⁶ NERC’s standards cover a range of categories applicable to the BPS, including supply chain risk management (NERC CIP-013), vendor electronic remote access security controls (CIP-003), as well as others.¹⁷ In addition,

¹³ Phoebe Benich, Emma Stewart, and Harry Krejsa, “Electrotech Moneyball: An Industrial Strategy for Ranking Risk and Opportunity in Energy & AI Supply Chains,” Carnegie Mellon Institute for Strategy and Technology, May 2026 <https://www.cmu.edu/cmist/tech-and-policy/electrotech-moneyball/index.html>.

¹⁴ “Cybersecurity Regulations: Multiple Sectors Are Subject to Potentially Duplicative Reporting Requirements,” GAO, July 22, 2026, <https://www.gao.gov/assets/gao-26-108606.pdf>.

¹⁵ 16 U.S.C. § 824o

¹⁶ Ibid.

¹⁷ “CIP - Critical Infrastructure Protection,” NERC, accessed October 6, 2026, <https://www.nerc.com/standards/reliability-standards/cip>.

federal contractors and agencies are subject to the National Institute of Standards and Technology's ("NIST") Cybersecurity Framework.¹⁸

- **Department-led Cyber Supply Chain Principles, Strategies, and Technical Assistance:** The Department has led development and adoption of Supply Chain Cybersecurity Principles,¹⁹ and is supporting ongoing research and analysis by the Departmental offices and national labs. The Department has also promulgated its own Cyber-Informed Engineering ("CIE") strategy that provides numerous resources for product designers, manufacturers, asset owners, and operators in implementing engineering solutions to secure technologies and equipment.²⁰ The Department also runs the Cybersecurity Testing for Resilient Industrial Control Systems ("CyTRICS") program for testing the security of software, firmware, and related aspects of critical infrastructure. These initiatives serve as important tools for identifying and mitigating risk and developing new and secure products and services.
- **Public-Private Information Sharing:** NERC's Electricity Information Sharing and Analysis Center ("E-ISAC") serves as the central public-private clearinghouse for information sharing related to the threat environment.²¹ Its mission is to reduce cyber and physical security risks by sharing trusted, timely, credible, and actionable information and analysis with over 1,900 member and partner organizations across North America's electricity industry. E-ISAC is separate from NERC's enforcement programs, and in addition to providing information, also provides training and exercises, as well as a vendor affiliate program focused on information sharing regarding supply chain risks.²²

Equipment Supply Chain Regulations and Resources

The U.S. government has taken numerous steps to restrict foreign adversary influence in sensitive supply chains, particularly for connected equipment that is used to support critical infrastructure. While these policies and programs are not exactly aligned with E.O. 14421, the following ICT supply chain policies are currently applicable to federal contractors, as well as other stakeholders that are also active in providing equipment and services for the BPS. The following programs, while not exhaustive, can serve as examples the Department can seek to build on, adopt, or otherwise align with to implement E.O. 14421:

¹⁸ "Frequently Asked Questions," NIST, accessed October 5, 2026, <https://www.nist.gov/cyberframework/faqs>

¹⁹ "Supply Chain Cybersecurity Principles," DOE, accessed October 5, 2026, <https://www.energy.gov/ceser/supply-chain-cybersecurity-principles>.

²⁰ "Cyber-Informed Engineering," DOE, accessed October 6, 2026, <https://www.energy.gov/ceser/cyber-informed-engineering>.

²¹ Michael Ball, Testimony before the Subcommittee on Energy, U.S. House Committee on Energy and Commerce, "Securing America's Energy Infrastructure: Addressing Cyber and Physical Threats to the Grid," December 2, 2025, <https://www.congress.gov/119/meeting/house/118711/witnesses/HHRG-119-IF03-Wstate-BallM-20251202.pdf>.

²² Ibid.

- **Federal Acquisition Supply Chain Security Act (FASCSA; P.L. 115-390):**²³ Enacted in 2018, this law and implementing regulations²⁴ created a government-wide framework to identify, assess, and mitigate supply chain risks in federal ICT acquisitions. Specifically, the FASCSA regime includes an interagency process for determining risks, issuing prohibition or removal orders for supplies or services, notifying prospective and existing contractors of those decisions, and providing for monitoring and reporting. These rules are currently applicable to federal contractors, and the government has established the infrastructure (e.g. online portals, resources, and guidance) for implementation.²⁵
- **Section 889 of the FY 2019 National Defense Authorization Act:**²⁶ Enacted in 2019, this law imposed federal procurement rules that prohibit agencies from obtaining telecommunications equipment, systems, or services reliant on such equipment or systems, if produced by certain foreign entities. Like the FASCSA regime, rules have been promulgated, implemented, and are applicable to federal contractors.²⁷ This regime provides numerous lessons for the Department to consider related to requirements, certifications, mitigation, and related matters that are directly relevant to this RFI. The GAO recently released a report²⁸ on the implementation of these requirements that finds that there has been a 90% decrease in contractor purchases of restricted equipment and services. GAO's report provides helpful insights into the lessons from the government's implementation of these requirements and recommendations for better coordination between federal agencies.
- **E.O. 13873, "Securing the Information and Communications Technology and Services Supply Chain:"**²⁹ E.O. 13873 was signed by President Trump in 2019, and subsequently implemented via regulations at 15 CFR Part 791.³⁰ This regime is directly analogous to the BPS order in that it relies on International Emergency Economic Powers Act ("IEEPA") authorities and seeks to address both cyber/connectivity concerns as well as physical equipment risks to the ICT supply chain. The rules provide a framework for identifying transactions and classes of transactions that may be subject to prohibition or mitigation, transaction reviews, processes for addressing identified concerns, and related matters.

²³ Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act, Pub. L. No. 115-390, 132 Stat. 1573 (2018).

²⁴ 41 C.F.R. 201-1

²⁵ "Quick guide to FASCSA implementation for GSA contractors," GSA, Accessed October 6, 2026, <https://www.gsa.gov/technology/government-it-initiatives/cybersecurity/cybersecurity-programs-and-policy/quick-guide-to-fascsa-implementation>.

²⁶ John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, 132 Stat. 1636 (2018).

²⁷ "Section 889 Policies," GSA, accessed October 6, 2026, <https://www.acquisition.gov/Section-889-Policies>.

²⁸ "Telecommunications: Better Information Sharing Needed to Ensure Compliance with Foreign-Sourced Equipment Prohibitions," GAO, September 2026, <https://www.gao.gov/assets/gao-26-108630.pdf>.

²⁹ Executive Order 13873, "Securing the Information and Communications Technology and Services Supply Chain," Federal Register 84, no. 96 (May 17, 2019): 22689-22692, <https://www.govinfo.gov/content/pkg/FR-2019-05-17/pdf/2019-10538.pdf>.

³⁰ 15 C.F.R. 791

- **Infrastructure Investment and Jobs Act (“IIJA,” or “Bipartisan Infrastructure Law;” P.L. 117-58) Foreign Entity of Concern (“FEOC”) Interpretive Guidance:** Enacted by Congress in 2021, Section 40207 imposed new FEOC restrictions as part of the Department’s \$6 billion battery materials processing, manufacturing, and recycling grant programs. The Department subsequently issued interpretive guidance³¹ to implement these restrictions, which provides a basis that can be used for E.O. 14421’s “Covered Foreign Entities” (“CFE”) provisions.

While E.O. 14421 explicitly combines both cyber/connectivity and physical equipment supply chain security issues, these existing policies and frameworks seek to address many of the same objectives as E.O. 14421, and are already in effect, understood, and implemented by various BPS stakeholders. The Department should look carefully at where it can align with or mirror the same requirements so that it is meeting the intent of E.O. 14421, as well as broader U.S. national security objectives, while also managing compliance requirements for the private sector.

ACORE’s specific responses to the questions posed in this RFI seek to draw substantially on these existing regimes.

Forward-Looking Framework Can Serve Long-Term U.S. Objectives

Over the past two decades, digital innovation has created tremendous benefits for American society. However, it has also led to novel challenges that more closely link economic, technological, and national security concerns and require a whole-of-society response. The Department’s implementation of E.O. 14421 can serve as an opportunity to build on and better align existing policies and requirements. It is also an opportunity to provide clear, administrable guidance that will provide private sector stakeholders with the certainty necessary to make long-term investments in their internal systems and policies, workforces, and supply chains, including new or expanded investments providing secure services and manufacturing capacity.

ACORE’s answers to the specific questions focus on several key principles and objectives for establishing such a regime:

- **Clearly Identify Risks:** Clearly define national security risks and CFEs of greatest concern and carefully scope the application of new rules and requirements based on the potential risk to the safe and reliable operations of the BPS posed by these factors.
- **Focus on Responding to Risks:** Establish a risk-informed, consequence-based regime focused on responding to potential operational control risks. This regime should distinguish between cybersecurity and physical equipment supply chain concerns.
- **Enhance Security but Minimize Disruption:** Provide near-term reliability authorizations or grandfathering of existing supply contracts. Such authorizations or other instruments may be

³¹ “Foreign Entity of Concern Interpretive Guidance,” DOE, accessed October 6, 2026, <https://www.energy.gov/cmei/manufacturing/foreign-entity-concern-interpretive-guidance>.

based on operator and vendor certifications that comply with existing requirements, such as NERC CIP-013 and/or appropriate/comparable standards. If mitigation is determined to be required, the Department should seek to use the least disruptive effective measure based on identified risks for existing systems and replacement should be a last resort. The Department should make clear that behind-the-meter and distribution-level equipment is excluded unless there is a strong and defined nexus to BPS security concerns and should consider providing liability protection for existing systems if they meet baseline compliance as part of any interim authorization program.

- **Prioritize Prospective, Effectively Resourced, and Appropriately Phased Implementation:** Establish a phased implementation approach that addresses near-term security risks, while providing clear direction and appropriate phase-in time for new requirements and standards, particularly if those new requirements require alternate sourcing or longer-lead investments in expanding capacity. Ensure that appropriate government systems, guidance, and other resources are allocated and in place prior to requirements taking effect to ensure compliance.
- **Build on and Align with Existing Policies:** Learn from and build on existing cybersecurity and physical equipment supply chain policies applicable to the ICT stack to provide consistency and alignment of standards across U.S. government agencies. Alignment of standards, requirements, and expectations will provide stability, reliability, and clarity of regulatory requirements that service providers, manufacturers, investors, and other stakeholders can effectively comply with and plan around.
- **Enhance Public-Private Risk Identification, Analysis, and Response:** Build on and enhance the U.S. government's coordination on identifying, analyzing, and communicating threats and risks to the private sector.
- **Give Clear Direction for Investment and Innovation:** A coordinated, phased approach to implementing new requirements coupled with alignment with federal funding (e.g. grants, loans, and other financial assistance) and research and development priorities will provide clear direction to U.S. stakeholders regarding the direction of future risks and requirements (e.g. future quantum computing standards and risks). This approach will provide the necessary stability and certainty to develop new products and services, shift sourcing, and expand capacity.

ACORE RESPONSES TO RFI QUESTIONS:

A: Scope, Definitions, and Covered Transactions (A1-6):

A-1:

ACORE Response:

ACORE³² is a nonpartisan, nonprofit organization that operates at the intersection of affordability, reliability, and clean energy deployment. Our work is focused on stabilizing energy prices, strengthening the electric grid, and driving investment in cost-effective technologies to ensure that clean energy delivers for people, businesses, and the U.S. economy. ACORE's membership includes clean energy investors, developers, energy buyers, power generators, manufacturers, and energy providers.

A-2 through A-5:

ACORE Response:

E.O. 14421 Section 2(a) directs the Secretary, in consultation with interagency partners, to identify transactions involving BPS electric equipment that is designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a CFE for prohibition based on criteria identified in the E.O.³³

In establishing the E.O. 14421 implementation program, the Department should first seek to provide additional clarity regarding the scope of BPS electrical equipment and transactions by relying on established definitions and regulatory structures where possible, and developing a phased, risk-based approach to the overall program.

First, the Department should clarify the definition of BPS pursuant to the order. ACORE recommends relying on the definition of BPS defined in the Federal Power Act³⁴ and implemented by NERC.³⁵ These terms and concepts are understood, currently implemented by BPS stakeholders, and are not inconsistent with the E.O.

Second, the Department should consider reviewing existing interagency review processes for evaluating and designating CFEs. The processes and procedures outlined in the Department of Commerce's information and communications technology and services ("ICTS") rules, Bureau of Industry and Security's ("BIS") Entity List rules,³⁶ and FASCSA rules provide examples of processes that provide for government assessment, review, and determinations of CFEs based on

³² "ACORE: Powering Investment in American Clean Energy," accessed August 25, 2026, <https://acore.org/>.

³³ Executive Order 14421, "Declaring a National Emergency to Secure the United States Bulk-Power System," Federal Register 91, no. 167 (August 31, 2026): 55995-55999, <https://www.govinfo.gov/content/pkg/FR-2026-08-31/pdf/2026-17843.pdf>.

³⁴ 16 U.S.C. § 824o

³⁵ "Bulk Electric System Definition Reference Document," NERC, April 30, 2026, <https://www.nerc.com/globalassets/programs/registration/registration-documentation/bes-reference-document-version-3---april-30-2026.pdf>.

³⁶ 15 C.F.R. 744.16

relative risk to the supply chain. These approaches allow the government to fully leverage national security information not available to the private sector to identify foreign entities that present risk, making determinations on the level of risk presented by a particular entity rather than imposing a blanket destination-based approach, and providing the private sector with clear guidance on the identities of prohibited CFEs. These regimes also provide guidance on administrative matters related to a CFE designation regime, such as information requirements, evidentiary basis, review, appeal, and removal as appropriate.

Third, the Department should consider clarifying the definition of “foreign-produced” for purposes of transaction review in a manner that focuses regulatory and private due diligence resources on equipment designed, developed, manufactured, or supplied by persons with a clear CFE nexus and focused on the relative risk or capabilities of the equipment. For example, imports from countries with robust rule-of-law frameworks, strong national security, trade, or technology relationships with the United States should be considered for preferential treatment under any transaction review or licensing regime. The Department should also draw on its experience implementing the FEOC requirements, as well as the lessons learned by other departments in the implementation of Section 889³⁷ regarding the challenges associated with obtaining upstream supplier information and other matters.

Finally, the Department should consider developing a risk-informed, consequence-based rubric that identifies transactions and classes of transactions and equipment that focuses on operational risks and addresses the two primary areas with a clear nexus to CFEs:

- 1) Connected systems and services; and**
- 2) Physical equipment and supply chains.**

A proposed framework for criteria to evaluate transactions or classes of transactions would provide clarity to the private sector regarding its requirements, while retaining flexibility for the government to address risks as they may arise on a transaction-by-transaction basis, etc.

- 1) High-Risk Systems and Equipment (Classification 1):** This class of transactions clearly meets all three criteria outlined in E.O. 14421 Section (2)(ii)(A)-(C) and encompasses systems, services, or equipment that have a high risk of negatively impacting the reliability, safety, and continuity of essential service and are subject to substantial direct foreign control by a defined CFE, and that such control, compromise, or malicious operation can directly impact or impair the reliable operations of the BPS in a systemic manner.
 - **Factors to Consider:** Level of reliance on CFE cloud operations, potential risk for surreptitious entry/control, contractual or operational grant of privileged or ongoing access that implicates operational control, aggregate capacity, critical function, and support for defense/critical loads.

³⁷ “Telecommunications: Better Information Sharing Needed to Ensure Compliance with Foreign-Sourced Equipment Prohibitions,” GAO, September 2026, <https://www.gao.gov/assets/gao-26-108630.pdf>.

- 2) **Priority Systems and Equipment (Classification 2):** This class of transactions and equipment has a high risk of material impact to reliability, safety, or delivery of essential services or BPS operations, but risks can be mitigated or constrained through measures subject to the control of U.S. BPS stakeholders.
- **Factors to Consider:** Whether ongoing monitoring, isolation, firmware updates, and other changes to cyber and physical equipment that affect operations and performance can mitigate such vulnerabilities. Availability of secure replacements, cost of disruption to the system, level of control by CFE, degree of impact to reliability, resilience of U.S. critical infrastructure or the economy, and safety and security of U.S. persons fall below Classification 1 and should be considered when determining whether prohibition, mitigation, contractual modifications, or other mechanisms may be appropriate.
- 3) **Limited Capability Systems and Equipment (Classification 3):** This class of transactions and equipment has a low risk of consequence to operations of the BPS pursuant to E.O. Section (2)(ii)(A)-(C).
- **Factors to Consider:** Systems, services, and equipment in this class have little or no capability as a single node or in the aggregate to impact BPS operations in a material way, such as individual pieces of hardware that can be repaired or replaced without disruption to the BPS. Consider items and equipment that do not have the capability for communication. This class of transactions may warrant establishment of safe harbors or general authorizations for operations or acquisitions.
- 4) **Transactions Determined Not to Implicate the BPS (Classification 4):** The Secretary should clarify the circumstances in which a transaction or class of transactions will not be considered subject to E.O. 14421.
- **Factors to Consider:** Systems, services, and equipment in this class are determined to serve facilities used in the local distribution of electric energy; behind-the-meter equipment (e.g. uninterrupted power systems (UPS), busduct, medium voltage (MV) switchgears and transformers, generators, etc.). Applicability of non-E.O. 14421 authorities, requirements, or compliance may be factored in (NOTE: The Department should consider whether provisions similar to the ICTS rules which exclude transactions subject to Committee on Foreign Investment in the United States (“CFIUS”) review, or the items are acquired by a U.S. person as a party to a transaction authorized under a U.S. government-industrial security program, may be appropriate.)

A-6:

ACORE Response:

Yes. The Department should consider providing Interim Reliability Authorizations or a similar type of instrument to system operators, asset owners, and/or vendors that meet existing standards, such as NERC CIP, or comparable standards. The Department should consider relying

on attestations or other existing documentation from vendors, asset owners, or other appropriate stakeholders that demonstrate compliance with cybersecurity policies, procedures, or related pre-existing information. Providing grid operators with interim reliability authorizations would allow for smooth functioning of the system, particularly for transactions and equipment that are already in service, to ensure affordable, reliable delivery of electricity as directed by Section 2(b) of the E.O. The Department should also consider whether such authorizations may provide liability protections for operators and vendors. Such authorizations would allow for continued operation of existing facilities and allow the Department time for the development and phased implementation of new rules and requirements that either prohibit transactions, impose standards that are higher or different than what currently exist, or require longer-lead supply chain changes.

B: Covered Foreign Entities and Supply Chain Risk Management (B 1-7):

ACORE Response:

The Department should sustain a risk-based approach to tracing ownership, manufacturing location, software provenance, firmware provenance, and access rights by CFEs.

In determining the appropriate scope of supply chain concerns presented by CFE-designed, developed, or produced equipment the Department consider the lessons from other agencies implementation of Section 889,³⁸ and the information sharing and other resources provided by NERC's E-ISAC.

As the GAO has reported, implementation of these requirements was phased over time, and the primary challenges confronted by the government included: 1) incomplete supply chain visibility; 2) difficulty complying with prohibitions in foreign countries; and 3) difficulty obtaining representation information for micro-purchases. These are directly relevant lessons because the agencies charged with implementing Section 889 are directly responsible for the majority of U.S. federal government contracting, including for the national security enterprise.

- 1) The government's response to incomplete supply chain visibility is relevant to the implementation of E.O. 14421. Federal contractors and the private sector can obtain regular and sufficient information for Tier 1 suppliers where supplier/country data is available and well-tracked. However, challenges arise deeper in the supply chain when looking at subcomponents. For example, ACORE understands that equipment classes such as certain UPS, MV switchgears, and others can be challenging.
- 2) In 2025, the General Services Administration ("GSA") established blanket purchase agreements to provide federal agencies with the ability to obtain commercial supply chain illumination services, which helped GSA to identify nearly 700 subsidiaries and affiliates of the five companies identified for Section 889 prohibitions.³⁹ These tools are available to the

³⁸ "Telecommunications: Better Information Sharing Needed to Ensure Compliance with Foreign-Sourced Equipment Prohibitions," GAO, September 2026, <https://files.gao.gov/reports/GAO-26-108630/index.html>.

³⁹ Ibid.

Department and private sector and can help improve visibility. The Department should consider making such resources available as appropriate to small- or medium-sized BPS stakeholders.

- 3) Consistent with a risk-based approach to the overall E.O. 14421 implementation process, the Department should consider:
- a. Establishing supply chain tracing and/or secure development lifecycle/remote access inventory, as well as related requirements for cyber-connected systems and equipment in a tiered manner, consistent with the operational concerns presented by transactions and equipment and nexus to a CFE;
 - b. Establishing a public list of determined CFEs (a “black list”), or of pre-approved suppliers (“a white list”), depending on relative risk of the equipment or supplier, and/or general authorizations for certain classes of equipment or services; and
 - c. Establishing a “reasonable inquiry” standard for services and equipment similar to the Section 889 standard, particularly if the BPS stakeholder demonstrates effective application of cyber and physical supply chain risk management frameworks and best practices promulgated by the Department, NERC, or other existing standards.

C: Risk Evaluation and Transaction Review (C 1-3)

ACORE Response:

Given the U.S. government’s unique resources, capabilities, and authorities for gathering information and intelligence related to cyber supply chain risks, the Department should leverage that information, as well as the work done by NERC, Idaho National Laboratory, and related stakeholders within the interagency and private sector to evaluate operational consequence and system criticality of the equipment and systems outlined in the E.O.

Regarding longer-term supply chain considerations, such as activities related to CFE supply concentration, the Department’s Manufacturing Deployment Office (formerly the Office of Manufacturing and Energy Supply Chains) should resume or continue work to develop its “Supply Chain Readiness Levels”⁴⁰ methodologies for providing information to private sector stakeholders with analysis of the risks at each level of the supply chain. These analyses provided detailed reviews of factors related to supply chain disruption, including sourcing risk management and related supply chain reliability factors.⁴¹

In both cases, the Department should consider building on existing or developing an ongoing, secure mechanism for receiving input and ongoing collaboration with the private sector.

⁴⁰ “Supply Chain Readiness Level Preliminary Analysis: Batteries Summary,” DOE MESC & MMAC, November 2024, [https://www.energy.gov/sites/default/files/2024-12/Supply_Chain_Readiness_Level_\(SCRL\)_Analysis_Nov2024--2024.12.04.pdf](https://www.energy.gov/sites/default/files/2024-12/Supply_Chain_Readiness_Level_(SCRL)_Analysis_Nov2024--2024.12.04.pdf).

⁴¹ Ibid.

D: Existing Equipment and Mitigation (D 1-4)**ACORE Response:**

E.O. 14421 makes clear that the Department must consider the “effects on reliability and safety, the availability of secure replacements, and continuity of essential service,” when it considers application of prohibition or mitigation measures on existing equipment.

To address potential near-term concerns, while preserving safety and reliability of the system, the Department should consider providing near-term reliability authorizations or the grandfathering of existing supply contracts. Such authorizations or other instruments may be based on operator and vendor certifications demonstrating that they are in compliance with existing requirements such as NERC CIP-013 and/or appropriate/comparable standards.

In addition, the Department should make clear behind-the-meter and distribution-level equipment is excluded unless there is a strong and defined nexus to identified BPS operational security concerns. The Department should also consider providing liability protection for existing systems if they meet baseline compliance.

If mitigation is determined to be necessary, the Department should seek to use the least disruptive effective measure based on identified risks for existing systems. The Department should consider replacement lead times and domestic manufacturing capacity before ordering disconnection or removal. For several categories, there are no U.S.-manufactured alternatives available today, and ordering removal without a secure replacement would impair reliability. As noted earlier, given the surge in electricity demand and need for equipment to meet that demand, order backlogs for key equipment continue to compound. If U.S. customers are forced to cancel contracts, equipment will be sold to other global markets.

E: Licensing, Mitigation Measures, and Prequalification (E 1)**ACORE Response:**

Any licensing regime should derive from risk-based classifications of transactions and equipment, clearly identify licensing requirements and which stakeholders are responsible for obtaining them, align requirements with other federal policies and requirements, and be appropriately resourced to ensure timely responses by the government.

The regime should be clear and predictable for market participants while providing the Department with information necessary to support national security and reliability objectives based on facts and circumstances. This approach allows the Department to retain authority and oversight of less consequential services and equipment, while prioritizing allocation of Department resources to be focused on highest priority issues and transactions.

The Department may want to consider licensing policies and structures like those administered by the Department of Commerce’s Bureau of Industry and Security (“BIS”) for export

licensing,⁴² securing the ICTS Supply Chain,⁴³ and information and certification requirements like those imposed under Section 889. A potential regime could include:

- 1) **Interim/Reliability Authorizations:** The Department should consider providing interim reliability authorizations to allow for smooth functioning of systems if certain basic certifications are met and can be provided to system operators and/or vendors that meet applicable standards (NERC CIP, DOE CIE, etc.). In the future, the Department may retain the authority to provide emergency authorizations for continued operations in exigent circumstances, subject to USG oversight and conditions as appropriate.
- 2) **Pre-Qualification/General Authorizations:** The Department should consider providing the ability to seek pre-qualification of products and services and/or providing general authorizations for classes of transactions and/or equipment presenting defined low risks, are widely commercially available, and/or for products and services that meet appropriate standards for cybersecurity and supply chain risk management. The Department may also choose to deem products and services that are compliant with other federal ICT regulations compliant and provide general authorizations to those classes of transactions. For example, the updated national security determination related to foreign-produced power inverters issued on August 20, 2026, identifies foreign-produced inverters that are eligible for the 45X Advanced Manufacturing Production Credit as those that do not pose the unacceptable security risks identified in the initial national security determination.⁴⁴ The Department should consider a similar approach in order to align with other Administration actions and priorities while also providing industry with clear signals for achieving compliance.
- 3) **Specific Licenses/Vendor Approvals:** Based on the risk and consequence-based criteria, transactions and equipment that present more significant degrees of risk to the BPS may require specific licenses or authorizations after review and approval from the Department instead of being deemed compliant. Such criteria could include: 1) operational risk to the system; 2) CFE or other foreign control over the service; 3) CFE or other foreign concentration of the supply chain; or 4) sensitivity of the load being served, etc.

Licenses could also be issued in the following cases:

- a. Licenses may be for specified terms based on overall lifecycle factors, which could include obsolescence of technology, adaptation to new technologies or standards (i.e. quantum cryptography, etc.), and others.
- b. Licenses may also include specific terms and conditions depending on relative risk and others factors as appropriate.

⁴² “About Licensing,” BIS, accessed October 7, 2026, <https://media.bis.gov/licensing>.

⁴³ “Office of Information and Communications Technology and Services (OICTS),” BIS, accessed October 7, 2026, bis.gov/OICTS.

⁴⁴ “FCC Announces Modification of Power Inverters on the Covered List,” FCC, August 20, 2026, <https://www.fcc.gov/document/fcc-announces-modification-power-inverters-covered-list>.

- c. Vendors that the Department approves based on testing and evaluation of product lines, supply chain information provided to the Department, application of Department-approved CIE, compliance with FAR 889 requirements, or other standards, etc. may receive a license.
 - d. Department may decide to issue list of pre-approved vendors.
- 4) **Advisory Determinations:** Stakeholders should be able to seek, and the Department should provide, advisory opinions or determinations that address the fact-specific scope or eligibility determinations as appropriate. The Department may make such determinations public as appropriate for matters of general interest/broad applicability. Vendors, service providers, or asset owners/grid operators may seek determinations.

F: Domestic Manufacturing, Secure Replacements, and Federal Procurement (F 1-5)

ACORE Response:

The Department’s Manufacturing Deployment Office should resume or continue work to develop its “Supply Chain Readiness Levels”⁴⁵ methodologies for providing information to private sector stakeholders with analysis of the risks at each level of the supply chain and align this analysis with federal financial support (e.g. grants, loans, and other financial assistance) to ensure that significant gaps in the supply chain are being addressed. As noted in ACORE’s response to Section E, the Department should also consider aligning with the approach taken under the updated national security determination related to foreign-produced power inverters issued on August 19, 2026. This national security determination states that foreign-produced inverters that are eligible for the 45X Advanced Manufacturing Production Credit do not pose the unacceptable security risks identified in the initial national security determination.⁴⁶

In addition, the Department should seek to coordinate with agencies charged with implementing Section 889 and the FASCSA to consider how they addressed similar questions in the national security supply chain, as these agencies have addressed issues related to mitigation, alternative sourcing, how to address “micro-purchases,” and other issues directly relevant to future E.O. 14421 implementation.

G: Economic and Regulatory Analysis (G 1-7)

ACORE Response:

The E.O. notes that “advanced manufacturing, data centers, artificial intelligence, and defense production,” all rely on reliable electricity. As the Department considers the economic and regulatory analysis to undergird its E.O. 14421 implementation, ACORE urges the Department

⁴⁵ “Supply Chain Readiness Level Preliminary Analysis: Batteries Summary,” DOE MESC & MMAC, November 2024, [https://www.energy.gov/sites/default/files/2024-12/Supply_Chain_Readiness_Level_\(SCRL\)_Analysis_Nov2024--2024.12.04.pdf](https://www.energy.gov/sites/default/files/2024-12/Supply_Chain_Readiness_Level_(SCRL)_Analysis_Nov2024--2024.12.04.pdf).

⁴⁶ “FCC Announces Modification of Power Inverters on the Covered List,” FCC, August 20, 2026, <https://www.fcc.gov/document/fcc-announces-modification-power-inverters-covered-list>.

to consider the indirect costs of potential mitigations, prohibitions, or other supply chain restrictions, particularly related to physical equipment.

As previously noted, substantial supply chain constraints and backlogs exist for key equipment, particularly for domestically produced equipment (e.g. PDC equipment, MV switchgear, and others), that is if domestic options exist. The Department's economic analysis should account for both direct costs related to the BPS supply chain, as well as indirect costs. Specifically, the Department should analyze the potential impact of E.O. 14421 implementation options for potential costs, delays, and abandoned projects for digital infrastructure, manufacturing, and defense production facilities, as well as the impact of those costs or reduction in planned projects intended to meet the Administration's broader economic, national security, and technological leadership objectives.

H: Implementation, Information Sharing, and Other Matters (H 1-3)

ACORE Response:

As highlighted throughout this comment, ACORE urges the Department to leverage existing federal policies, research and analysis, and other resources to implement E.O. 14421. These include standards developed by NERC, NIST, the Department, as well as private sector standards developed by entities such as the International Organization for Standardization ("ISO"), International Electrotechnical Commission ("IEC"), UL Standards & Engagement ("UL"), and others. Alignment with existing federal or industry-standards will help BPS stakeholders to manage compliance costs, plan around future compliance requirements, and ultimately achieve the Administration's security objectives.

If you have any questions about these comments, please do not hesitate to contact Jeremy Horan at horan@acore.org.

/s/ Jeremy Horan

Vice President, Government Affairs

ACORE

1150 Connecticut Ave NW, Suite 401

Washington, DC 20036

horan@acore.org

(202) 843-1987