

October 9, 2026

Filed Electronically via Regulations.gov

Mr. Eric Rollison, Assistant Director, Technology Development
Office of Cybersecurity, Energy Security, and Emergency Response
U.S. Department of Energy
1000 Independence Ave. SW
Washington, DC 20585-0121

RE: Bulk-Power System Executive Order RFI
Docket Number: DOE-HQ-2026-1123

Dear Mr. Rollison:

On behalf of the National Rural Electric Cooperative Association (NRECA) and our member cooperatives, we are writing in response to the Department of Energy's (DOE) Request for Information on "Executive Order (EO) 14421, *Declaring a National Emergency to Secure the United States Bulk-Power System.*"

I. Introduction and Background

Electric cooperatives support the White House's goals of strengthening the security and resilience of the bulk-power system (BPS) and reducing national security risks associated with vulnerable equipment, supply chains, and foreign adversary access. However, DOE should ensure that any new requirements avoid unnecessary delays to critical generation and transmission investments and preserve electric reliability and affordability.

To that end, DOE must consider the following in its implementation guidance for the EO:

- Cooperatives work closely across the electric sector and with government stakeholders to develop effective cyber, physical, and supply chain security programs. DOE should build upon these proven practices and frameworks, and the collaborative processes used to develop them, to avoid creating unnecessary requirements that provide limited additional security benefits.
- Implementation of the EO must recognize the scale of existing utility investments and protect critical generation, transmission, and grid modernization projects that are already underway.

- Supply chain security measures must be aligned with manufacturing realities and recognize that restrictions alone will not make up for a shortfall in domestic capacity.
- Cooperatives cannot independently assess the national security risk associated with complex global supply chains and require clear, authoritative federal guidance on prohibited suppliers, technologies, and transactions.

The electric sector is experiencing a period of unprecedented demand growth and DOE's implementation of the EO could have significant impacts on billions of dollars of equipment that are necessary to support our Nation's ability to meet that demand. As noted in EO 14262, "This increase in demand, coupled with existing capacity challenges, places a significant strain on our Nation's electric grid...The United States' ability to remain at the forefront of technological innovation depends on a reliable supply of energy".

Given the significance of the actions contemplated by this EO, DOE should view this RFI as the beginning of an ongoing stakeholder engagement process rather than the sole opportunity for public input. The implementation of the EO could have far-reaching implications for the availability, cost, and deployment timelines of critical bulk-power-system equipment, with direct consequences for the Administration's efforts to expand domestic energy production, accelerate infrastructure development, and meet growing electricity demand. Consistent with President Trump's emphasis on transparent rulemaking in EO 13891, which states that "Americans deserve an open and fair regulatory process" and that agencies should "take public input into account when appropriate," DOE should provide additional opportunities for public review and comment on any proposed regulations, implementation guidance, supplier determinations, or other requirements before they are finalized. This will help ensure that final requirements are practical, technically feasible, and aligned with the operational realities of maintaining and expanding the nation's electric grid.

NRECA Background

NRECA is the national trade association representing nearly 900 local electric cooperatives and other rural electric utilities. America's electric cooperatives are owned by the people that they serve and comprise a unique sector of the electric industry. From growing regions to remote farming communities, electric cooperatives power 1 in 8 Americans and serve as engines of economic development for 42 million Americans across 56 percent of the nation's landscape.

Electric cooperatives operate at cost and without a profit incentive. Each cooperative is governed by a board of directors elected from its membership. NRECA's member cooperatives include 64 generation and transmission (G&T) cooperatives and 832 distribution cooperatives. The G&Ts generate and transmit power to distribution cooperatives that provide it to the end of line cooperative consumer-members. Collectively, G&T cooperatives generate and transmit power to nearly 80% of distribution cooperatives, which in turn provide power directly to consumer-members at the end of the line. The remaining distribution cooperatives receive power directly from other generation sources within the electric utility sector. Both distribution and G&T cooperatives share an obligation to serve their consumer-members by providing affordable, reliable, and safe electric service.

Because many of the equipment categories potentially affected by EO 14421 are deployed primarily on transmission and generation systems, G&T cooperatives will be among the entities most directly impacted by DOE's implementation actions.

II. Overarching Considerations for DOE Implementation

NRECA developed these comments through direct engagement with member cooperatives to understand how implementation of EO 14421 could affect utility operations, reliability, cybersecurity, procurement, and future investments. While the RFI contains numerous individual questions, member feedback consistently centered on four overarching considerations that are outlined in the body of this section. Annex A provides additional detail, examples, and responses to specific RFI questions where further discussion is warranted.

Cooperative Operations and Procurement Requirements Have a Strong Foundation in Security

Cooperatives have built a strong foundation of cybersecurity, supply chain, and procurement practices designed to safeguard systems from malicious activity. This includes substantial investment in resources and programs designed to identify, assess, and mitigate many of the same risks the EO seeks to address. DOE should recognize these efforts and build upon the extensive work that has already been done by integrating any new requirements with these existing frameworks rather than layering them on top as additional compliance requirements.

Many cooperatives already manage supply chain and technology risks through mandatory reliability requirements and industry-led security initiatives. Cooperatives subject to the NERC Critical Infrastructure Protection (CIP) standards maintain supply chain risk management programs under CIP-013 and related standards that require the assessment of vendor risks, cybersecurity practices, software and firmware risks, and controls for critical systems and services. At the same time, cooperatives leverage industry resources and voluntary programs developed specifically for the electric sector, including NRECA's Cooperative Cyber Goals, cybersecurity self-assessment tools, Threat Analysis Center, information-sharing programs, and other resources that help cooperatives identify vulnerabilities and implement practical mitigations.

Cooperatives are keenly aware of the geopolitical threats posed by foreign entities of concern and avoid sourcing equipment from them wherever possible. The electric sector recognized early on that eliminating all potentially vulnerable devices from our systems was not feasible, given the complexity of global supply chains. Therefore, cooperatives, especially those that are part of the BPS and subject to NERC CIP requirements, employ strict cybersecurity controls and security measures such as network segmentation, restrictions on remote access, enhanced monitoring, and other risk-management practices designed to achieve the same end state as the EO.

Recommendation:

- Leverage and build upon existing regulatory and voluntary frameworks rather than creating duplicative programs that strain utility resources without providing additional security benefits.

Implementation Must Protect Reliability and Support Load Growth

The electric sector is entering a period of unprecedented infrastructure expansion. Cooperatives across the country are investing in new generation, transmission, energy storage, grid modernization, and control system upgrades to meet accelerating electricity demand and maintain reliability. As DOE implements the EO, it is critical that any restrictions, compliance measures, or security requirements balance those concerns with the impacts to reliability and affordability and the ability of cooperatives to support the Administration's broader Energy Dominance and Speed to Power initiatives.

NERC's long-term reliability assessments have repeatedly highlighted the challenges posed by accelerating load growth, expanding data center demand, and the need for significant additions of generation and transmission infrastructure. Within this context, implementation measures that delay projects, restrict available equipment, or divert resources away from grid expansion could conflict with the overall reliability and resilience objectives of the EO.

Impacts on Grid Expansion

DOE must carefully account for the realities of utility infrastructure planning and procurement. Major transmission and generation equipment is often designed, engineered, and ordered years before it enters service. Utilities cannot quickly substitute alternate equipment, suppliers, or technologies without considering engineering requirements, system compatibility, operational impacts, and manufacturing constraints.

Many cooperatives report that critical equipment such as transformers, breakers, relays, communications equipment, EMS and SCADA systems, and other technologies already face lead times measured in years. Restrictions affecting these assets could result in project delays and increased costs without necessarily reducing risk in a commensurate manner. DOE must ensure that implementation measures do not create reliability risks that exceed the risks they are intended to mitigate.

The potential impacts extend far beyond future procurement decisions. Cooperatives have already made substantial investments in equipment inventories, long-term purchase commitments, generation projects, transmission expansions, and grid modernization initiatives that are needed to maintain reliability and serve growing load.

Member responses demonstrate the scale of these investments.

- One cooperative has approximately 1000 MW of new generation projects already under development, with estimated stranded costs of \$1-2 billion if those projects cannot move forward.
- Another cooperative expects to invest approximately \$7.8 billion in existing and new generation and transmission assets through 2036, including 1,750 MW of new generation, 11 substations, and roughly 900 miles of high-voltage transmission.
- A third cooperative noted that they have roughly \$7 billion in projects planned over the next seven years that may involve equipment which could be within the eventual scope of DOE's requirements. These investments will support over 2600 MW of new generation and battery storage.

Other cooperatives reported significant investments in combustion turbines, battery energy storage systems, transformers, breakers, SCADA and EMS upgrades, cybersecurity systems, communications equipment, and other infrastructure necessary to support reliable operations and future load growth. Committed costs associated with these investments represent billions of dollars in additional expenses that would be passed on to consumers if they are unable to proceed. Further, some equipment and components may not be replaceable, or readily replaceable, because of their integration into an operating facility, original equipment manufacturer (OEM) design requirements, or the limited availability of technically compatible alternatives. A restriction or replacement mandate in those circumstances could jeopardize grid reliability and materially increase costs for distribution cooperatives and the homes, farms, and businesses they serve.

Battery storage projects present a particularly significant example. One cooperative identified approximately 450 MW of battery storage resources that have already been committed to satisfy near-term capacity needs. Replacing those resources would require redesign, re-procurement, additional interconnection studies, and could delay needed capacity beyond existing reliability timelines. Similar concerns exist across a range of generation, transmission, and control system projects that are already underway. Abrupt implementation measures could disrupt investments that utilities have made in good faith and that are urgently needed to maintain reliability and meet growing demand.

Impacts on Existing Equipment

DOE must avoid implementation approaches that rely on broad, mandatory replacement requirements where risk can be effectively mitigated through other means. Large-scale “rip-and-replace” mandates could create substantial capital expenditures, engineering challenges, construction delays, and reliability risks – particularly where replacement equipment is already unavailable or subject to multi-year lead times. Additionally, conducting comprehensive inventories and audits of potentially covered equipment already in operation presents their own challenges, given the size of cooperative service territories and the fact that some equipment has been in operation for decades. A complete review of equipment in use would require substantial resources, take years to complete, and cost millions of dollars – if it is even possible.

Experience in other critical infrastructure sectors demonstrates the risks of a mandatory “rip and replace” approach. For example, the FCC's order for telecom providers to remove Huawei and ZTE devices illustrates the challenges associated with replacing critical infrastructure at scale. While Congress initially appropriated \$1.9 billion, participating carriers ultimately identified nearly \$5 billion in eligible replacement costs, leaving a funding shortfall of more than \$3 billion. The FCC reported that nearly 40% of participants could not complete the required work without additional funding, several rural providers warned of potential network disruptions, and the agency granted dozens of deadline extensions due in large part to funding and implementation challenges.

For the electric sector, replacement of critical generation equipment, controls, or integrated systems at existing facilities could require engineering redesign, removal and installation work, controls programming, testing, commissioning, operator training, and extended planned outages. Replacement equipment would be subject to historically long lead times, particularly for highly engineered equipment such as combustion turbines, large power transformers, industrial control

systems, and associated software and services. One cooperative noted that, depending on DOE's final scope and the number of affected assets, extensive equipment replacement and retrofit work at existing facilities could cost hundreds of millions of dollars and result in costs and outages that would affect reliable operation for nearly 10,000 MW of generation and ultimately increase costs for consumers.

In many circumstances, existing mitigations and established cybersecurity controls can provide meaningful risk reduction without requiring immediate replacement of otherwise functional equipment. Utilities already employ measures such as network segmentation, restricted remote access, monitoring, and other security controls to reduce risk. Where risks can be effectively managed through mitigation, DOE must prioritize those approaches over wholesale replacement requirements that may provide limited incremental security benefits while imposing significant financial and reliability costs.

Apart from equipment already installed in their systems, cooperatives often acquire, transfer, and install BPS equipment through mutual assistance in response to a disaster. A determination that the EO is applicable to these types of arrangements would jeopardize long-standing contractual arrangements across the United States and reduce the reliability, security, and resiliency of the BPS in the times of greatest need (e.g., in response to a hurricane, earthquake, or other event). NRECA urges DOE to determine that the EO is not applicable to equipment sharing and emergency assistance agreements between utilities. Clarification on this issue is necessary as such agreements already exist and have subject inventories, the costs of which are being borne by utilities. Further, there could be significant costs incurred to re-negotiate existing agreements or, if necessary, terminate such agreements.

Implementation Timelines Must be Realistic

As previously noted, major projects and investments are planned years in advance and cannot be adjusted overnight. Utilities need predictable implementation timelines that are achievable, given existing supply chain limitations.

DOE must provide reasonable transition periods, grandfathering protections for existing equipment and projects already underway, and flexibility where compliance would create reliability concerns or where replacement equipment is not reasonably available. Implementation timelines must reflect actual manufacturing lead times and the realities of utility planning cycles. A phased, risk-informed approach will strengthen security while preserving the reliability, affordability, and infrastructure development needed to meet the nation's rapidly growing electricity demands.

Recommendations

- Ensure that any security requirements are appropriately tailored and implemented in a manner that preserves electric reliability and affordability, and do not unnecessarily delay critical generation or transmission investments.
- Use a risk-based framework when assessing equipment that is already installed, prioritizing mitigation and compensating controls over replacement.

- Provide cooperatives grandfathering protections, waivers, and employ phased transition timelines for existing inventories and projects under development to avoid project delays, reliability impacts, and unnecessary costs to consumers.

Domestic Manufacturing Capacity Must Meet Supply Chain Needs

While domestic manufacturing capacity has expanded in some areas, cooperatives continue to face limited supplier availability for many categories of critical grid equipment. In several product categories, including transformers, breakers, protection and control systems, and certain operational technologies, the market is served by a relatively small number of qualified manufacturers. To illustrate this point, a 2020 Department of Commerce report noted that only 20% of the large power transformers used in the U.S. were produced domestically.¹

Cooperatives are already facing significant supply chain challenges for critical grid infrastructure, with natural gas generation equipment commonly carrying lead times of four to five-and-a-half years, power transformers often requiring three to five years, and some high-voltage breakers taking more than two years to obtain. Given that domestic suppliers struggle to meet current demand, additional restrictions would extend these timelines, increase costs, and delay critical generation and transmission projects.

For some equipment, domestic alternatives may not exist at all, may not satisfy utility specifications, or may be unavailable within the timeframes needed to support planned projects. Imposing restrictions before replacement sources are available at the scale required for the current demand will increase competition, extend lead times, raise costs, and slow deployment of critical infrastructure.

Many cooperatives already operate under federal domestic sourcing requirements through USDA Rural Utilities Service financing programs. Cooperatives have spent years adapting procurement practices, supplier relationships, and purchasing decisions to comply with Buy American and related federal requirements. These existing sourcing requirements already influence procurement decisions and have demonstrated the capabilities, and limitations, of the domestic supply chain which should represent an important baseline to inform implementation of the EO.

Accordingly, DOE should align restrictions with the practical availability of secure alternative suppliers and existing manufacturing capacity. Where adequate domestic sources do not yet exist, DOE must consider the use of mitigation through cybersecurity measures and compensating controls. Furthermore, any proposed restrictions should be phased and target the highest priority risks, while also providing support for increasing the capacity of domestic manufacturing. Building secure supply chains is a long-term objective that requires sustained investment in domestic manufacturing and supplier diversity; it cannot be achieved simply by restricting access to equipment before viable alternatives are available.

Recommendations

¹ U.S. Department of Commerce, Bureau of Industry and Security, Office of Technology Evaluation, *The Effect of Imports of Transformers and Transformer Components on the National Security: An Investigation Conducted Under Section 232 of the Trade Expansion Act of 1962*, Final Report (Oct. 15, 2020), Washington, D.C.

- Ensure that any potential restrictions on equipment sourced from covered foreign entities account for the practical limitations of domestic manufacturing and supply chain capacity.
- Permit the use of proven cybersecurity measures, mitigations, and compensating controls to protect grid systems while domestic manufacturing options mature.

Utilities Require Clear Guidance on Prohibited Suppliers or Equipment

Electric utilities have limited visibility into global supply chains and are not positioned to independently make national security determinations regarding equipment suppliers, software providers, or technology risks. Utilities can evaluate vendors, assess operational needs, implement cybersecurity controls, and make procurement decisions based on available information. They cannot independently assess foreign ownership structures, intelligence regarding foreign adversaries, state influence over manufacturers, or the national security implications of particular technologies. Those determinations are appropriately made by the federal government using information and authorities that are unavailable to individual utilities.

Cooperatives work diligently to understand the supply chains associated with the equipment they procure. Many maintain visibility into manufacturers, suppliers, and final assembly locations and routinely obtain country-of-origin information as part of the procurement process. However, electric utilities generally purchase finished products rather than individual components. Visibility becomes increasingly limited below the manufacturer level, particularly for sub-tier suppliers, embedded software, firmware, chipsets, software dependencies, and other upstream elements. Several cooperatives noted that while they can often identify the vendor and manufacturer of a product, detailed component-level provenance, software lineage, and complete hardware or software bills of materials are often unavailable or controlled by the manufacturer.

This challenge is particularly significant for digital technologies. Many software-driven systems, communications platforms, EMS and SCADA systems, control systems, and other operational technologies rely upon complex and evolving software and firmware supply chains whose provenance cannot be independently verified by utilities. Compliance obligations can therefore only be as effective as the information manufacturers, suppliers, and software providers are able or willing to provide. Requiring utilities to independently verify information that resides exclusively with equipment manufacturers would create substantial administrative burdens while providing little additional value.

Utilities need clear, actionable guidance from authoritative sources regarding the equipment they purchase. For this reason, DOE should adopt a threat-informed approach that relies on federal expertise, rigorous testing, and intelligence capabilities to identify specific equipment, technology, or vendors that pose a potential national security risk. Furthermore, manufacturers and vendors, not utilities, should be responsible for determining the origin and provenance of the various inputs and technology that make up the equipment they sell and for complying with any restrictions or limitations imposed by DOE.

Regulatory certainty is also essential. Unclear or overly broad restrictions will delay procurement decisions, increase project costs, and create uncertainty for both utilities and manufacturers. These issues will exacerbate challenges with long-lead-time infrastructure projects where equipment procurement decisions must often be made years before construction is complete.

The costs associated with uncertainty are significant. Cooperatives reported that conducting asset inventories, equipment reviews, supply chain assessments, and documentation efforts could require years of effort and cost millions of dollars. As not-for-profit utilities, these costs are ultimately borne by cooperative consumer-members. DOE can substantially reduce these burdens by establishing clear compliance expectations and creating centralized processes that utilities can rely upon with confidence, such as product allow-listing, block-listing, or qualified vendor lists.

Recommendations

- Leverage federal intelligence, threat information, and national security expertise to identify elevated-risk suppliers or equipment rather than requiring utilities to make those determinations independently.
- Establish centralized processes and authoritative guidance identifying acceptable or prohibited suppliers, technologies, equipment categories, and transactions to provide utilities with clear and actionable compliance directions.
- Place disclosure, certification, and supply chain documentation responsibilities on manufacturers, vendors, and suppliers and limit utility compliance obligations to information that is reasonably available to equipment owners and operators.

III. Conclusion

NRECA and the Nation's electric cooperatives strongly support efforts to strengthen the security and resilience of the BPS and share the Administration's objective of reducing risk to vulnerable equipment and supply chains in a manner that protects both national security and electric reliability.

As DOE moves forward, NRECA encourages the Department to:

- Leverage the collaborative process used to create existing cybersecurity, supply chain security, and procurement frameworks to ensure that new requirements account for mitigations that are already in place and avoid creating unnecessary requirements that provide limited additional security benefits.
- Ensure that any security requirements are appropriately tailored and implemented in a manner that preserves electric reliability and affordability, and do not unnecessarily delay critical generation or transmission investments.
- Align restrictions with domestic manufacturing capacity and the availability of secure alternative suppliers, while permitting the use of mitigations and compensating controls where viable replacement options do not yet exist.
- Provide clear, authoritative federal guidance regarding prohibited suppliers, technologies, and transactions, recognizing that utilities do not have the visibility, threat intelligence, or authorities necessary to independently make national security determinations.
- Establish practical implementation timelines, grandfathering provisions, and compliance expectations that reflect utility planning cycles, equipment lead times, and ongoing reliability obligations.

Finally, the potential implications of this EO for grid reliability, infrastructure development, supply chains, and the Administration's broader energy objectives are too significant for this RFI to represent the final opportunity for stakeholder engagement. NRECA encourages DOE to treat this proceeding as the first step in an ongoing dialogue with industry and to provide additional opportunities for review and comment on proposed regulations, implementation guidance, supplier determinations, and other requirements before they are finalized. NRECA and its member cooperatives look forward to continuing to work with DOE to develop an implementation framework that strengthens the security of the BPS while preserving the reliable and affordable electric service upon which rural America depends.

Respectfully submitted,

John Ransom
Director of Regulatory Affairs
National Rural Electric Cooperative Association
4301 Wilson Blvd
Arlington, VA 22203
Phone: 571-565-6509
Email: john.ransom@nreca.coop

Annex A: Responses to Specific RFI Questions

Annex A contains additional detail for certain questions not fully answered in the narrative in Section II. These additional responses are identified with the alpha-numerical designation from the RFI, along with a paraphrased description of the question.

Section A. Scope, Definitions, and Covered Transactions

A-2 Definitions needing additional clarification

Bulk-Power System

The term “Bulk-Power System” (BPS) as defined in the EO references the “interconnected electric energy transmission network (or any portion thereof)” and “transmission lines rated at 69 kV or more but does not include facilities used in the local distribution of electric energy.” This definition does not align with the existing BPS definition as it is implemented through the definition of Bulk Electric System (BES) under the North American Electric Reliability Corporation’s (“NERC”) electric Reliability Standards. For the purposes of Section 215 of the FPA, NERC has defined the BES as:

“Unless modified by the lists shown below, all Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher. This does not include facilities used in the local distribution of electric energy.”

This definition is subject to both exclusions and inclusions based on additional criteria set forth in the definition. While not always, radial systems and equipment rated at 69 kV or less are typically excluded from the definition of BPS when their primary use is for the local distribution of electric energy. Further, this definition respects the well-established boundary between the state and federal jurisdictions.

With this understanding, and to ensure compatibility between the EO, Sections 205 and 215 of the FPA, and the FERC/NERC/ERO regulations/standards, NRECA recommends that DOE align the scope of applicability for the EO with the BES definition set forth under the NERC electric reliability standards. More specifically, if facilities would not be in scope pursuant to the BES definition, they should not be considered in-scope for the purposes of the EO.

Finally, the alignment of scope between the EO’s implementing regulations and the existing regulatory frameworks will establish a critical foundation for ensuring the compatibility of the various, overlapping regulatory frameworks. In particular, it will allow utilities to leverage their existing programs, processes, and procedures to ensure compliance with these new regulations. Simply put, a common set of applicable assets, programs, processes, and controls will improve the overall effectiveness and efficiency of supply chain risk management as well as facilitate the long-term sustainability of such efforts.

Digital Technologies, Software, and Services

There is additional uncertainty regarding the application of the EO to software, firmware, communications services, cloud-hosted platforms, EMS systems, and other digital technologies. DOE should clearly identify when software, support services, communications systems, or embedded digital components are considered covered equipment and distinguish between bulk-power-system operational technologies and general corporate IT systems. Equipment supporting

EMS, SCADA, telecommunications, and control center functions may involve globally sourced software, firmware, and support services that are fundamentally different from traditional power system equipment and may require different implementation approaches.

Inverter-Based Resources and Battery Energy Storage Systems

DOE should also clarify how the EO applies to inverter-based resources, battery energy storage systems (BESS), and associated control systems. Several cooperatives noted uncertainty regarding whether energy storage projects connected to distribution facilities, distribution-serving BESS installations, distributed energy resources, or inverter-based resources that do not directly affect bulk-power-system operations would be considered covered equipment. For example, cooperatives identified battery storage systems connected on the distribution side of substations that are used for peak-demand management and are configured not to export power onto the BPS. Such systems should not be treated as bulk-power-system equipment solely because they are electrically interconnected with facilities that ultimately connect to the transmission system.

More broadly, DOE should clearly distinguish between bulk-power-system assets, generation resources directly interconnected to the BPS, and distribution-connected resources whose primary purpose is serving local load. This distinction is particularly important for battery storage projects and inverter-based resources, where project developers may otherwise face uncertainty regarding compliance obligations, procurement decisions, and future operational requirements. Several cooperatives also expressed concern that restrictions affecting inverters or inverter-based resources could trigger redesigns, re-procurement efforts, and additional interconnection studies that would delay projects already under development. Clear definitions regarding the treatment of BESS, inverters, distributed energy resources, and associated control systems will be necessary to provide regulatory certainty and avoid unintended impacts on infrastructure deployment.

Section B. Covered Foreign Entities and Supply Chain Risk Management

B-3 Utility supply-chain risk assessment practices

Utilities are subject to the jurisdiction and regulatory requirements of various agencies, such as the Department of Justice, FERC, NERC, the Rural Utilities Service, etc. These regulatory requirements include the development and maintenance of an internal compliance program as well as specific rules, regulations, and standards that address risk and vulnerability management, e.g., the CIP reliability standards (18 C.F.R. § 40), and the Vulnerability and Risk Assessment requirements set forth at 7 C.F.R. § 1730.27. Additionally, utilities that produce nuclear power are also subject to specific risk management requirements under the NRC regulatory framework, including import and export control (10 C.F.R. § 110) and cyber and physical vulnerabilities (10 C.F.R. § 73.54). As a result of these and to better assure operational excellence, electric cooperatives conduct enterprise risk assessments that include evaluations of cybersecurity in several ways. These include:

- Completing assessments via integrated security management systems;
- Adopting comprehensive enterprise risk management programs that identify and evaluate cybersecurity risks; and

- Periodically evaluating through third-party surveys/assessments, compliance audits, and internal vulnerability assessments.

While the examples cited above illustrate a variety of approaches in the industry for assessing and mitigating security risks, many of these efforts do not specifically focus on foreign ownership, control, or influence (FOCI) but rather incorporate knowledge from government and open sources regarding FOCI areas of concern into the supply chain or enterprise risk assessment processes. Some of these assessments or programs are conducted in-house by cooperative asset owner personnel whereas other entities have utilized vendors to perform the service. In addition, electric cooperatives that have loans from the U.S. Department of Agriculture's Rural Utilities Service (RUS) are required to adhere to "Buy American" requirements in the federal regulations and RUS requirements. Only specific NERC registered electric cooperatives are required to comply with NERC CIP-013 (Supply Chain Risk Management). NERC CIP-013 requires applicable NERC registered entities to seek certain provisions and information in procurement and services from third-party vendors, manufacturers, and service providers. However, vendors, manufacturers and service providers are not subject to the NERC requirements and can't be forced to comply. If they don't agree to including certain provisions and information, then those NERC registered entities must demonstrate they tried to collect the information and describe alternate mitigation steps to reduce supply chain vulnerabilities.

In some cases, due to previous NERC Alerts or Recommendations to Industry or Advisories (applicable to NERC Registered entities) concerning foreign threats, electric cooperatives have reviewed various classes of systems to identify equipment of concern. Based on this analysis, steps have been taken to address risk associated with foreign components/ownership.

Supply Chain Risk Assessment programs evaluate security risks associated with various equipment vendors. This includes evaluating the ownership of the vendor company and the potential for equipment or parts of equipment to be manufactured or assembled outside the U.S. This assessment is difficult given the shifting and complicated ownership arrangements of the vendor community.

We recommend that DOE develop and manage a database that will track the lineage of vendors and their owners. If DOE had a database that traced vendors back through their chain of ownership, that would accelerate the ability of utilities to know who the "real" owner of the company is and avoid purchasing equipment if the owner is a covered foreign entity.

B-4 Utility governance of sub-tier suppliers

As asset owners and vendors have individual and unique relationships based on their negotiated contracts, vendor management/governance, monitoring, and tracking varies widely across the cooperative sector and has not been broadly subjected to robust metrics. In some cases, contractors provide lists of all subcontractors, in other cases entities may be required to comply with the RUS Buy American requirements and require vendors to sign a sourcing document indicating that the vendor is compliant. Others may not have a pathway or ability to manage their sub-tier vendors. If, when, and how an entity has governance around sub-tier vendors depends on many factors including its size, relation to the BPS, applicable regulatory requirements, and capabilities. For the entities that do have governance around sub-tier vendors, it is often addressed in the contract standard terms and conditions and taken into consideration when choosing vendors and contractors.

In addition, the supply chain risk management requirements of CIP 013 require policies/procedures to govern vendors. These policies/procedures include contract language, a risk base questionnaire, a security assessment, and other controls. If guidance is developed for service provider activities (e.g., integrator, installer, maintenance), it should clearly align with present NERC impact levels (low, medium, high) and focus on NERC's glossary term 'BES Cyber System' to ensure industry-wide continuity.

B-5: Utility capabilities to provide supply-chain provenance and authenticity

Cooperatives support tools that improve supply-chain transparency and product provenance, provided those tools are maintained by manufacturers, suppliers, or federal agencies rather than utilities. Cooperatives can typically identify a limited level of information about the equipment they purchase, such as manufacturers, suppliers, and country-of-origin, but they do not have independent access to detailed component-level information, software provenance, or complete hardware and software bills of materials. DOE should establish a centralized certification process or federal databases that allow utilities to rely on manufacturer disclosures and government determinations rather than independently recreating complex global supply chains. Provenance tools will be most effective when they place reporting and certification responsibilities on the entities with direct visibility into manufacturing and supplier relationships.

B-6 Utility security practices for software and services

Existing NERC Reliability Standards require policies/procedures to be in place. Some but not all electric cooperatives are subject to NERC standards. These policies include controlled electronic access, providing a security briefing and expectations to third parties for work on BPS cyber systems, contract language, and third-party certification. Any guidance from DOE should align with the current NERC impact levels (low, medium, high) and focus on the NERC Glossary term "BES Cyber System" to ensure industry continuity.

With regard to access control policies, NERC registered electric cooperatives have electronic and physical security controls in place for BPS sites, as required by NERC Reliability Standard CIP-003-8, CIP-004, CIP-005, CIP-006. In general, training, use of escorts and in some cases background checks are required for access to BPS sites. Access is granted based on need and applicable electric cooperatives document authorization for access to BPS sites. Installations are performed using asset owner controlled and maintained computers. Under CIP-003-8, if a vendor computer is necessary for installation, there must be a process in place to perform a security verification of the vendor computer.

Some electric cooperatives do not allow third-party remote monitoring or management of systems. For those that do, there are a variety of policies and practices in place including performing risk assessments, configuring remote access with multiple levels of security enabled, requiring multifactor authorization to access, requiring vendors who perform the monitoring and managing to submit a SOC 2 or SSAE 18 audit annually.

Additional controls for supply chain risk management are outlined in CIP-013 that require utilities to implement a documented supply chain risk management program to mitigate cybersecurity risks associated with BPS assets and vendors. Many generation and transmission cooperatives report that they already implement NERC CIP-013 supply chain risk management controls. However, while CIP-013 provides meaningful visibility into suppliers and vendor risk, CIP-013

does not provide component-level visibility into hardware, firmware, software, or sub-tier supply chains. As a result, while CIP-013 provides a strong basis for DOE to build upon, any enhanced traceability and certification obligations are better suited to be on manufacturers and suppliers rather than utility owners and operators.

Section C. Risk Evaluation and Transaction Review

C-3: How to measure supply disruption risk

Today's challenging electric supply chain environment compounds the complexity that cooperatives are navigating as they try to meet the forecasts of skyrocketing electricity demand without jeopardizing affordability or reliability. To successfully navigate this unprecedented time, cooperatives need to build new generation and upgrade and expand transmission and distribution systems. In a recent survey, cooperatives indicated they anticipate at least \$88 billion in total capital expenditure to meet the needs of their communities.

Most of the planned investment in new generation capacity over the next decade is natural gas combustion. Cooperatives are reporting lead times of 48-66 months, up 200-250% since 2022, for simple cycle gas generation units while prices have increased by as much as 95%, in some instances, since February 2025.

Transformers experienced a similar increase in cost and lead times over the previous years.

- For a 345 kV 168 MVA GSU transformer from Delta Star (made in the United States), the cost has risen about 5.5 times from eight years ago and the lead time is now up to 220 weeks.
- For a 10 MVA transmission transformer from Prolec GE (made in the United States), a cooperative reported a 1-year delivery time from 2024 to receipt in 2025, followed by a 2026 order being quoted a 1.5-year delivery time and a 33% cost increase.
- For multi-size and voltage rated GSU and transmission transformers coming from the U.S. (Delta Star or Virginia Transformer), cooperatives experienced triple-digit price escalations over the last several years and triple-digit percent increases in the lead times.
- For power transformers, cooperatives report that costs have doubled or run even higher compared to 2018-2020, and lead times have tripled to 3-5 years.

Additionally, high voltage circuit breakers and circuit switchers remain some of the most difficult to obtain in terms of price and lead time. According to cooperatives, as of May 2026:

- Prices on high voltage circuit breakers have risen significantly, with one cooperative reporting 69 KV breakers from GE being priced 219% higher today than in 2021. Prices can change by the time the breaker is shipped, and some manufacturers are restricting the size of the orders they will accept.
- 69 kV circuit breaker lead times sit at 62 weeks compared with 26 weeks in 2021.
- For two U.S.-manufacturers of 161 kV circuit breakers, lead times increased from a low of 22 weeks in 2022 to as high as 130 weeks in 2026. Price increases for the same manufacturers and times have increased by an average of 52% annually.

- For a 69 kV circuit switcher, the lead time went from 18-20 weeks in 2011 to 70-74 weeks in 2025.
- For a 115 kV circuit switcher, the lead time went from 12-14 weeks in 2010 to 88-90 weeks in 2023.
- Station Control Buildings have increased in price 225% from 2020 – 2025 and lead times increased to 35 weeks from 30 weeks.

Sourcing challenges that would arise with prohibited transactions include even longer lead times for procurement resulting in missing project deadlines, limited availability of supplies, delayed delivery, increased costs related to available supplies and resources devoted to review.

Electric cooperatives would need time to evaluate and qualify new suppliers and/or specific equipment to ensure they could meet applicable specifications. Additionally, prohibited transactions may have the potential to eliminate the cost differential waiver to procure from non-domestic suppliers currently allowed by the RUS Electric Program causing increased costs.

Section E. Licensing, Mitigation Measures, and Prequalification

E-1: License application requirements and review process

Licensing, waiver, and approval processes should be predictable, timely, and closely coordinated with utility procurement and construction schedules. Cooperatives frequently procure major equipment years before installation and often face long manufacturing lead times for transformers, breakers, and other critical infrastructure. Additional licensing reviews that occur late in the procurement process could delay projects, increase costs, and create reliability risks. DOE should establish clear review timelines, provide grandfathering protections for equipment already ordered or under contract, and create expedited processes for emergency procurement, storm restoration, equipment failures, and reliability-critical projects.

Section F. Domestic Manufacturing, Secure Replacements, and Federal Procurement

F-1: Assessing foreign dependency in critical supply chains

Given the limited capacity of domestic manufacturing, cooperatives depend on global supply chains for various equipment including transformers, breakers, capacitor banks, combustion turbines, communications equipment, software platforms, control systems, and other operational technologies. Even where final assembly occurs in the United States, equipment often relies on globally sourced components, embedded software, firmware, semiconductors, communications modules, and support services. While utilities generally have visibility into the final manufacturer or point of assembly, they lack visibility into deeper supply chain tiers. These realities demonstrate that dependence on covered foreign entities may exist at the component level rather than the finished equipment level.

F-5: Policies needed to strengthen secure supply chains

Policies to strengthen secure supply chains should focus not only on restrictions, but also on expanding available alternatives. DOE should enact policies to increase domestic manufacturing

capacity for critical grid equipment and develop centralized federal processes for identifying trusted suppliers and technologies. DOE should assume primary responsibility for identifying elevated-risk suppliers and maintaining authoritative supplier determinations, allowing utilities to focus resources on implementation rather than conducting duplicative investigations.

Section G. Economic and Regulatory Analysis

G-1: Compliance cost estimates

The costs associated with compliance will extend well beyond equipment replacement. Supply-chain reviews, documentation, engineering studies, supplier qualification efforts, legal reviews, cybersecurity analyses, and inventory assessments could require substantial new staffing and consultant support. One cooperative estimated that expanding cybersecurity monitoring capabilities to support additional compliance obligations would require approximately \$3.3 million in one-time costs and \$4.5 million annually thereafter. Other cooperatives indicated that comprehensive equipment reviews could require years of effort and cost millions of dollars.

G-6: Small-entity implementation challenges

The majority of electric cooperatives fall under the Small Business Administration's definition of small business; thus, this question is of critical concern to the electric cooperative community. First and foremost, increased costs, while likely for all utilities, are of special concern to small utilities. Additional evaluation and risk assessment processes will be time-consuming and costly. Given that electric cooperatives serve 92% of the persistent poverty counties in the United States, compliance costs run the risk of creating additional stress in these communities. Most of the additional costs won't scale; being small does not necessarily reduce the cost associated with complying with the EO.

In addition to having limited influence over vendors and product suppliers, small businesses have limited staff to address additional workload created by any regulations to implement the EO. We recommend that the DOE consult with the Small Business Administration and develop a process for identifying and mitigating small business impacts of implementing the EO.

Further, for utilities that are subject to the NERC reliability standards and the RUS Buy American obligations, application of a different and additional set of regulatory constraints relative to supply chain and associated processes and transactions presents a unique challenge. This potential for differing scopes of equipment to which these regulations apply creates further complexity and challenges for smaller entities. The costs of managing compliance with these new regulations while balancing and maintaining compliance with the existing regulations are a new and different cost from the potential increases in equipment, supply, and services costs and must also be considered.