To: U.S. Department of Energy
Office of Cybersecurity, Energy Security, and Emergency Response (CESER)
BulkPowerEO@doe.gov

From: The GridWise Alliance
Karen Wayland, PhD
Chief Executive Officer
kwayland@gridwise.org
(202) 580 - 6280

Date: October 9, 2026

Re: Request for Information (Docket No. DOE-HQ-2026-1123) on Securing the United States Bulk-Power System

A. Scope, Definitions, and Covered Transactions

A-1 *Respondent role/experience*

The GridWise Alliance appreciates the opportunity to provide our response to the Department of Energy's Request for Information on Securing the United States Bulk-Power System (DOE-HQ-2026-1123).

GridWise Alliance is a nonprofit membership organization serving the grid modernization and energy technology industry, with a membership spanning utilities, technology providers, consulting companies, national laboratories, independent system operators, and other stakeholders across the electricity value chain.

A-2 *Equipment categories needing clarification*

GridWise urges DOE to define "bulk-power system electric equipment" with clear, objective thresholds (e.g. voltage, capacity, function) rather than broad categorical sweeps, so that distribution-level or behind-the-meter equipment such as smaller BESS, DERs, and UPS, which pose limited bulk-system risk, is not inadvertently captured. GridWise notes that inverters, BESS, and industrial control systems are increasingly software-defined and multi-function and ask DOE to clarify whether classification should turn on nameplate capacity, point of interconnection, or actual grid function. Critically, EO 14421 notes that the "bulk-power system" includes transmission lines rated at 69 kilovolts (kV), "but does not include facilities used in the local distribution of electric energy." This 69 kV threshold should serve as a benchmark for DOE's assessment for whether certain transmission facilities are considered in scope of the order.

A-3 *Associated components/services in scope*

GridWise supports a risk- or function-based test (e.g. whether the item affects operation, protection, control, monitoring, or recovery of BPS equipment) over an absolute list to keep the rule administrable as technology evolves. GridWise suggests that DOE exclude general-purpose IT, commercial cloud, and enterprise software from

scope unless specifically configured for BPS control functions, to avoid chilling effects on unrelated commercial relationships.

Additionally, DOE should establish a presumption of approval for cybersecurity updates, including software patches, firmware updates, security, vulnerability-remediation packages, and malware signatures necessary to maintain the secure, reliable, and safe operation of already-installed bulk-power system electric equipment."

A-4 *Mixed-use items*

GridWise GWA recommends DOE rely on methods for entities to leverage documented configuration, deployment, and connectivity, such as network architecture diagrams and data flow mapping, as the practical basis for distinguishing in-scope from out-of-scope mixed-use items and provide a safe-harbor or self-certification pathway for common mixed-use equipment.

A-5 *Foreign-produced definition*

GridWise encourages DOE to align “foreign-produced” and substantial-transformation criteria with existing country-of-origin frameworks and focus any new compliance regime only on sanctioned countries rather than create a new, inconsistent country-of-origin standard. GridWise notes the practical difficulty of tracing sub-tier component origin and recommends phased, good-faith compliance standards, particularly for legacy equipment where records may not exist.
GridWise also encourages DOE to consider the risk that foreign-developed hardware or software could claim domestic-content status on the basis that its development involved commercially available U.S.-origin AI tools (e.g., large language models). DOE should clarify that use of a commercially available AI tool does not, by itself, constitute U.S. design, development, or manufacture for purposes of the foreign-produced definition.

A-6 *Prioritization / risk-based thresholds*

DOE should prioritize implementation around the highest-consequence equipment first (e.g. large-scale transmission-connected inverters and BESS, and SCADA/ICS with remote access) rather than a uniform rollout across all equipment classes, phasing in lower-risk categories over time.

B. Covered Foreign Entities and Supply Chain Risk Management

B-1 *Data sources for ownership/control*

GridWise notes that commercially available ownership-tracing tools have real limitations for privately held, joint-venture, or state-linked entities, and that DOE should not assume asset owners can achieve certainty. A “reasonable diligence” standard is more workable than a strict-liability one.

B-2 *Sub-tier tracing depth*

DOE should set a materiality- or criticality-based limit on how far down the supply chain tracing must go (for example, tier 1–2 for most equipment, with deeper tracing reserved for high-criticality, high-connectivity items) consistent with existing NERC CIP supply chain risk management practices.

B-3 *Enterprise risk assessments*

The existing NERC CIP-013 supply chain risk management processes should serve as a starting framework that DOE should build on rather than duplicate.

B-4 *Sub-tier vendor governance*

DOE should conduct stakeholder engagement to understand the contractual practices members already use concerning audit rights, incident notification, and security requirements in procurement contracts. However, GridWise cautions that utilities have a lack of visibility into sub-tier ownership changes over the life of a contract.

B-5 *SBOM/HBOM, provenance, anti-counterfeiting*

GridWise notes that software bill-of-materials practices are considerably more mature than hardware bill-of-materials practices. DOE should recognize this asymmetry rather than impose a one-size-fits-all documentation mandate.

B-6 *Securing software/firmware/remote access*

DOE should incorporate the secure-development and remote-access practices already required under NERC CIP for BES Cyber Systems (multifactor authentication, least privilege, session logging) and harmonize any new standards with these existing requirements rather than layer on new, potentially conflicting ones.

B-7 *Vulnerability testing, disclosure, insider risk*

DOE should leverage existing vulnerability disclosure and information-sharing channels, such as E-ISAC and ICS-CERT/CISA, rather than stand up a new parallel reporting regime.

C. Risk Evaluation and Transaction Review

C-1 *Consequence/criticality evaluation*

GridWise supports a multi-factor risk approach that accounts for function, redundancy, substitutability, concentration, and cascading impact. ***GridWise strongly recommends that DOE weigh the availability of secure replacements and lead times heavily, given current supply constraints***.

C-2 *Evidence for risk evaluation*

GridWise recommends tiered evidence approach for risk evaluation: more rigorous documentation for higher-risk, higher-criticality equipment, and streamlined attestation for lower-risk items. This approach would keep the process administrable for smaller utilities and vendors.

C-3 *Supply disruption risk factors*

GridWise cautions that certain categories, including large power transformers, HVDC components, and specialized inverter and BESS components, already face long lead times and concentrated global supply. Therefore, we urge caution in enacting any restrictions on the deployment of grid equipment that could worsen existing reliability risk without adequate transition time.

D. Existing Equipment and Mitigation

D-1 *Data fields currently maintained*

Asset owners' recordkeeping varies widely, especially for older installed equipment. DOE should not assume complete historical records exist. Reasonable-estimate and best-available-information approaches should be permitted.

D-2 *Mitigation options for existing equipment*

GridWise supports a menu of mitigation options (segmentation, monitoring, access restriction, and phased replacement) rather than a default requirement to remove or replace equipment, given cost, availability and lead-time realities.

D-3 *Reliability/safety factors before directed action*

GridWise strongly recommends that DOE weigh reliability and continuity-of-service impacts, and consult transmission planners and reliability coordinators/transmission operators before directing disconnection or removal of in-service equipment. GridWise also recommends that DOE conduct a formal reliability impact assessment before any mandatory action is taken.

D-4 *Monitoring/verification of implementation*

GridWise recommends attestation-based compliance paired with risk-based auditing, rather than universal independent assessment, to reduce burden. DOE must also protect confidential business information and sensitive security information in any reporting regime.

E. Licensing, Mitigation Measures, and Prequalification

E-1 *License application content/process*

DOE should build in expedited pathways for emergency restoration, imminent outages, and time-sensitive procurements, and to keep review timelines predictable (for example, through a defined shot-clock), so utilities can plan procurement and construction schedules. DOE could establish a robust prequalification program for vendors and equipment to reduce repetitive case-by-case review burden.

F. Domestic Manufacturing, Secure Replacements, and Federal Procurement

F-1 *Foreign dependence by category*

Procurement lead times and capacity constraints for categories of equipment such as large power transformers, certain inverter and BESS components and specialized ICS hardware are significant and changing rapidly.

F-2 *U.S. manufacturing capacity*

DOE should pair any restrictions with concrete demand-signal and capacity-building support, such as tax incentives, loan guarantees, and workforce investment, since expanding capacity for many equipment categories will take years.

F-3 *Secure alternatives available*

The development of technical equivalence, certification, and interoperability testing for alternative or domestic equipment can itself take significant time, therefore DOE should build transition periods around realistic secure-replacement timelines and and consider other mitigating activities that address the potential risk rather than relying on security goals alone.

F-4 *Federal procurement prioritization*

GridWise notes that the electric grid relies on a global supply chain and will continue to do so long into the future even with specific federal policies to reduce this dependence. Therefore, to maintain reliability and affordability, GridWise supports a “buy domestic where reasonably available” approach, with clear waiver and exception criteria for cases where reliability or cost would otherwise be compromised.

F-5 *Improving supply resilience*

DOE should consider aggregated and advance procurement commitments and strategic spares programs, which several members have found effective for long-lead-time equipment, and support standardization efforts for equipment that would expand the pool of qualified suppliers.

G. Economic and Regulatory Analysis

G-1/G-2 *Compliance costs*

GridWise recommends gathering aggregated, anonymized member input from utilities of all sizes and business models and grid equipment manufacturers on estimated compliance costs (documentation, supplier

requalification, and audits) rather than submitting unsupported cost claims. However, we recognize this may be difficult because the scope of the inquiry would be so broad.

G-3 *Market effects*

GridWise notes the risk of reduced supplier competition and higher equipment prices if the scope is defined too broadly or transition periods are too short, particularly for the BESS and inverter markets, which currently rely heavily on global supply.

G-4 *Reliability/safety costs and benefits*

GridWise emphasizes that forced accelerated replacement or reduced access to vendor support could itself create reliability risk. DOE should weigh these costs symmetrically against the anticipated security benefits.

G-5 *Benefits to quantify*

GridWise supports DOE's effort to quantify avoided-risk benefits, while cautioning that many benefits — such as avoided sabotage or avoided cascading outages — are inherently probabilistic and difficult to monetize with precision. Qualitative scenario analysis should accompany any quantitative estimates.

G-6 *Small-entity impacts*

Small utilities, cooperatives, and smaller vendors and manufacturers may lack the ownership-tracing, legal, and technical resources that larger entities have, so DOE should provide templates, safe harbors, and possibly a phased compliance timeline given the potential costs and staffing levels necessary to comply.

G-7 *Regulatory alternatives to reduce burden*

GridWise recommends that if DOE is to institute a new compliance regime, that it is a phased, risk-tiered approach that includes standardized forms and technical assistance, consistent with our response to H-1, as the primary tools for reducing burden while preserving DOE's security goals.

H. Implementation, Information Sharing, and Other Matters

H-1 *Technical assistance/pilot programs*

GridWise recommends that DOE fund or support pilot programs and model contract clauses developed in partnership with industry associations. GridWise offers the benefit of our diverse membership as a potential partner and convener for member education efforts.

H-2 *Other issues*

As noted above, GridWise strongly recommends coordinating any new security efforts with NERC CIP standards to avoid duplicative or conflicting compliance regimes. We further note the importance of interstate and interconnection-wide consistency so that multi-state utilities are not managing inconsistent state and federal requirements, and the need for workforce and vendor-transition support during any mandated equipment changes.

H-3 *Leveraging industry standards/third parties*

GridWise supports leveraging existing standards bodies and accredited testing and certification labs, such as UL and existing NERC-recognized processes, rather than having DOE build new certification infrastructure from scratch, which would speed implementation and reduce duplicative cost.