



October 9, 2026

Submitted electronically via BulkPowerEO@doe.gov.

Re: Securing the United States Bulk-Power System – Docket No. DOE-HQ-2026-1123

The American Public Power Association (APPA) and Large Public Power Council (LPPC) respectfully submit these comments in response to the Request for Information (RFI) issued by the Department of Energy (DOE) on September 9, 2026, regarding implementation of Executive Order (EO) 14421, *Declaring a National Emergency to Secure the United States Bulk-Power System*.

ABOUT THE AMERICAN PUBLIC POWER ASSOCIATION AND LARGE PUBLIC POWER COUNCIL
APPA is the voice of not-for-profit, community-owned utilities that power 2,000 towns and cities nationwide. Public power utilities are in every state except Hawaii. They collectively serve over 55 million people in 49 states and five U.S. territories, and account for 15 percent of all sales of electric energy (kilowatt-hours) to end-use consumers.

LPPC represents 29 of the nation's largest state and locally owned, not-for-profit public power systems, serving 30.5 million Americans across 23 states and territories. LPPC's members include the larger, asset-owning members of the public power community and own or contract for approximately 110 gigawatts of generating capacity. They account for approximately 90 percent of the transmission assets owned by public power. LPPC members are also members of APPA.

Public power utilities are load-serving entities, with the primary goal of providing the communities they serve with safe, reliable electric service at the lowest reasonable cost, consistent with good environmental stewardship. This orientation aligns the interests of the utilities with the long-term interests of the residents and businesses in their communities. Across both memberships, public power utilities are purchasers of bulk-power system equipment rather than manufacturers or suppliers of it, and the comments that follow are offered from that perspective.

Communications regarding these proceedings should be directed to:

Jonathan D. Schneider
Stinson LLP
1775 Pennsylvania Avenue NW
Suite 800
Washington, DC 20006
(202) 785-9100
jonathan.schneider@stinson.com

Latif Nurani
Senior Regulatory Counsel
American Public Power Association
2451 Crystal Dr., Suite 1000
Arlington, VA 22202
(202) 505-5381
lnurani@publicpower.org

Attorney for LPPC

GENERAL COMMENTS

Bulk-power system security is a central concern for public power utilities. When the grid is compromised, our communities suffer the consequences. That is certainly true for the hundreds of distribution-only public power utilities that are entirely dependent on the reliability and security of the bulk-power system to serve their communities; and it is doubly true for the many public power utilities that also own and operate bulk-power system facilities. No public power utility wants to install a relay, control system, or transformer monitor that a foreign adversary could manipulate. We therefore support federal government actions that can reduce those threats.

But security is not our members' only obligation. Especially during this period of significant investment in expanding the grid's capabilities, it is essential that public power utilities continue to serve their customers affordably. As not-for-profit utilities, our members have no shareholders to absorb cost increases: every dollar spent on equipment, compliance, or delay is ultimately paid by the communities that own the utility. Thus, our members have a duty to build in a way that is both secure and cost-conscious.

That duty is why APPA and LPPC have consistently urged that federal supply chain measures adhere to some basic principles:

- **Risk-based.** Requirements should be tailored both to the threats and to the potential impact to national security and grid operations posed by the potential compromise of particular equipment and facilities. Appropriate security measures for a 750 kilovolt (kV) substation are not the same as for a 20-megawatt (MW) backup generator.
- **Practical to implement.** A utility can only comply with obligations it can reasonably meet. Requirements should be based on information that a utility can access through normal commercial channels, not on knowledge that is accessible only to vendors, their suppliers, or the federal government.
- **Cost conscious.** The security benefits of any measure should justify its cost, especially when those costs are paid by retail customers.
- **Built on existing frameworks.** The electric sector already operates under mandatory, risk-based supply chain and cybersecurity standards developed by the North American Electric Reliability Corporation (NERC) and approved by the Federal Energy Regulatory Commission (FERC). DOE should build on those existing frameworks and ensure that new requirements are harmonized with them, rather than creating overlapping and potentially inconsistent obligations.
- **Clear and prospective.** Utilities need to know which equipment and transactions are covered before they have to comply. They also need a reasonable transition period for existing equipment and for procurements already underway.

These principles do not compete with security. Rather, they ensure that new security measures will work in practice without creating unintended consequences for the reliability and affordability of the grid.

APPA and LPPC therefore appreciate and support DOE’s stated intention to develop “practical, risk-informed, and administrable approaches” to implementing EO 14421. The comments that follow are intended to inform DOE on how to achieve those objectives.

RESPONSES TO SPECIFIC RFI QUESTIONS

In this section, we offer feedback on many of the questions posed in the RFI, grouped around several core recommendations. We have identified the RFI questions to which each section of our input is responsive.

To inform this input, APPA and LPPC conducted a survey of our bulk-power system owning members. Respondents generally reported that they can identify who owns the vendors they buy from directly, but have very limited ability to determine where those vendors’ component parts, software, and firmware come from, and members that have pressed suppliers for that information have often met resistance. Those findings shape many of the recommendations that follow, particularly our view that any prohibition must rest on information utilities can actually obtain.

Two stages. Our recommendations fall into two stages, divided by what information exists today and who holds it. The first is what DOE can do in its December 24 rule: a risk-based prohibition on new purchases, limited to the highest-impact facilities, to equipment that can affect grid operations, and to what a purchaser can learn from its own supplier, with compliance self-certified. The second applies only if DOE wants to go further, to suppliers’ suppliers or to inverter-based resources (IBRs) and batteries in the aggregate. It requires pieces that do not exist today. We believe those pieces would harmonize best with existing programs if built through North American Electric Reliability Corporation (NERC) standards developed within the scope DOE sets. In both stages, restrictions should apply prospectively to purchases, and mitigation should be preferred to replacement for installed equipment. We describe the two stages in connection with compliance and enforcement.

DOE should scope any measures to the highest impact facilities, using categories that already exist. (A-2, A-6, C-1)

Although EO 14421 allows the Secretary to prohibit, or take other measures, for *any* foreign-produced bulk-power system equipment and associated cyber assets that are deemed to pose undue risk, implementing such measures for *all* equipment connected at or operating above 69 kV is not needed to protect the grid. We urge DOE to adopt a risk-based approach that would prioritize measures affecting equipment used at higher impact bulk-power system substations, control rooms, and power generation.

To identify those facilities, we urge DOE to use NERC’s FERC-approved definitions of facility categories, as well as the definitions of Critical Defense Facility (CDF) and Defense Critical Electric Infrastructure (DCEI), rather than new definitions. Existing definitions under the Federal Power Act would facilitate harmonization and consistency with other regulatory frameworks.

Applying those definitions, we identify three categories of facilities warranting coverage in the December 24 rule, and a fourth for the second stage.

Defense critical infrastructure. The highest impact facilities are those that comprise DCEI that directly serve CDFs. Those DCEI facilities, and the equipment used in them, are—by definition—impactful on national security. DOE recognized the potential impact of these facilities in December 2020 when implementing EO 13920.¹ That prohibition order, which was subsequently revoked in April 2021, prohibited acquiring or importing specific equipment² used at DCEI facilities if that equipment was manufactured or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the People’s Republic of China.³

CIP-014 facilities. Another set of facilities that have very high impact on the grid are those covered by NERC’s CIP-014 reliability standard. That standard applies to high-voltage transmission facilities that, if rendered inoperable or damaged, could result in instability, uncontrolled separation, or cascading within an interconnection.⁴ Asset designation under the standard is subject to third-party review and NERC audit.⁵ FERC found that the facilities covered by this standard are “the most critical Bulk-Power System facilities.”⁶ And earlier this year, FERC approved modifications to the CIP-014 standard, reiterating that it provides “a consistent approach for identifying and assessing transmission stations, transmission substations, and primary control centers critical to the operation of the Bulk-Power System.”⁷

CIP-013 cyber systems. The third set of facilities that have high or medium impact on the grid are Bulk Electric System (BES) Cyber Systems covered by NERC’s CIP-013 reliability standard,⁸ and the covered equipment associated with the facilities in which those cyber systems function.⁹ CIP-013 requires security controls to manage supply chain risk associated with “High and Medium Impact BES Cyber Systems,” which are defined in NERC’s CIP-002 reliability

¹ [Prohibition Order Securing Critical Defense Facilities](#), 86 Fed. Reg. 533 (Jan. 6, 2021).

² The covered equipment consisted of power transformers and associated control and protection systems, generator step-up transformers, circuit breakers, reactive power equipment, and associated software/firmware. *Id.* at 536 (Attachment 1 – Regulated Equipment).

³ *Id.* at 534.

⁴ North American Electric Reliability Corporation, Reliability Standard NERC CIP-014-3, *Physical Security*, <https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-014-3.pdf>; see also Federal Power Act § 215, 16 U.S.C. § 824o (defining “reliable operations”).

⁵ North American Electric Reliability Corporation, Reliability Standard NERC CIP-014-3, Requirement R3.

⁶ *Physical Security Reliability Standard*, 149 FERC ¶ 61,140, P 2 (2014). FERC declined to expand the scope of this standard to include generating facilities, agreeing that a generating facility “does not have the same critical functionality as certain Transmission stations and Transmission substations due to the limited size of generating plants, the availability of other generation capacity connected to the grid, and planned resilience of the transmission system to react to the loss of a generation facility.” *Id.*, P 99.

⁷ *Order Approving Reliability Standard CIP-014-4*, 196 FERC ¶ 61,184, P 20 (Sept. 10, 2026).

⁸ North American Electric Reliability Corporation, Reliability Standard CIP-013-2, *Cyber Security—Supply Chain Risk Management*, <https://www.nerc.com/standards/reliability-standards/cip/cip-013-2>.

⁹ See our response to Questions A-3 and A-4 for a discussion of covered equipment.

standard.¹⁰ Attachment 1 to that standard identifies the facilities in which those systems function that would pose substantial risk to the grid if disabled. They include the following (each meeting specified criteria): control centers and backup control centers, commissioned generation, reactive resources, generating facilities, transmission facilities, special protection systems, and automatic load shedding systems.

Inverter-based resources and batteries. In the second stage, APPA and LPPC would add a fourth: IBRs and batteries purchased from a covered foreign entity that, in aggregate for any given balancing authority, would present as a single contingency triggering instability, uncontrolled separation, or cascading failures. We would add this category in recognition of the fact that while mis-operation of any given facility would not pose a risk to the BES, the equipment may, in aggregate, pose a substantial threat if sourced from a single covered foreign entity and operated in concert.

The concern is not hypothetical. In May 2025, Reuters reported that undocumented communication devices had been found in some inverters manufactured in a covered country, and cellular radios in some batteries from that country's suppliers, which could provide a communications path around the firewalls on which asset owners rely.¹¹

This category cannot be implemented by December 24. It depends on two things that do not exist today: a threshold for aggregate risk, which should be set for each balancing authority in a NERC standard, and the equipment information needed to measure against it.

NERC could, however, adopt a reporting standard quickly after December 24. Each entity registered as the owner of a covered IBR would report to its balancing authority the resources and batteries registered under that function, identifying the manufacturer and country of origin, or that the origin is unknown after reasonable diligence, without any threshold, study, or mitigation requirement attaching at that stage, and without any obligation to establish where every component or subcomponent was made. That reflects the records equipment owners typically keep, as described below in connection with existing equipment. The aggregation threshold would follow, and the reporting would give NERC the data needed to calibrate it.

NERC has just this past year implemented a program to have IBRs registered (including battery storage facilities), and is moving ahead with the application of substantive standards.¹² Owners and operators of IBRs with an aggregate nameplate capacity of 20 megavolt-amperes (MVA) or more, connected at 60 kV or above, are now registered with NERC as Category 2 Generator

¹⁰ North American Electric Reliability Corporation, Reliability Standard CIP-002-5.1a, *Cyber Security—BES Cyber System Categorization*, attach 1, <https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-002-5.1a.pdf>.

¹¹ Sarah McFarlane, *Rogue Communication Devices Found in Chinese Inverters*, Reuters (May 14, 2025), <https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/>.

¹² NERC, *NERC Files IBR Registration Update, Marking Milestone for Grid Reliability* (Apr. 29, 2026), <https://www.nerc.com/newsroom/nerc-files-ibr-registration-update-marking-milestone-for-grid-reliability>.

Owners and Generator Operators, effective May 15, 2026.¹³ That is why the reporting standard can move quickly: the entities that would report are already registered, and DOE would not need to identify them from scratch.

Only direct reporting by the registered owners reaches all of these resources. Many IBRs on the grid are owned by independent power producers, and many sell their output under power purchase agreements with entities other than the interconnecting utility. In those cases the utility has no contract that could give it visibility into the equipment, and where a utility does buy the output, existing agreements may not give it that information either. Among survey respondents that have, or may have, power purchase agreements or customer-owned equipment at 69 kV or above, none could fully identify the suppliers of that equipment, and most could not identify them at all.

The aggregation analysis also depends on DOE providing a list of the vendors, product lines, and firmware families it treats as presenting concerns—a list that we discuss in more detail below. Registered entities would check their asset registries against the list, and the list can identify the suppliers that share a risk or a common dependency. Without such a list, equipment sold under different brands that shares a common module or firmware family, and would fail together, appears unrelated.

Within the four categories, coverage should turn on whether an item can affect operations. (A-3, A-4)

We urge DOE to adopt a two-element test for coverage within each of the four categories. An item should be within scope only if (1) it contains software, firmware, or programmable logic, or provides a communications or remote-access interface, that can affect the operation, protection, control, or monitoring of bulk-power system equipment, and (2) it originates from and is provided by a Covered Foreign Entity. Items that fail the first element should be categorically excluded regardless of origin.

Those exclusions cover passive mechanical, structural, and electrical components, which contain no processor, executable code, communications interface, or programmable function and present no cyber pathway: carbon steel valve bodies, piping, fittings, flanges, gaskets, fasteners, pump casings, impellers, heat exchanger shells, storage tanks, mechanical turbine components including blades, vanes, bearings and seals, structural steel, and conductor, cable, bus bar, insulators and grounding materials. Without exclusions of this character, transaction review

¹³ NERC Rules of Procedure, App. 5B, *Statement of Compliance Registry Criteria* (Category 2 Generator Owner and Generator Operator), approved in N. Am. Elec. Reliability Corp., 187 FERC ¶ 61,196 (2024); see also ERO Enterprise, *CMEP Practice Guide: Application of the Registration Criteria for Category 2 Generator Owner and Generator Operator Inverter-Based Resources*, [https://www.nerc.com/pa/comp/RegistrationReferenceDocsDL/CMEP%20Practice%20Guide%20-%20Application%20of%20the%20Registration%20Criteria%20for%20Category%202%20Generator%20Owner%20and%20Generator%20Operator%20Inverter-Based%20Resources%20\(2\).pdf](https://www.nerc.com/pa/comp/RegistrationReferenceDocsDL/CMEP%20Practice%20Guide%20-%20Application%20of%20the%20Registration%20Criteria%20for%20Category%202%20Generator%20Owner%20and%20Generator%20Operator%20Inverter-Based%20Resources%20(2).pdf).

could extend to hundreds of thousands of routine maintenance and repair purchases annually across the industry, without corresponding security benefit.

A second limiting principle concerns depth rather than breadth. As described below in connection with supply chain tracing, public power utilities can see their direct supplier but not what lies beneath it, and none reported systematically maintaining records of component provenance for installed equipment, as described below in connection with existing equipment. One surveyed public power utility put the point directly: if the prohibition is confined to the equipment level, the effect on its procurement process would be manageable; if it extends to subcomponents, software, firmware, and supplier ownership, the effect becomes substantial and very difficult to quantify.

We therefore urge DOE to confine the prohibition, in the first instance, to what a purchaser can establish from the party with which it contracts: the identity and ownership of the supplier, and the origin of the equipment itself. Any obligation reaching below that level should take effect only when a mechanism exists to support it. That mechanism does not exist today. It would have to be built through third-party certification, on the models the nuclear industry uses for joint supplier audits and the Department of Defense uses for third-party cybersecurity assessment of its contractors, as described below in connection with supply chain tracing and the second stage described in connection with compliance and enforcement.

DOE should not prohibit existing equipment without specific and serious threat information and then order threat-specific mitigations rather than replacement. (D-1 through D-4)

Mitigation before replacement. We strongly urge DOE to implement EO 14421 prospectively. Section 2(b) of the EO reaches equipment already in service, not only future purchases, and directs the Secretary to evaluate what is installed and recommend whether it should be replaced or the risks mitigated. While the President has authorized DOE to order the isolation, disconnection, or replacement of existing equipment posing unacceptable risk to national security, DOE must “consider effects on reliability and safety, the availability of secure replacements, and continuity of essential service, and may establish phased compliance” before issuing such an order. Given the very serious reliability risks posed by removing equipment, DOE should treat this authority as an extraordinary measure to address the most serious and specific threats.

Information sharing is a central pillar to protect the grid from supply chain threats related to existing equipment. DOE and other federal agencies have access to intelligence that utilities lack. If DOE has specific threat information associated with specific equipment or vendors, providing that information to the utilities will allow utilities—in partnership with DOE and others—to address the identified risks.

The most appropriate mitigating action will depend on the nature of the threat and how the particular piece of equipment is being used within a given facility. Public power utilities report a variety of measures that they already implement to mitigate risk: network segmentation, monitoring, and restricted vendor remote access were the most commonly cited measures. Some utilities report the ability to fully isolate cyber assets from external connectivity.

We urge two structural features in any mitigation requirement. First, the required mitigation should be specified for a type of equipment rather than determined separately for each installed unit. Whether a given model requires network segmentation, firmware verification, or removal of remote access is a question about the model, and answering it once avoids every owner of that model repeating the same analysis. Second, a utility should be able to satisfy the requirement either through its own inspection, testing, and documented mitigation plan, or by relying on work performed by a qualified third party with respect to that type of equipment, on the model described below in connection with the nuclear supply chain.

Implementing mitigation measures such as the ones described above is faster and more affordable than replacement. Several utilities described extremely limited spare equipment that could be used to replace existing equipment. And most reported that replacing equipment can take 24-48 months, if it can be replaced at all. One utility described having Chinese-made hydroelectric equipment that is infeasible to retrofit.

In comparison, mitigation measures can be implemented relatively quickly: a few months, rather than years. The cost difference is also significant: several utilities described the ability to implement effective mitigation measures at less than a tenth of the cost of replacing the equipment.

When using mitigating measures, we recognize the need for DOE to verify that those measures are in place and operational. As discussed below, we believe that those compliance and enforcement mechanisms should be harmonized with existing processes, such as the NERC processes.

Identifying what you have. Another challenge utilities might face is identifying whether they have existing equipment that poses a risk. Many utilities have equipment that has been operating for many decades, with minimal records. For more recent vintage, however, most utilities surveyed by APPA and LPPC systematically maintain the following information about critical equipment: manufacturer, model number, serial number, supplier, and installation date. Very few utilities systematically track the country of manufacture or assembly for existing equipment, and none of the utilities surveyed reported systematically maintaining records of component provenance.

Data Field	Systematic Record Maintenance
Manufacturer	Most
Model	Most
Serial Number	Most
Production Facility	Very Few
Country of Manufacture/Assembly	Very Few
Supplier	Most
Integrator	Few
Installation Date	Most
Firmware/Software Versions	Very Few
Component Provenance	None
Network Connectivity	Most
Remote Access Pathways	Most
Service Provider	Few
Replacement Lead Time	Few

Restrictions on new purchases should be clear and prospective, with workable paths for pending procurements and emergencies. (E-1, F-3, F-5)

Public power utilities are in the middle of a long buildout. Many of the transformers, breakers, relays, and control systems they will install over the next several years are already under contract, already being made, or already in a procurement process. How DOE treats those transactions will determine whether EO 14421 improves security or simply delays the grid investments the EO itself identifies as essential to national security.

EO 14421 prohibits only transactions “initiated after the date of this order,” and only after the Secretary makes the determinations described in section 2(a). DOE should clarify that a transaction is initiated when the utility signs a binding contract or issues a purchase order, and that later steps under that contract, such as delivery, importation, or installation, are not new transactions. Large equipment can take years to arrive, and a utility that acted in good faith should not find equipment it ordered before any determination prohibited when it arrives. For transformers, breakers, and other long-lead equipment, that outcome would add to the project delays the buildout described above is already experiencing.

DOE should also make clear that a prohibition applies only to transactions initiated after DOE publicly identifies the covered equipment, vendors, or Covered Foreign Entities. Utilities cannot comply with a prohibition before they know what it covers.

Maintenance and firmware updates. We also urge DOE to confirm that applying firmware to equipment already in service is not an acquisition within the meaning of the EO. Nearly all members surveyed reported that no arrangement renews, updates, or deploys firmware absent a separate decision, so each update is a deliberate act by the utility rather than a vendor-initiated event. The equipment was acquired once. Maintaining it is not a second acquisition and treating

it as one would make the continued operation of installed equipment contingent on repeated review. Members identified this as among the clarifications they most need.

Equipment during emergencies. DOE should also create pathways—in advance—for procuring equipment during emergencies. When a storm, fire, or equipment failure takes a facility out of service, utilities need to restore it with whatever equipment is available, including equipment borrowed through mutual assistance. DOE should exempt emergency restoration from prior review, allow notice after the fact, and, where warranted, require that the replacement be addressed within a reasonable time after restoration.

Any supply chain tracing requirements must be practical to implement; further partnership is needed to systematically improve industry’s ability to see deeper into supply chains. (A-5, B-1 through B-7)

DOE should consider the practical realities of the global supply chain for electric equipment and the limited existing capability of utilities to determine the security risk associated with the third-party suppliers that provide components to the utility’s primary vendors. It would be unreasonable to implement EO 14421 in a way that would require each utility to individually conduct an investigation into sub-tier suppliers beyond what is available through existing commercial and governmental channels.

APPA and LPPC’s survey of their members reveals that they have a good understanding of the supply chain risks associated with their primary vendors. For their primary vendors, most know who owns and controls the vendor. Fewer know where the equipment was made, and very few record the country of manufacture systematically, as shown in connection with existing equipment. A few also have visibility into the ownership and manufacturing location of major components. Some members report the ability to trace software and firmware provenance with primary vendors. Nearly every member surveyed has control over access rights and remote-access pathways; many have this ability for sub-tier vendors as well.

Members also report that the capabilities needed to trace major components back through their suppliers’ suppliers do not presently exist at scale. Asked to rate software and hardware bills of materials, provenance and white-labeling tracking, component and update authentication, anti-tampering verification, and sub-tier supplier monitoring, members rated these capabilities emerging or unavailable almost without exception.

The majority of our members describe using vendor questionnaires as a principal tool for identifying supply chain risks. Some members use commercial databases to validate some of the information they receive, but there is no single vendor that currently provides comprehensive security risk validation of every vendor.¹⁴

¹⁴ Other than Dun & Bradstreet, which is used by several of our survey respondents, there was no commercial service that was widely used by public power utilities.

Our members widely report difficulties in using questionnaires or contractual terms to improve visibility into the ownership or control of their vendors' vendors. Many vendors refuse to provide information about components on the grounds that it is proprietary. Contractual terms can generally impose conditions for origin disclosure, but only at the equipment level, not components or subcomponents provided by third parties.

NERC reached the same conclusion in drafting CIP-013. The note to Requirement R2 provides that the actual terms and conditions of a procurement contract, and vendor performance and adherence to a contract, are outside the scope of the requirement, in acknowledgement that a single purchaser cannot compel a vendor. What a purchaser can extract is a function of its purchasing leverage rather than of the risk presented, with the result that contractual protection tracks purchasing power rather than system criticality.

We therefore raise for DOE's consideration whether a standard origin disclosure provision should be required in procurement contracts for covered equipment rather than left to negotiation. A term of this character is beyond the reach of any individual purchaser unless it is required of all purchasers.

A certification regime. APPA and LPPC believe that this is a situation that should be remedied. We envision a successful strategy to be one that includes joint action undertaken by industry and the government to press suppliers to disclose the provenance of product components, combined with a plan by DOE (and eventually, NERC) to develop a set of criteria governing third-party review and certification of the component parts of purchased equipment and software. Having expert organizations positioned to see vendors and supply practices across the industry, and which would work in conjunction with experts at DOE, NERC, and possibly other governmental authorities, would be a vastly superior approach to the utility-by-utility investigation described above. Reviewing and certifying entities that meet DOE/NERC criteria for activity in this area would then be authorized to certify that the vendors they have reviewed meet DOE specifications.

The mechanism matters as much as the principle, and the sequence by which it would be established is described below in connection with compliance and enforcement. The manufacturer holds the bill of materials, and the work should be placed there. An accredited certifying entity would audit a manufacturer once per product line, including following the chain of suppliers, with leverage no single utility possesses: a manufacturer that declines to disclose its ownership, its corporate records, or its parts list to a certifying entity may find that utilities are unable to purchase its product.

A certifying entity would not certify that firmware is secure. It would determine who owns, controls, and holds jurisdiction over the entities that produced the critical components and firmware, which is a documentary determination rather than a security judgment. Confidentiality matters equally. The proprietary objection noted above is not unreasonable when the alternative

is disclosure to every purchaser on the electric grid. A certifying body operating under an obligation of confidentiality reviews the material once and publishes only a conclusion.

We note that the nuclear industry has a model for joint action in ascertaining and verifying the security of components of the supply chain, developed after concerns surfaced regarding the authenticity of elements of the supply chain. Formed in 1989 and with membership comprising the owners of all U.S. nuclear generating facilities, in addition to foreign owners, the Nuclear Procurement Issues Corporation (NUPIC) organizes members to undertake joint supplier audits and share results.¹⁵ The organization also provides the industry with a list of certified suppliers and its audits are recognized by the Nuclear Regulatory Commission (NRC) in satisfaction of the NRC's supplier security regulations.

In describing the NUPIC process, the NRC asserts that "NRC staff continues to rely on the effectiveness of the NUPIC joint utility audit process for evaluating the implementation of quality assurance programs of suppliers to the nuclear industry."¹⁶ Under relevant regulations, the NRC is authorized to accept the work of third-party reviewers (Dedicating Entities), which can provide assurance that basic components of the nuclear supply chain can perform their intended safety functions.¹⁷

The federal government has also recently adopted a closely analogous structure in another sector. Under the Cybersecurity Maturity Model Certification program, now in force under 32 C.F.R. Part 170 and the corresponding acquisition rule, a single accreditation body authorizes third-party assessment organizations, those organizations conduct assessments, the Defense Contract Management Agency assesses both the accreditation body and the assessors, and requirements flow down to subcontractors. Assessment is tiered, with self-assessment at the lowest level, third-party assessment at the intermediate level, and government assessment at the highest. These precedents demonstrate that a federal agency can rely on accredited private assessors without constructing assessment capacity of its own.

DOE should consider the impact on small, not-for-profit utilities when scoping any implementing rules. (G-6, G-7)

APPA and LPPC's recommendations above matter most for the smallest public power utilities. EO 14421 defines the bulk-power system to include transmission facilities rated at 69 kV or more. That definition reaches many small- and mid-sized public power utilities that own a few miles of 69 kV line, a single substation, or a small generating unit. Many of these utilities have no dedicated supply chain or cybersecurity staff. They buy equipment in small quantities, so they have little leverage to demand ownership or component information from large manufacturers.

¹⁵ Nuclear Procurement Issues Corporation, *NUPIC*, <https://www.nupic.com/NUPIC/Home/Home.aspx>.

¹⁶ U.S. Nuclear Regulatory Commission, *Nuclear Procurement Issues Corporation (NUPIC) and Industry Interactions*, <https://www.nrc.gov/facilities-safety/new-reactors/how-we-regulate/regulatory-oversight/quality-assurance-for-new-reactors/nuclear-procurement-issues-corporation-nupic-and-industry-interactions>.

¹⁷ See generally 10 C.F.R. Part 21.

They also lack the capital to replace equipment ahead of schedule. In many cases, those customers are in rural and remote communities that already pay a high cost to be served.

We cannot responsibly estimate the effect on electricity rates until DOE determines which equipment and vendors are covered. Our survey does show the scale at stake. Members reported that replacing a single category of existing equipment can cost tens of millions of dollars and take years. Mitigating the same equipment costs a fraction of that and takes months. Whether EO 14421 imposes the first set of costs or the second will largely be decided by the implementation choices DOE makes now.

Compliance and enforcement mechanisms should be harmonized with existing federal regulations. (H-2)

As discussed above, APPA and LPPC share the Administration's and DOE's security concerns, and we support efforts to develop frameworks that will allow utilities to procure equipment that is both secure and affordable. To the extent that DOE concludes that regulatory measures are needed to reduce risk, those measures should be harmonized with existing regulations, particularly NERC's regulations. Establishing separate regulatory frameworks and separate compliance/enforcement mechanisms would impose undue burden on regulated entities.

Stage 1: the December 24 rule. By December 24, DOE can adopt a rule that operates on information that exists today, with responsible entities self-certifying compliance, consistent with the approach taken in response to EO 13920. The rule would prohibit acquisition, for new purchases, of equipment in the three designated categories that meets the two-element test described above, at the level of the original equipment manufacturer. That is the level described above in connection with scope, and a purchaser can require a representation to that effect, so the measure operates on records and contractual relationships that exist today.

We note candidly the limit of a prohibition at this level. Because the representation covers who manufactured the equipment, not only whose name it carries, it reaches equipment a covered foreign entity makes and another company sells. It does not reach the components and firmware inside the equipment, and that gap is what the second stage would close.

Stage 2: if DOE wants to go further. Reaching suppliers' suppliers, or IBRs and batteries in the aggregate, requires pieces that do not exist today. Someone must set the procedure a certifying entity follows and audit that it is followed, both by the certifiers and by the roughly 1,500 registered entities that buy covered equipment. Someone must also set the aggregate risk threshold for IBRs and batteries and obtain the equipment information from their owners. Utilities do not hold that information; it sits with independent power producers and behind power purchase agreements and third-party contracts. Each of these pieces should be risk-based, and each fits within an existing framework rather than a new one.

The legal path to development of such standards may be DOE's issuance of a Notice of Proposed Rulemaking (NPR) under section 403 of the Department of Energy Organization Act,

specifying what DOE seeks to achieve. A DOE NOPR may call for FERC to direct NERC to develop standards consistent with that scope. The NOPR may be as specific as thought necessary to reasonably accomplish the Administration's security objectives. NERC's work would be bounded by it: FERC's direction should state expressly that NERC is to implement DOE's scope, and not to expand what registered entities are audited against more generally.

We anticipate four NERC standards:

- An audit standard that implements DOE's objective by setting the procedure a certifying entity must follow, against which NERC audits the certifiers.
- A standard for purchasers, requiring that covered equipment be bought from a certified source or supported by the purchaser's own diligence, against which NERC audits registered entities.
- A standard directing owners of IBRs and batteries to disclose their equipment to their balancing authority. Because NERC already registers those owners, this standard could follow quickly after December 24 as the reporting requirement described above.
- A standard setting the aggregation risk threshold for IBRs and batteries for each balancing authority, using a defined methodology and data supplied by the equipment owners. Responsibility for verifying and mitigating that equipment would remain with its owners and operators, not with the balancing authority in whose area it operates.

Why NERC. There are several factors commending NERC as the institution best suited to develop these standards and oversee its compliance and enforcement. Through the development and implementation of its current suite of reliability standards, NERC has unequaled line of sight into the set of BES assets, which, if compromised, threaten the grid and the nation's economic vitality. It also maintains the compliance registry of the owners, operators, and users of the bulk-power system, roughly 1,500 entities before the IBR registrations described above.¹⁸ No other institution has that list, and a rule needs one to know whom it reaches. That expertise was applied in the development of Reliability Standard CIP-014 and the supply chain standard, CIP-013. Particularly in connection with the administration of CIP-013, NERC has developed expertise in understanding and reviewing supply chain risk and practices, of which EO 14421 is an extension.

Further, NERC has compliance and enforcement machinery, which, to APPA and LPPC's knowledge, DOE currently does not have. It bears emphasizing that APPA and LPPC's objective here is not to minimize compliance risk, but to ensure that real risks to the grid are effectively managed.

Industry builds it; the regulator audits it. Any program of this kind requires someone to audit compliance with it. In both precedents described above, that role sits with the regulator, which audits the process rather than performing the assessments itself.

¹⁸ FERC, *Commission Information Collection Activities (FERC-725)*, 87 Fed. Reg. 1746 (Jan. 12, 2022) ("Reviewing the NERC Compliance database, we determined the number of unique U.S. entities is 1,496").

The nuclear experience is instructive in a further respect. NUPIC was not created by the NRC. The requirement came first, and the industry then organized to meet it jointly, because no single licensee could audit every supplier. The NRC recognized the result rather than designing it.

We propose the same sequence here. DOE specifies what a certification must establish, NERC sets the procedure a certifying entity must follow, and DOE publishes the list of entities of concern. Industry then organizes to perform the work in the second stage, as the nuclear industry did. We are not asking DOE to build a certification body; we are asking for a rule that makes one possible.

Who does what. What NERC would do is set the audit standard and audit against it: that a certifying entity followed the procedure the standard sets, and that a responsible entity either relied on a certification or performed its own diligence. Both are records examinations of the kind NERC's regional entities conduct today in connection with CIP-013. The standard in each case is procedural. A certifying entity can evaluate only what the approved procedure permits it to reach, and a purchaser can rely only on what a certification states.

Neither should be held to a standard of certainty about origin that no party in the supply chain is able to deliver: a purchaser that reasonably relies on a valid certification or a supplier's representation, without knowledge of contrary information, should be treated as compliant if that information later proves inaccurate, with a reasonable period to address the equipment once it learns otherwise.

What NERC would not do is identify the entities that present the concern. That determination rests on intelligence and government records to which NERC has no access and in which it holds no expertise, and NERC has declined comparable list-maintenance roles in connection with CIP-013 and in the pending project addressing third-party cloud services. We do not suggest that position is mistaken. Nor would NERC audit supply chains.

What DOE would do is supply what only the federal government holds. DOE should publish one list: the vendors, product lines and firmware families it treats as presenting the concern. Within that list, DOE should identify those that share a common dependency, such as a common module or firmware family, and would be expected to fail together. Common dependency is one of the risks the list should capture, not the only one, and it is the one that makes the aggregation analysis for IBRs and batteries possible. The list is what a purchaser, a certifying entity, and an owner of installed equipment each check against.

Neither party can produce it alone: a certifying entity sees what is in the supply chain but cannot know which names are of concern, and DOE knows which names are of concern but does not see the chain. What is needed is not a list of approved vendors but an identification of those that present the concern, maintained jointly.

CONCLUSION

APPA and LPPC share DOE's goal of keeping foreign adversaries out of the bulk-power system. We also share DOE's view that the way to get there is through "practical, risk-informed, and administrable approaches." The recommendations in these comments are meant to make that possible, in two stages. By December 24, DOE can adopt a risk-based rule for the highest-impact facilities, limited to equipment that can affect grid operations and to what a purchaser can learn from its own supplier, with compliance self-certified. If DOE wants to go further, to suppliers' suppliers or to IBRs and batteries in the aggregate, we believe the pieces that requires would harmonize best with existing programs if built through NERC standards developed within the scope DOE sets. In both stages, rules for new purchases should be prospective, and installed equipment should be mitigated rather than replaced.