[6450-01-P]

This document is scheduled to be published in the Federal Register on 2026-09-09 and available online at **https://www.federalregister.gov/d/2026-18370**, and on **https://govinfo.gov**

DEPARTMENT OF ENERGY

[DOE-2026-HQ-2026-1123]

RIN 1901-AB79

Securing the United States Bulk-Power System

AGENCY: Office of Cybersecurity, Energy Security, and Emergency Response, Department of Energy.

ACTION: Request for information (RFI).

SUMMARY: Consistent with the Executive order of August 26, 2026, *Declaring a National Emergency to Secure the United States Bulk-Power System*, the Department of Energy (DOE or the Department) is seeking information from industry and other stakeholders to inform DOE actions to implement the Executive order. Specifically, DOE seeks information regarding the scope of covered equipment and transactions; risks associated with Covered Foreign Entities and foreign-produced bulk-power system electric equipment; supply chain, software, firmware, digital service, maintenance service, and remote-access practices; existing equipment and potential mitigation; licensing and prequalification; domestic manufacturing and secure replacement capacity; Federal procurement; and potential economic, reliability, safety, and small-entity impacts.

DATES: Written responses, data, and information are requested and will be accepted on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**. If you anticipate difficulty in submitting responses within that period, contact the person listed in **FOR FURTHER INFORMATION CONTACT** as soon as possible. DOE will hold a public meeting via webinar on Wednesday, September 16, 2026, from 3 to 4 p.m. EDT. See section III of this document, "Public Participation," for webinar registration information, participant instructions, and information about the capabilities available to webinar participants.

ADDRESSES: Interested persons are encouraged to submit responses using the Federal eRulemaking Portal at *www.regulations.gov* under docket number DOE-HQ-2026-1123. Follow the instructions for submitting responses. Alternatively, interested persons may submit responses, identified by "Bulk-Power System Executive Order RFI" and Docket No. DOE-HQ-2026-1123, by any of the following methods:

Email: BulkPowerEO@doe.gov. Include "Bulk-Power System Executive Order RFI" in the subject line of the message.

Postal Mail/Hand Delivery: Eric Rollison, Assistant Director, Technology Development, Office of Cybersecurity, Energy Security, and Emergency Response, U.S. Department of Energy, 1000 Independence Avenue SW, Washington, DC 20585-0121. If possible, please submit all items on a compact disc (CD), in which case it is not necessary to include printed copies.

No telefacsimilies (faxes) will be accepted. For detailed instructions on submitting responses and additional information, see section IV of this document. Instructions for submitting Confidential Business Information (CBI) are provided in section IV. Do not submit CBI through the Federal eRulemaking Portal.

Docket: The docket for this activity, which includes *Federal Register* notices, responses, comments, and other supporting documents/materials, is available for review at *www.regulations.gov*. All documents in the docket are listed in the *www.regulations.gov* index. However, some documents listed in the index, such as those containing information that is exempt from public disclosure, may not be publicly available.

The docket webpage can be found at *www.regulations.gov/docket/DOE-2026-HQ-2026-1123*. The docket webpage contains instructions on how to access all documents, including public comments, in the docket. See section IV of this document for information on how to submit responses through *www.regulations.gov*.

FOR FURTHER INFORMATION CONTACT: Eric Rollison, Assistant Director – Technology Development, U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, 1000 Independence Avenue SW, Washington, DC 20585-0121. Email: *BulkPowerEO@doe.gov*. Telephone: 202-586-1769.

SUPPLEMENTARY INFORMATION:

Table of Contents

I. Introduction

A. Background

The bulk-power system provides the electricity that supports United States national defense, vital emergency services, critical infrastructure, and the economy. Executive Order

(E.O.) 14421 of August 26, 2026, *Declaring a National Emergency to Secure the United States Bulk-Power System*, found that certain foreign actors are increasingly creating and exploiting vulnerabilities in the United States bulk-power system and that the rapid growth of advanced manufacturing, data centers, artificial intelligence, and defense production has increased the Nation's dependence on abundant, reliable electricity and magnified the consequences of a potential successful attack or supply disruption. 91 FR 55995 (Aug. 31, 2026) (E.O. 14421).

E.O. 14421 further found that minimal restrictions on acquisition or operation in the United States of foreign-produced bulk-power system electric equipment augment the ability of some foreign entities to create and exploit vulnerabilities in such equipment; for instance, such equipment might have digital backdoors built into their systems that allow a foreign country to access that equipment remotely. E.O.14421, Sec. 1. It also found that continued United States reliance on foreign sources of bulk-power system electric equipment with these potential national security vulnerabilities creates a supply chain vulnerability that could eliminate the supplies of these products in the United States as a result of disruptions in international trade or other causes. E.O. 14421, Sec. 1.

Based on these findings, E.O. 14421 declared a national emergency with respect to the threat to the bulk-power system in the United States and directed the Secretary of Energy (Secretary) to address transactions, existing equipment, mitigation, licensing, prequalification, and Federal procurement of such equipment. E.O.14421, Secs. 1 through 4. Consistent with the Department's commitment to public participation, DOE is soliciting views and information before developing measures to implement this directive.

B. Executive Order 14421

On August 26, 2026, the President issued E.O. 14421, *Declaring a National Emergency to Secure the United States Bulk-Power System*. The principal implementation elements of E.O. 14421 include the following:

(1) *Transactions involving foreign-produced bulk-power system electric equipment.* E.O. 14421 prohibits any acquisition, importation, transfer, or installation of foreign-produced bulk-power system electric equipment by any person, or with respect to any property, subject to the jurisdiction of the United States where the transaction involves any property in which any foreign country or a national thereof has any interest, including through an interest in a contract for the provision of the equipment; the transaction was initiated after the date of the Executive order; and the Secretary makes the determinations specified in section 2(a). E.O. 14421, Sec. 2(a). Those determinations encompass bulk-power system electric equipment and associated critical components, software, firmware, digital services, maintenance services, or remote-access capabilities designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a Covered Foreign Entity, where the transaction poses an undue or unacceptable risk described in E.O. 14421. E.O. 14421, Sec. 2(a)(i) through (ii).

(2) *Existing equipment.* For foreign-manufactured or operated bulk-power system electric equipment acquired or installed before the date of E.O. 14421, the Secretary may impose conditions on continued use, operation, maintenance, servicing, or updating, including requirements to identify, isolate, monitor, secure, disconnect, replace, or remove equipment. Before directing isolation, disconnection, replacement, or removal, the Secretary must consider effects on reliability, safety, the availability of secure replacements, and continuity of essential service, and may establish phased compliance. E.O. 14421, Sec. 2(b).

(3) *Mitigation, exceptions, licensing, prequalification, and anti-evasion*. The Secretary may design or negotiate measures to mitigate concerns and may make such measures a precondition to approval of a transaction or class of transactions. E.O. 14421 contemplated regulations, orders, directives, or licenses that may authorize conduct otherwise within a prohibition. It also authorized criteria and procedures for recognizing particular equipment and vendors as prequalified for future transactions, while providing that prequalification does not

limit the Secretary's authority to prohibit or otherwise regulate a transaction. Transactions that evade or avoid, have the purpose of evading or avoiding, cause a violation of, or attempt to violate a prohibition or requirement, and conspiracies to violate a prohibition or requirement, are prohibited. E.O. 14421, Sec. 2(c) through (f).

(4) *Implementation rules and existing-equipment recommendations*. E.O. 14421 directed the Secretary, within 120 days of its date and in consultation with other agencies, to publish rules or regulations implementing the Executive order, as needed. E.O. 14421, Sec. 3(b). It also directed the Secretary to identify bulk-power system electric equipment associated with Covered Foreign Entities that presents the risks described in the Executive order and to develop recommendations on ways to identify, inventory, isolate, monitor, or replace such items, taking into consideration overall risk to the bulk-power system. Rules and regulations issued pursuant to E.O. 14421 may also determine that particular countries or persons are a Covered Foreign Entity and identify persons owned by, controlled by, or subject to the jurisdiction or direction of a Covered Foreign Entity, exclusively for the purposes of the order. E.O. 14421, Sec. 3(b) through (c).

(5) *Federal procurement.* Within 180 days of the date of E.O. 14421, the Secretary, in consultation with the Federal Acquisition Regulation (FAR) Council and any other senior executive branch official the Secretary deems appropriate, must develop recommended revisions to the FAR to ensure that national security risks are adequately considered in Federal procurements concerning energy infrastructure and to prioritize acquisition of U.S.-manufactured energy infrastructure. E.O. 14421, Sec. 4(a) through (b).

When determining whether equipment is within the scope of E.O. 14421, consideration may also be given to associated software and firmware, remote-access capabilities, lifecycle maintenance and update mechanisms, and other supply chain dependencies that could present an unacceptable risk to the bulk-power system. Items not included in the list, or that have broader

application beyond the bulk-power system unrelated to the national security concerns identified in E.O. 14421, are outside the scope of the Executive order. E.O. 14421, Sec. 5(b).

C. Purpose and Scope of this Request for Information

DOE seeks public input to develop practical, risk-informed, and administrable approaches to implementing E.O. 14421. The Department is particularly interested in information from electric utilities and other asset owners and operators; independent power producers; equipment manufacturers; original equipment manufacturers; component and sub-tier suppliers; software and firmware developers; digital, cloud, maintenance, monitoring, and remote-access service providers; engineering, procurement, construction, integration, installation, testing, and repair firms; distributors and resellers; investors and insurers; labor organizations; standards development and conformity assessment organizations; trade associations; academic and research institutions; State, local, Tribal, and territorial governments; consumer representatives; and other interested parties.

Respondents need not answer every question. To the extent possible, respondents should identify the question number addressed; distinguish current practices from recommended approaches; identify the equipment, service, transaction, business model, or segment to which the response applies; provide quantitative data and explain assumptions; describe feasible alternatives; and identify reliability, safety, national security, competition, cost, schedule, workforce, or implementation considerations. Respondents may provide aggregated or anonymized examples where transaction-specific information is sensitive.

This request for information is issued solely for informational and planning purposes. It does not constitute a proposed rule, order, directive, license, or determination concerning any country, person, transaction, equipment, or vendor. Participation is voluntary, and responses do not bind DOE or the public. Please carefully read section IV regarding the public nature of submissions and the procedures for submitting CBI. Do not include classified national security

information, detailed exploit instructions, or other information whose public disclosure is restricted by law.

II. Request for Information

The Department seeks information responsive to the following questions. To the extent possible, respondents should provide supporting data, explain the basis for estimates, identify the period covered by the information, and note whether the response reflects a current practice, a planned practice, or a recommendation.

A. Scope, Definitions, and Covered Transactions

(A-1) Please identify the respondent's role or roles in the bulk-power system electric equipment market or supply chain, the types of equipment or services with which the respondent has experience, and the basis for that experience. Where relevant, identify the approximate size of the respondent, the geographic regions served, and whether the response reflects the perspective of an asset owner or operator, manufacturer, supplier, developer, service provider, integrator, installer, repair provider, distributor, purchaser, investor, insurer, standards body, governmental entity, or other stakeholder.

(A-2) Which equipment categories or applications in the Executive order's definition of "bulk-power system electric equipment" require further clarification to enable consistent compliance? What objective characteristics should DOE consider for utility-scale and other grid-connected inverters, battery energy storage systems (BESS), universal power systems (UPS) supporting critical infrastructure, small generators, backup generators, industrial control systems, and equipment used in facilities that combine transmission and distribution functions? Identify any equipment-specific voltage, capacity, connectivity, function, location, or criticality thresholds that would improve clarity without creating material security gaps.

(A-3) What criteria should DOE use to determine when a critical component, software, firmware, digital service, maintenance service, remote-access capability, is sufficiently "associated with" bulk-power system electric equipment to fall within the scope of a transaction

review or other implementation measure? Separately, when determining whether equipment itself is within the definition of "bulk-power system electric equipment," how should DOE consider associated lifecycle maintenance and update mechanisms and other supply chain dependencies that could present an unacceptable risk to the bulk-power system?

(a) Should this inquiry turn on whether the item or service can affect operation, protection, control, monitoring, availability, configuration, integrity, confidentiality, safety, or recovery of the equipment or the bulk-power system?

(b) How should DOE treat general-purpose hardware, commercial software, open-source software, telecommunications, cloud infrastructure, and enterprise services that support both bulk-power system and non-bulk-power-system functions?

(A-4) How should DOE distinguish items that have broader application beyond the bulk-power system and are unrelated to the national security concerns identified in E.O. 14421 from mixed-use items whose configuration, deployment, connectivity, or function creates a material bulk-power-system risk? What documentation is ordinarily available to make that distinction?

(A-5) For purposes of the definition of "foreign-produced," what facts should DOE consider when determining whether an article is manufactured, produced, or assembled in the United States?

(a) How should DOE treat final assembly, substantial transformation, domestic content, contract manufacturing, original design manufacturing, white-labeling, refurbishment, remanufacturing, repair, and incorporation of foreign critical components?

(b) What facts should DOE consider when determining whether software, firmware, digital services, maintenance services, or remote-access capabilities associated with such equipment were "designed, developed, manufactured, or supplied" by persons owned by, controlled by, or subject to the jurisdiction or direction of a Covered Foreign Entity?

(c) What records can manufacturers, importers, distributors, and purchasers reasonably provide to substantiate country of manufacture, production, or assembly?

(A-6) Are there transaction classes, equipment classes, or risk-based thresholds that DOE should prioritize for early implementation or, where consistent with E.O. 14421, address through categorical procedures? Explain the relevant factors, such as equipment criticality, deployment scale, voltage or capacity, network connectivity, remote-access capability, concentration of supply, replacement lead time, consequences of failure, or use in support of defense, emergency, or other critical loads. Describe safeguards needed to prevent evasion through segmentation, relabeling, or *de minimis* arrangements.

B. Covered Foreign Entities and Supply Chain Risk Management

(B-1) What commercially available data sources, supplier disclosures, corporate records, certifications, or third-party services are used to identify foreign ownership, control, jurisdiction, direction, or influence? Describe their accuracy, limitations, coverage, update frequency, cost, and treatment of privately held firms, trusts, investment funds, State-owned enterprises, and opaque ownership structures.

(B-2) How far into sub-tier supply chains can asset owners, vendors, and service providers reasonably trace ownership, manufacturing location, software and firmware provenance, and access rights for bulk-power system electric equipment? What materiality, criticality, or risk thresholds should govern the depth of tracing, and how should unknown or unavailable information be treated?

(B-3) Do energy sector asset owners, operators, manufacturers, vendors, and service providers conduct periodic enterprise risk assessments or cybersecurity maturity evaluations that address foreign ownership, control, jurisdiction, direction, or influence and supply chain risk? Describe the scope, frequency, governance, evidence, and remediation processes, including the treatment of access to company and utility data, product development, source code, research partnerships, sub-tier suppliers, and critical services.

(B-4) What governance of sub-tier vendors is currently used? Address procurement contract language, security requirements, audit rights, cost-schedule-performance metrics,

supplier scorecards, incident notification, location and ownership changes, integrator and installer controls, maintenance provider controls, and termination or transition rights. Which practices are effective, and what are the common gaps?

(B-5) What capabilities exist to provide and maintain software, firmware, and hardware bills of materials; track supply chain provenance and white-labeling; authenticate genuine components and updates; prevent tampering, unauthorized production, and counterfeits; and monitor sub-tier adherence to security requirements? Identify equipment categories for which such capabilities are mature, emerging, impracticable, or unavailable.

(B-6) What practices are used to secure software, firmware, digital services, maintenance services, and remote-access capabilities associated with bulk-power system electric equipment?

(a) Address secure development lifecycles, source code protection, reproducible or controlled builds, code signing, secure update mechanisms, vulnerability disclosure, patch validation, end-of-life support, escrow or continuity arrangements, and integrity verification.

(b) Address remote-access inventory, authorization, multifactor authentication, least privilege, time-limited access, session logging, monitoring, geographic restrictions, jump hosts, vendor credentials, emergency access, revocation, and the ability to disable remote access without impairing safe operation.

(c) Address telemetry, data collection, data residency, cloud hosting, license validation, digital rights management, remote monitoring, and vendor access to operational or configuration data.

(B-7) What information is available concerning vulnerability testing standards, independent product testing, penetration testing, compromise history, remediation timelines, and the effectiveness of mitigations for bulk-power system electric equipment and associated enterprise systems?

(a) How are vulnerabilities reported by researchers, vendors, asset owners, government entities, and other external parties received, validated, prioritized, remediated, and communicated?

(b) What records are maintained, for how long, and in what form?

(c) Which insecure-by-design or vulnerable communication protocols, services, or default configurations remain in use, cannot be disabled, or require compensating controls?

(d) What physical, logistical, role-based access, personnel screening, and insider-risk practices are used during manufacturing, shipping, installation, commissioning, maintenance, and repair?

(e) How do stakeholders participate in information-sharing and testing programs, and what barriers limit timely exchange of supply chain risk, vulnerability, and indicator information with other stakeholders and the Federal Government?

C. Risk Evaluation and Transaction Review

(C-1) How should DOE evaluate consequence and system criticality of equipment identified as part of E.O. 14421? Within your response, address, as applicable, the equipment's function; location; voltage or capacity; role in protection, control, restoration, blackstart, or defense-critical service; redundancy; substitutability; network connectivity; remote-access capability; number and concentration of deployments; common-mode exposure; time to detect and recover; availability of spares; and potential cascading, regional, economic, safety, or national defense effects.

(C-2) What evidence should DOE consider when evaluating technical and supply chain risk? Address vendor and product history; ownership and control information; design and development practices; production and testing records; certifications; independent laboratory results; vulnerability and incident history; software and firmware provenance; update and remote-access architecture; secure development practices; supply concentration; geopolitical and logistics exposure; and the quality, recency, and verifiability of evidence.

(C-3) What factors best measure the risk of supply disruption? Identify equipment or critical inputs for which single-source or concentrated supply, limited domestic capacity, unusually long lead times, scarce testing capability, unique intellectual property, restricted technical data, specialized transportation, critical minerals or materials, or dependence on foreign maintenance and updates creates material risk. Explain how such risks vary over the equipment lifecycle.

D. Existing Equipment and Mitigation

(D-1) Which data fields do asset owners and operators currently maintain, such as manufacturer, model, serial number, production facility, country of manufacture or assembly, supplier, integrator, installation date, firmware and software versions, component provenance, network connectivity, remote-access pathways, service provider, support status, and replacement lead time?

(a) For installed equipment, what information is commonly unavailable, and what reasonable methods can be used to estimate or validate origin, ownership, access, and risk?

(D-2) For foreign-manufactured or operated existing equipment that may present one or more of the risks described in the Executive order, what measures are technically and operationally available to identify, isolate, monitor, secure, disconnect, replace, or remove the equipment? How should DOE compare the effectiveness, limitations, implementation time, cost, verification methods, and residual risk of these measures, including network segmentation, monitoring, access restrictions, firmware replacement, removal of remote access, vendor transition, spare strategies, and physical controls.

(D-3) What reliability, safety, availability-of-secure-replacement, and continuity-of-essential-service factors should DOE evaluate before directing isolation, disconnection, replacement, or removal? What technical studies, operating criteria, contingency analyses, or certifications should support that evaluation?

(D-4) How should DOE monitor and verify implementation and continuing effectiveness of measures applied to existing equipment? What reporting, testing, inspection, attestation, independent assessment, change-notification, and recordkeeping approaches are practical? Describe mechanisms that would allow DOE to obtain useful information while protecting CBI, sensitive security information, and system-specific details. Non-sensitive case studies and aggregate data are encouraged.

E. Licensing, Mitigation Measures, and Prequalification

(E-1) What information should a license application contain, who should be responsible for submitting and certifying it, and what review timelines and completeness criteria would be workable? How should DOE treat pending procurements, imminent outages, emergency restoration, unavailable secure replacements, or other time-sensitive circumstances?

F. Domestic Manufacturing, Secure Replacements, and Federal Procurement

(F-1) Which categories of bulk-power system electric equipment, critical components, software, firmware, production tooling, testing capability, critical minerals, or other supply chain inputs are materially dependent on foreign sources or concentrated in a limited number of countries or suppliers? Provide, where available, aggregate information on source concentration, domestic and foreign capacity, lead times, substitution constraints, and the causes of dependence, such as lack of domestic capability, cost, quality, intellectual property, specialized materials, workforce, or testing infrastructure.

(F-2) What is the current and reasonably anticipated U.S. manufacturing, assembly, integration, repair, testing, and service capacity for major categories of bulk-power system electric equipment and critical components? Identify capacity constraints, minimum efficient scale, capital and permitting needs, workforce needs, expected time to expand capacity, and the demand certainty required to support investment.

(F-3) For equipment that may require replacement or restricted sourcing, what secure alternatives are available or under development? Address technical equivalence, interoperability,

certification, footprint and civil works, control integration, software and firmware compatibility, warranty and support, lead time, lifecycle cost, and the ability to maintain reliability and continuity of essential service during transition.

(F-4) How can Federal procurement prioritize U.S.-manufactured energy infrastructure while preserving competition, reliability, safety, quality, interoperability, timely delivery, and value? Identify appropriate transition periods, exceptions, waivers, alternate-source requirements, or emergency procedures and the criteria that should govern them.

(F-5) What additional actions could improve the availability and resilience of secure supply? Address long-term demand signals, aggregated procurement, advance purchase commitments, strategic spares or reserves, mutual assistance, standardization, modularity, interoperability, repair capability, domestic testing facilities, workforce development, information sharing, coordination between Federal and non-Federal purchasers, and other market or policy mechanisms. Describe potential benefits, costs, risks, and implementation lead times.

G. Economic and Regulatory Analysis

(G-1) What are the estimated one-time and recurring costs of developing, implementing, and periodically revising compliance plans and procedures associated with E.O. 14421 and potential DOE implementation measures?

(a) Evaluating applicability and requirements.

(b) Developing supply chain documentation, ownership and control evaluations, risk assessments, inventories, and internal review processes.

(c) Implementing new supplier qualification processes, contractual provisions, audits, testing, monitoring, training, and change-notification processes.

(d) Preparing and supporting transaction reviews, license applications, mitigation agreements, prequalification submissions, records retention, and responses to information requests.

(e) Identifying, isolating, monitoring, securing, disconnecting, replacing, or removing existing equipment.

(f) Other compliance, legal, engineering, cybersecurity, reliability, outage, financing, or administrative costs.

(G-2) Provide cost estimates, where possible, by respondent type and size, equipment category, transaction type, and implementation alternative. Identify labor hours and wage assumptions, capital costs, third-party fees, testing costs, inventory and carrying costs, outage or downtime costs, schedule effects, and the expected frequency of recurring activities.

(G-3) How could prohibitions, transaction reviews, licensing, mitigation, prequalification, domestic manufacturing preferences, or existing-equipment measures affect equipment prices, lead times, supplier concentration, competition, innovation, financing, insurance, warranties, contractual risk allocation, maintenance support, and availability of secure equipment and services? Identify equipment categories and market segments most likely to be affected.

(G-4) What reliability, safety, resilience, and continuity-of-essential-service costs or benefits could result from different implementation approaches? Include effects associated with delayed projects, forced outages, accelerated replacement, reduced access to vendor support, increased spare inventories, diversification of supply, improved security, and reduced likelihood or consequence of disruption.

(G-5) What benefits should DOE consider and, where possible, quantify? Address avoided or reduced risks of sabotage, subversion, unauthorized access, malicious remote action, supply disruption, cascading outages, emergency response, public health and safety impacts, economic losses, and national defense impacts. Identify data, models, scenarios, or proxies that could support estimation without requiring disclosure of sensitive system information.

(G-6) What unique challenges could E.O. 14421 and potential DOE implementation measures present to small businesses and other small entities? Address access to ownership and

provenance information, bargaining power with large suppliers, certification and testing costs, legal and technical expertise, minimum order quantities, long lead times, access to capital, participation in prequalification, and the ability to replace or mitigate existing equipment. What flexibilities could reduce disproportionate burden while maintaining security?

(G-7) What regulatory alternatives, thresholds, sequencing, phased compliance approaches, safe transition mechanisms, standardized forms, shared services, or technical assistance could achieve the objectives of E.O. 14421 with lower cost or burden? Describe potential effects on consumers, electricity rates, regional markets, rural and remote systems, publicly owned and cooperative utilities, and the broader economy, and explain the basis for any quantitative estimates.

H. Implementation, Information Sharing, and Other Matters

(H-1) What technical assistance, pilot programs, voluntary measures, templates, model contract clauses, data standards, or stakeholder engagement would help asset owners, manufacturers, vendors, and service providers prepare for implementation?

(H-2) Please identify any additional issue relevant to DOE's implementation of E.O. 14421 that is not addressed above and provide specific recommendations and supporting information.

(H-3) DOE seeks information about whether and how industry standards and/or third-party laboratories and certification bodies can be leveraged to implement E.O. 14421, limit the U.S. government role in initial execution, and maintain industry flexibility.

III. Public Participation

A. Participation in the Webinar

The time and date for the webinar meeting are listed in the **DATES** section at the beginning of this document. Webinar registration information, participant instructions, and information about the capabilities available to webinar participants will be published on CESER's webpage here: *https://www.energy.gov/ceser/office-cybersecurity-energy-security-and-*

emergency-response. Participants are responsible for ensuring their systems are compatible with the webinar software.

B. Conduct of the Webinar

DOE will be hosting an informational webinar to assist the public in responding to this RFI. A designated Federal Officer will preside at the webinar. A transcript of the webinar will be included in the docket, which can be viewed as described in the *Docket* section at the beginning of this document.

IV. Submission of Responses

DOE invites all interested parties to submit in writing by the date specified in the **DATES** section of this document, responses and information on matters addressed in this request. To the extent possible, please reference the question number addressed in each response.

Submitting responses through www.regulations.gov. The *www.regulations.gov* website requires you to provide your name and contact information. Your contact information will be viewable to DOE staff only. Your contact information will not be publicly viewable except for your first and last names, organization name (if any), and submitter representative name (if any). If your response is not processed properly because of technical difficulties, DOE may use this information to contact you. If DOE cannot read your response due to technical difficulties and cannot contact you for clarification, DOE may not be able to consider your response.

Your contact information will be publicly viewable if you include it in the response or in any documents attached to the comment. Any information that you do not want to be publicly viewable should not be included in your response or in any document attached to your comment. If this instruction is followed, persons viewing responses will see the submitter information made public by the portal, correspondence containing responses, and any documents submitted with the responses.

Do not submit through *www.regulations.gov* information for which disclosure is restricted by statute, such as trade secrets and commercial or financial information (referred to in

this notice as CBI). Responses submitted through *www.regulations.gov* cannot be claimed as CBI, and submission received through the website will waive any CBI claim for the information submitted. For instructions on submitting CBI, see the Confidential Business Information section.

DOE processes submissions made through *www.regulations.gov* before posting. Normally, responses will be posted within a few days of submission. However, if large volumes of responses are being processed, your response may not be viewable for several weeks. Please keep the tracking number that *www.regulations.gov* provides after you have successfully uploaded your response.

Submitting responses by email, hand delivery, or postal mail. Responses and documents submitted by email, hand delivery, or postal mail will also be posted to *www.regulations.gov*. If you do not want your personal contact information to be publicly viewable, do not include it in your response or any accompanying documents. Instead, provide your contact information on a cover letter. Include your first and last names, email address, telephone number, and optional mailing address. The cover letter will not be publicly viewable as long as it does not include any information responsive to the request for information.

Include contact information each time you submit responses, data, documents, or other information to DOE. If you submit via hand delivery or postal mail, please provide all items on a CD, if feasible, in which case it is not necessary to submit printed copies. No faxes will be accepted.

Responses, data, and other information submitted electronically should be provided in PDF (preferred), Microsoft Word, Microsoft Excel, or text file format. Provide documents that are not secured, are written in English, and are free of defects or viruses. Documents should not contain special characters or any form of encryption and, if possible, they should carry the electronic signature of the author.

Campaign form letters. Please submit campaign form letters through the originating organization in batches of between 50 and 500 form letters per PDF, or submit one form letter with a list of supporters' names compiled into one or more PDFs. This practice reduces processing and posting time.

Confidential Business Information. Under 10 CFR 1004.11, a person submitting information that the person believes to be confidential and exempt by law from public disclosure should submit by email two well-marked copies: one copy marked "confidential," which includes all information believed to be confidential, and one copy marked "non-confidential" with the information believed to be confidential deleted. Submit both copies to *BulkPowerEO@doe.gov* with the subject line "CBI - Bulk-Power System Executive Order RFI - Docket No. DOE-HQ-2026-1123." DOE will make its own determination regarding the confidential status of the information and will treat the information according to that determination.

It is DOE's policy that all responses may be included in the public docket, without change and as received, including personal information provided in the responses, except information DOE determines is exempt from public disclosure. Do not submit classified information or other information whose public disclosure is prohibited by law.

IV. Approval of the Office of the Secretary

The Secretary of Energy has approved publication of this request for information.

Signing Authority

This document of the Department of Energy was signed on September 4, 2026, by Andrew McClure, Director, Office of Cybersecurity, Energy Security, and Emergency Response, pursuant to delegated authority from the Secretary of Energy. The document with the original signature and date is maintained by DOE. For administrative purposes only, and in compliance with requirements of the Office of the Federal Register, the undersigned DOE Federal Register Liaison Officer has been authorized to sign and submit the document in electronic format for

publication as an official document of the Department of Energy. This administrative process does not alter the legal effect of the document upon publication in the Federal Register.

Signed in Washington, DC, on September 4, 2026.

Jennifer Hartzell,
Alternate Federal Register Liaison Officer,
U.S. Department of Energy.

[FR Doc. 2026-18370 Filed: 9/8/2026 8:45 am; Publication Date: 9/9/2026]