

Mike Davin
Senior Director, Energy and Resources Policy

Christopher Phalen
Vice President, Domestic Policy

October 9, 2026

Mr. Andrew McClure
Director
Office of Cybersecurity, Energy Security, and Emergency Response
U.S. Department of Energy
1000 Independence Avenue SW
Washington, DC 20585-0121

**RE: Comments of the National Association of Manufacturers on DOE's Request
for Information on the Bulk-Power System Executive Order (Docket No.
DOE-HQ-2026-1123, Sept. 9, 2026)**

Dear Director McClure:

The National Association of Manufacturers respectfully submits these comments in response to the Department of Energy's ("DOE" or "the agency") request for information ("RFI") *Securing the United States Bulk-Power System*. The NAM appreciates the opportunity to submit feedback in response to the RFI and the DOE's commitment to considering industry feedback as it finalizes implementation guidance.

The NAM is the voice of the manufacturing community and the leading advocate for a policy agenda that supports and empowers the 13 million people who make things in America. As the largest manufacturing association in the U.S., the NAM's membership includes businesses of all sizes, across all industrial sectors, and in all 50 states. Manufacturers collectively contribute \$3.2 trillion to the U.S. economy—and right-sized, commonsense regulations are critical to sustaining the manufacturing strength that underpins our nation's prosperity.

To ensure continued economic growth and the expansion of domestic manufacturing, it is essential that the electric grid be modernized and hardened against natural and man-made disasters. According to the NAM's Q3 2025 Manufacturers' Outlook Survey, 86% of manufacturers support policy efforts to streamline improvements to the grid.¹ The United States needs strong production of and access to all types of energy as well as significant expansions of and improvements to its electric generation, transmission and distribution infrastructure.

While manufacturers in the United States have made significant investments in the domestic production of components and equipment, it is clear that we must continue to modernize to address growing domestic needs and to ensure any security vulnerabilities are addressed. At the same time, expanding domestic capabilities across the supply chains supporting the bulk-power system will take time to reach fruition, and not all equipment and components are currently available at the necessary specifications and scale from U.S. suppliers. The agency should give due weight to the national security risks of regulatory actions that could create significant unintended supply chain disruptions and materially impair the competitiveness and

¹ Victoria Bloom, "NAM Manufacturers' Outlook Survey, Third Quarter 2025," Sept. 16, 2025. See link: https://nam.org/wp-content/uploads/securepdfs/2025/09/NAM_Q3_2025_Outlook_Write_Up.pdf.

strength of American industry. If not carefully designed, actions intended to strengthen national security and reshore industrial supply chains could have the opposite effect.

Given that the United States is facing a once-in-a-generation demand to bring new power generation onto the nation's electric grid, manufacturers believe it is critical for the administration to take the following considerations into account to help clarify the full scope and purpose of this executive action for manufacturers. This will ensure there are no disruptions to our sector's work to achieve energy dominance, grid reliability, and affordability for all Americans.

I. Manufacturers Must Maintain Their Ability to Advance Grid Reliability, Energy Affordability, and Supply Chain Security

Manufacturing growth and investment in the United States depend on ensuring access to and delivery of affordable, abundant, and reliable energy. Sufficient generation of all types of energy allows our industry to meet demand and innovate, build, and grow domestically. While manufacturers strongly support national security goals and the modernization of the U.S. electrical grid, imposing strict sourcing requirements or import restrictions on critical energy equipment will severely undermine grid reliability, increase costs, and impede the grid and the manufacturing sector's growth objectives.

Manufacturers have made significant investments in the domestic production of components and equipment that allow for the reliable generation and transmission of this energy. However, certain materials, equipment, and parts have little to no domestic production, particularly at the necessary specifications and grades, and so our industry must leverage international partnerships to meet the moment. Any effort to protect national security through import restrictions must also consider the impacts on grid reliability, as the two issues are intertwined.

Fulfilling the president's vision of a modern and robust grid, which manufacturers fully support, would be severely delayed or hampered if manufacturers were required to source solely from domestic supply chains. Modern manufacturing depends upon integrated global supply chains that leverage regional specializations, technical expertise, and production capabilities developed over decades. For multinational manufacturers, secure supply chains often incorporate inputs and components sourced from multiple countries, even when final products are designed, developed, and manufactured in the United States. A regulatory framework that recognizes these realities while focusing on actual security risks would better support both national security objectives and domestic manufacturing growth.

For example, restricting the import of certain gas turbines and generator equipment would decrease the likelihood that manufacturers could expand factory output in the future. Ambiguity regarding implementation of this executive order, combined with the tariff costs of importing necessary machinery and equipment, is also already impacting recent or imminent purchase orders for the equipment needed to boost grid modernization. Manufacturers are working to diversify sources for certain key components, but new suppliers must complete a lengthy certification process to ensure compatibility, efficacy, and conformance with specifications.

Without clarification, the executive order could also result in indirect negative consequences for other sectors of the manufacturing economy. Our nation's electrical utilities are leading the way in providing reliable energy to power the growth of manufacturing. Without clarification around sourcing requirements and supply chain tracking, these utilities would be forced to shift funding away from traditional investment pathways or expend additional resources on compliance rather

than investing in their systems to provide reliable and affordable electricity. Supply chain decisions for grid materials are often jointly governed by utilities and equipment manufacturers, making rapid sourcing changes difficult and potentially disruptive. The DOE should carefully explore options for coordinated transition planning where compliance actions cross over between utility and manufacturer ownership boundaries.

Additionally, there are manufacturers that make products, like transformer fluid, that improve the operability of bulk-power system equipment that would be adversely impacted by restrictions on the importation of critical grid equipment. With fewer transformers being imported into the United States due to the proposed restrictions, there will be fewer opportunities to sell their product, resulting in unused inventory or production cuts. The consequences for grid and economic security cannot be ignored and should be taken into account as the DOE works to finalize its guidance.

To protect national security while maintaining grid reliability and supporting manufacturing growth, manufacturers request that the administration be more explicit about how industry will be required to comply.

II. Manufacturers Need Clear Guidance to Invest in Grid Security and Support Grid Expansion

Manufacturers require predictability and up-to-date regulations to inform long-term business and investment decisions that involve significant capital expenditures to deliver on projects. With the growth in electrification over the past decade, new and advanced grid equipment and components are in high demand. For example, in 2025, power and distribution transformers saw demand surge by 116% and 41%, respectively.² According to the DOE's own data, distribution-transformer lead times can stretch to one to two years or longer, with large-transformer lead times stretching up to three to four years.³ Given the difficulty in obtaining this equipment, any restrictions on their importation through valid purchase orders or on their current use would pose immediate challenges to maintaining grid reliability.

Manufacturers seek clarification regarding key elements of the executive order, including questions around the scope and scale of the restrictions, how certain aspects of the bulk-power system will be defined, how existing equipment operating on the grid should be treated and if it would need to be replaced, how existing purchase orders for equipment are impacted, what the true deadlines for compliance are, and how far in the supply chain manufacturers will need to determine and document compliance. Clear and unambiguous federal guidance would help avoid uncertainty and unintended consequences that would otherwise impede manufacturing growth in the United States.

a. Ripping and Replacing Equipment Would Pose Major Challenges to Grid Reliability and Increase Energy Costs

The NAM opposes any guidance that would place restrictions on existing equipment or any requirements that would push for the removal and replacement of existing equipment on the

² Wood Mackenzie, "Power Transformers and Distribution Transformers Will Face Supply Deficits of 30% and 10% in 2025," August 14, 2025. See link: <https://www.woodmac.com/press-releases/power-transformers-and-distribution-transformers-will-face-supply-deficits-of-30-and-10-in-2025/>.

³ U.S. Department of Energy, *Distribution Transformer Convening Webinar* (Mar. 5, 2026). DOE reported that the most recent underlying data, from 2024, showed distribution-transformer lead times of one to two years or longer and large-transformer lead times of up to three to four years.

grid. We also encourage the DOE to establish transition protection for projects that completed supplier selection, financing, permitting, studies, detailed design, or major equipment integration before the implementing regulations are issued, even if a final purchase order has not yet been placed.

Should the DOE ultimately make the determination that existing equipment would need to be replaced with compliant equipment, then we would urge the Department to conduct a thorough risk assessment before mandating removals rather than broadly applying restrictions across entire equipment classes or technologies. There must be a legal process in place before any potential mitigative actions are taken. These assessments should focus on areas of the highest risk and outline criteria that would be applied for equipment security.

This process would be a costly endeavor that would be lengthy and unpredictable, while ultimately increasing energy prices for consumers and undermining grid reliability.

b. DOE Must Clarify the Scope and Criteria for Determining Equipment Restrictions

When determining the criteria for applying security restrictions, we recommend that the DOE clarify that its focus is solely on equipment that is connected to or can directly affect the operation of a bulk-power transmission network. As the executive order reads, the equipment categories could include hardware that is used inside manufacturing facilities that have no connection to the bulk-power system. The restrictions could also be interpreted to apply to co-generation, behind-the-meter, and low-voltage equipment that only supports downstream load, does not significantly export to the grid, and does not provide black-start, protection, control, restoration, or other grid reliability functions. There are also questions about the executive order's application to equipment that operates above and below the 69 kV threshold.

As the administration's intent is to specifically address cybersecurity vulnerabilities in the bulk-power system, manufacturers request clarity regarding the kV above which such equipment would be subjected to coverage under the executive order and similarly requests that the restrictions only apply to equipment that is deployed on the bulk-power system, and not equipment that is deployed behind-the-meter, for low-voltage distribution, used for co-generation, or is unconnected to the grid and in use at a manufacturing facility. In providing this clarification, the DOE also needs to establish a process to certify whether equipment is actually deployed on the bulk-power system or serves the broader electrical system in a different capacity. Equipment incapable of causing bulk-power system instability, cascading outages, loss of transmission functionality, or other measurable reliability impacts should be excluded.

Rather than applying restrictions to entire categories of bulk-power system electric equipment originating from a country of concern, the DOE should judiciously consider imposing restrictions only on high-risk products, components and technologies. The potential unintended consequences of wholesale category bans, without recognizing actual relation to and integration with critical grid nodes, would be staggering. Such a judicious approach, keeping in mind actual connectivity and prophylactic measures taken, could include bulk-power system electric equipment whose software comes from a country or entity of concern, whose trustworthiness has not been adequately improved by risk-mitigation measures⁴ and whose compromise would demonstrably weaken the bulk-power system's reliable support of the economy, human health and safety and national defense of the United States. For example, the point of cyber

⁴ See section III below about cyber frameworks.

compromise is not the turbine or transformer itself, but the operational technology (OT) components that monitor and control that turbine or transformer, and whose software may contain vulnerabilities if their risk is not properly mitigated. Focusing restrictions on the software rather than the entire equipment would appropriately focus companies' due diligence and software assurance lifecycle management on points of actual risk and create space in the implementation guidance for risk-mitigation measures.

To that end, the NAM urges the DOE to work closely with industry stakeholders to identify which categories of bulk-power system equipment, associated software, firmware, digital services, and critical components have the technical capability for remote connectivity and operational control, and which do not. A connectivity- and control-based framework would allow the DOE to focus regulatory scrutiny on higher-risk technologies that could facilitate unauthorized access, malicious remote action, or operational disruption, while avoiding unnecessary restrictions on products and components that lack such capabilities and therefore present materially lower cybersecurity and national security risks.

c. Supply Chain Sourcing Requirements Must be Workable and Explicit

Final guidance must also provide clarity around supply chain sourcing and tracking. To ease the costs of compliance and the burdens placed on manufacturers that are seeking to comply with any new restrictions, the DOE should clarify to which supply chain tier, and for what critical components, companies must track and verify. If equipment is manufactured in the United States but includes de minimis subcomponents or materials that were indirectly sourced from a restricted country, that piece of equipment should not be targeted for restrictions or removal. Any sourcing concerns should be addressed at the direct supplier level in the form of restricted suppliers and specific manufacturing locations to support specific reviews and actions, rather than a country-wide embargo or restriction. The DOE should also work to ensure information around the sourcing of components is kept confidential as publicizing this information can create advantages and disadvantages for suppliers in the marketplace, as these supply chains themselves are proprietary.

III. Leveraging Existing Cyber Frameworks and Avoiding Duplication to Ensure the Security of America's Grid

The rapid expansion of interconnected technologies has driven a related rise in cybersecurity threats. This concern has prompted industry and the federal government to develop standards, frameworks, and regulatory regimes to manage cyber supply chain risk. Manufacturers have engaged heavily in efforts to detect and prevent risks to the grid to both protect the provision and growth of utility services and to bolster national security. Before issuing new requirements and restrictions, manufacturers encourage the DOE to examine existing frameworks that could be built upon or applied to this context.

Relevant frameworks include policies developed by DOE's Office of Cybersecurity, Energy Security, and Emergency Response ("CESER") and the National Institute of Standards and Technology ("NIST") Special Publication 800-161 Revision 1, including the November 1, 2024

update,⁵ and the NIST Cybersecurity Framework 2.0.⁶ Additional relevant frameworks also include the International Organization for Standardization and International Electrotechnical Commission ("ISO/IEC") 27036 series⁷ and applicable North American Electric Reliability Corporation ("NERC") Critical Infrastructure Protection ("CIP") supply-chain requirements.⁸

The DOE should accept equivalent evidence when it addresses the same risk. For example, a manufacturer should not be required to repeat substantially identical reviews for multiple federal programs. Those reviews may address supplier ownership, software provenance, remote access, or cybersecurity. DOE recognition of equivalent evidence should not be treated as changing a manufacturer's registration status under NERC's separate registration criteria.

In addition, the rising number of constraints on how companies can secure their bulk-power equipment could further impact efforts by U.S. companies to build up domestic capacity. We recommend providing clarity on how these requirements would overlap with other existing regulations or rulemakings, including the addition of foreign-produced power inverters to the Federal Communication Commission's (FCC) Covered List on July 28 and the expansion of the Uyghur Forced Labor Protection Act (UFLPA) Entity List on July 31. As one example, the FCC clarified on August 20 that power inverters eligible for section 45X provisions are not under the scope of its Covered List, but that same inverter could be captured for restrictions under the bulk-power systems EO.

The DOE should also account for the fact that in 2025, Congress amended section 45X to incentivize the production of certain products. Some of those products (e.g., battery cells used in battery energy storage system applications) may also be subject to the requirements DOE promulgates here. Congress defined "material assistance from prohibited foreign entities" and disqualifies products from the tax incentive where such assistance rises above defined thresholds. Congress likewise codified detailed definitions for Prohibited Foreign Entity and related terms. Here, DOE must ensure the agency does not prohibit products and services which Congress just last year decided to incentivize. Such policy incoherence would undercut the investments made by U.S. companies in reliance on that legislation.

Finally, it is important for DOE to address precisely the scope of the terms "undue risk" and "unacceptable risk" from the executive order. Manufacturers believe that existing critical infrastructure risk management practices should be updated for the specific risks cited in the order and gaps identified before a sweeping new regulatory framework is created. The specific risks mentioned in the order ("sabotage, subversion, unauthorized access, malicious remote action, or supply disruption") should be DOE's primary focus as it considers responses to the RFI. The Department should start by defining "undue risk" in terms of gaps where existing risk management best practices may be insufficient, and cannot be updated in consultation with industry, such that stronger interventions may be needed. Defining these key terms carefully and

⁵ National Institute of Standards and Technology, *NIST SP 800-161r1-upd1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* (updated Nov. 1, 2024), DOI: 10.6028/NIST.SP.800-161r1-upd1.

⁶ National Institute of Standards and Technology, *Cybersecurity Framework 2.0* (Feb. 2024). Its Govern, Identify, Protect, Detect, Respond, and Recover functions provide a common cybersecurity framework that DOE can recognize while preserving DOE-specific national-security requirements.

⁷ International Organization for Standardization and International Electrotechnical Commission, *ISO/IEC 27036 series, Information Security for Supplier Relationships*. The series provides recognized supplier-security governance and contractual controls.

⁸ North American Electric Reliability Corporation, Reliability Standard CIP-013-2, *Cyber Security - Supply Chain Risk Management*. NERC lists CIP-013-2 as mandatory and subject to enforcement and CIP-013-3 as subject to future enforcement, with a U.S. effective date of October 1, 2028. Project 2025-06 continues to develop CIP-013-4, which is in draft status and not an enforceable Reliability Standard.

precisely is the surest way to ensure the rulemaking results in non-disruptive standards that apply only to grave risks that cannot otherwise be mitigated.

The NAM recommends avoiding unnecessary and confusing duplication wherever possible and ensuring consistent guidance across agency rulemakings.

IV. Transparent and Substantive Regulatory Processes are Necessary to Ensure Durability and Industry Buy-In

Manufacturers have consistently supported workable regulatory processes that provide predictability to industry while also being good stewards to their communities and to the United States. As we noted earlier, our industry requires predictable licensing and prequalification procedures before companies can make major capital commitments. At the same time, we also believe maintaining national security is paramount to our ability to grow and compete. Unfortunately, it is unclear how the department will proceed with finalizing implementation guidance and providing a reasonable amount of time for manufacturers to make transition plans. There is concern that industry will not have sufficient time to redesign, rebid, or replace equipment, which would increase uncertainty around the grid's ability to maintain its protections against cyber threats. Manufacturers strongly caution against finalizing any guidance that results in truncated and unrealistic transition timelines, and similarly urges the Department to closely consult industry to understand how potential decisions would supply chain transition planning.

Manufacturers also recommend an expedited determination process through which they can obtain a binding decision regarding equipment and components before making a major procurement commitment.

We urge the department to formalize a public process that will allow for additional stakeholder input around these matters before the implementation guidance is finalized at the end of the year.

V. Outstanding Questions That Require Continuous Dialogue Between the Administration and Manufacturers

While manufacturers appreciate the DOE's willingness to accept direct feedback, there remain several outstanding questions that industry will need the administration to answer.

- *What is the official regulatory process that the DOE will follow to complete implementation of the executive order?* Our members believe that the DOE should commit to a transparent administrative process with formal notice-and-comment opportunities, allowing for a minimum of 45 days to provide written feedback to proposed guidance and a public meeting. There must also be an adequate phase-in period to ensure manufacturers can comply with the new restrictions and procedures.
- *How many supply chain tiers must manufacturers go through to determine compliance with the executive order?* There would be substantial costs and the need to deploy additional dedicated resources if manufacturers are expected to trace each subcomponent and material that enters their product's supply chain to determine if they are at risk of falling out of compliance with the new guidelines. For example, if there are subcomponents that are used in bulk-power equipment that are not relevant to cyber

vulnerabilities, would that directly impact compliance? It would be helpful if the DOE established criticality and materiality thresholds rather than requiring identification of every minor component and material.

- *How will this executive order determine criticality for the U.S. grid and what exactly is in scope?* As previously discussed, it is unclear if the scope of the executive order only encompasses grid-related equipment. It is not clear if behind-the-meter generators and microgrids, which can be used as back-up power sources for advanced manufacturing facilities and data centers, are deemed essential or are within the order's scope. There are also questions over whether commercial producers of energy are key targets or if commodities for direct purchase are also in scope. Finally, there needs to be clarity around the order's application to the software and hardware that are used to make the bulk-power systems equipment that would be restricted.
- *How will the DOE define "designed" and "developed?"* It is crucial that DOE define these terms in a way that allows the U.S. to maintain critical supply chains with respect to components that pose no national security risk. Generally, the NAM believes that "designed" and "developed" should apply to the overall system, such that components that are part of a system designed or developed by non-Covered Entities are exempt. Specifically, manufacturers believe the definition of "designed" should focus on the entity exercising primary authority over engineering specifications, cybersecurity architecture, and functional design decisions. Additionally, "developed" should refer to the entity primarily responsible for creating the core software or hardware product, not where minor modifications, maintenance, testing, or technical support occurs. Given the global footprint of many manufacturers, activities such as customer support, quality control testing, component sourcing, or engineering support should not cause equipment to be considered "designed" or "developed" in a particular country or region. The DOE should keep the focus on any actual and significantly substantive control by a Covered Foreign Entity and avoid sweeping in secure U.S. designs that happen to draw on limited amounts of global professional talent.
- *What is the approach towards Defense Federal Acquisition Regulation recommendations?* Manufacturers urge the DOE to coordinate its procurement recommendations with the Federal Acquisition Regulation and the Defense Federal Acquisition Regulation Supplement.
- *How will the DOE address existing business activities and contracts that were signed or modified to govern the procurement of equipment?* Manufacturers urge the department to confirm that a change order, delivery extension, quantity adjustment, assignment, innovation, or other ordinary contract modification will not convert a pre-existing transaction into a new covered transaction unless it materially changes the manufacturer, equipment, country of production, digital functionality, or security risk. There should also be a safe harbor for equipment covered by binding contracts, purchase orders, letters of intent, manufacturing-slot reservations or other enforceable commitments that were entered in before issuance of the executive order, even if the manufacture, shipment, installation, commissioning, or payment occurred afterwards. The DOE should consider allowing class licenses or portfolio-level approvals covering product families, standardized designs, repeat purchases, framework agreements, and substantially similar projects, rather than requiring a separate license for each transaction. Finally, projects that have completed engineering design, permitting,

financing approval, supplier qualification and selection, integration, or equipment reservation prior to issuance of final guidance should receive grandfathering protections from the DOE.

- *Should manufacturers expect a final list of compliant and non-compliant equipment with the implementation guidance, and will there be processes to inform the initial list as well as amend this list?* As our members have expressed, it is critical that there is clarity in the implementation of these restrictions. Having a clear, well-defined list could be a useful tool for manufacturers to reference. The DOE should maintain a transparent prequalification list and should also publish procedures for additions, removals, and appeals.

To assist the administration in resolving these questions and others in a timely manner, we would welcome the opportunity to convene the interagency with private sector stakeholders to discuss practical implementation strategies.

* * * * *

The NAM appreciates the DOE's consideration of the information in these comments and the requests for further clarification on outstanding confusion over the initial executive order. Our industry supports the administration's objectives of securing the United States bulk-power system from foreign cyber threats as well as supporting a modern and strengthened grid. Final implementation guidance that is precise, risk-based, and administrable will achieve these goals.

We look forward to continuing to work collaboratively with the DOE to develop effective, sensible policies that secure our nation's critical energy infrastructure while promoting manufacturing growth in the United States, and would welcome continued engagement with utilities, manufacturers, equipment suppliers, and defense agencies.

Sincerely,



Mike Davin
Senior Director, Energy and Resources Policy



Christopher Phalen
Vice President, Domestic Policy