

PUBLICATION

What the New Executive Order Means for Grid Cybersecurity and Supply Chain Risk

Authors: Elizabeth Haskins, John D. Koesters, Stephen E. Luttrell, Matthew George White
August 28, 2026

President Trump signed an Executive Order (EO) on August 26, declaring a national emergency with respect to risks posed by certain foreign-produced bulk-power system electric equipment. The EO authorizes the Department of Energy (DOE) to prohibit, condition, monitor, or require replacement of covered foreign-made equipment where DOE determines that the equipment presents an unacceptable cybersecurity, grid reliability or resilience, or other national security risk.

The EO reflects increasing federal concern regarding the growing dependence of the U.S. electric system on foreign-manufactured components and associated software, firmware, maintenance services, and remote-access capabilities. This concern has intensified as grid modernization efforts have introduced internet-connected devices, cloud-based monitoring platforms, and automated control systems that create new potential entry points for cyber adversaries. As an example, earlier this year, security researchers discovered unauthorized "kill switches" and communication connections back to China in power inverters installed in American solar farms. According to the White House, the EO is intended to address these threats and vulnerabilities that could permit sabotage, unauthorized access, cyber intrusion, or disruption of critical infrastructure.

Key Provisions

The EO authorizes the DOE to review transactions involving foreign-produced bulk-power system equipment and to prohibit or impose conditions on acquisitions, imports, transfers, or installations that present identified risks. "Foreign-produced" equipment means articles not manufactured, produced, or assembled in the U.S. "Bulk-power system electric equipment" means "items used in bulk-power system substations, control rooms, or power generating stations," including:

- substation transformers;
- grid-connected inverters;
- battery energy storage systems (BESS);
- large, small, and backup generators;
- industrial control systems (including remote terminal units and programmable logic controllers); and
- protective relays.

Notably, agencies have broad authority to consider 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 in defining qualifying equipment.

The DOE's risk analysis is designed to reduce the risk of:

- unauthorized remote access or cyber-enabled manipulation of critical infrastructure;
- sabotage or disruption of grid operations;
- supply-chain vulnerabilities arising from foreign dependence; and
- catastrophic impacts on critical infrastructure resilience and national security.

The EO also extends beyond future purchases. The DOE may – in consultation with the Secretary of Defense, the Secretary of Commerce, the Secretary of Homeland Security, and the Director of National Intelligence – require already-installed equipment to be identified, monitored, isolated, secured, disconnected, replaced, or removed if it determines that the equipment creates unacceptable risks. The DOE is directed to consider reliability and safety, secure replacement availability, and continuity of service issues in implementing these authorities.

Implementing rules and regulations will be promulgated within 120 days.

Why This Matters

The EO arrives at a time when electric utilities, renewable energy developers, data center operators, and industrial facilities are rapidly expanding infrastructure to support artificial intelligence, advanced manufacturing, electrification, and defense-related projects. These growing electricity demands are increasing the consequences of grid disruptions.

Organizations with significant deployments of imported energy infrastructure – particularly solar generation assets, battery storage, and modern grid-control technologies – should expect heightened scrutiny of equipment provenance, component sourcing, software supply chains, and vendor relationships.

The EO's provisions create new compliance obligations and risks from equipment procurement through project development and financing. Organizations subject to these requirements will need to implement procedures and contractual structures to demonstrate compliance to enforcement authorities, along with project sponsors, investors, and lenders. This may include protocols for tracking compliance of bulk power system purchases, contractual terms requiring express compliance with the EO, and other terms allocating risks and indemnities related to non-compliance.

Cybersecurity Implications

The EO is consistent with a broader trend of growing concern regarding cybersecurity threats embedded within energy infrastructure.

Recent industry reporting highlighted discoveries of undocumented communications devices and remote-access capabilities in certain foreign-manufactured solar inverters and battery systems. These concerns center on the possibility that undisclosed communications pathways could bypass traditional cybersecurity controls and potentially allow unauthorized manipulation or disruption of grid-connected assets. Such equipment could enable remote disabling of infrastructure, operational interference, espionage, or coordinated attacks affecting grid reliability.

Nation-state threat actors have demonstrated both the capability and intent to target energy-sector infrastructure. Recent years have seen documented incidents involving reconnaissance of U.S. grid systems, deployment of malware specifically designed for industrial control environments, and pre-positioning of access within utility networks. The EO reflects recognition that supply chain compromise represents a persistent threat vector that traditional perimeter-based cybersecurity defenses may not adequately address.

These risks are amplified by the increasing convergence of operational technology and information technology networks, which expands the attack surface available to adversaries. Legacy industrial control systems were often designed for isolated environments and may lack modern authentication, encryption, or logging capabilities. As grid infrastructure becomes more connected to support advanced monitoring, predictive maintenance, and distributed energy resource management, the potential consequences of a successful cyber intrusion grow correspondingly.

For owners and operators of generation and transmission assets, regulators are increasingly emphasizing:

- supply-chain security reviews;
- vendor due diligence;
- Software Bills of Materials (SBOMs);
- network segmentation;
- removal or limitation of unnecessary remote access capabilities;
- continuous monitoring of operational technology (OT) environments;
- third-party cybersecurity risk governance; and
- implementation of zero-trust architecture principles for critical OT assets.

Recommended Considerations

Cybersecurity is quickly becoming intertwined with energy-sector regulatory compliance and critical infrastructure oversight. In light of this EO, operators and developers should consider evaluating:

Inventory and Asset Visibility

- identification of all foreign-manufactured bulk-power system equipment;
- mapping of operational technology and industrial control systems; and
- inventory of embedded software, firmware, communications modules, and remote-access tools.

Operational Technology Security

- segmentation of OT and enterprise networks;
- multifactor authentication for privileged access;
- monitoring of vendor and third-party remote connections;
- vulnerability management for industrial control systems (ICS);
- security information and event management (SIEM) integration for OT environments; and
- implementation of encrypted communications for all ICS/SCADA traffic.

Vendor and Supply-Chain Risk

- assessment of country-of-origin risks;
- review of cybersecurity representations in vendor contracts;
- evaluation of replacement or diversification options for critical equipment;
- contractual provisions requiring notification of security vulnerabilities and firmware/software updates; and
- requirement of SBOMs from all critical equipment vendors.

Resilience Planning

- black-start and continuity planning;
- backup communications protocols;
- incident response procedures that address cyber-physical disruptions;
- integration with the Cybersecurity and Infrastructure Security Agency (CISA), Information Sharing and Analysis Centers (ISACs), and federal threat intelligence sharing programs; and
- tabletop exercises simulating cyber-physical attack scenarios.

Regulatory Preparedness

- monitoring forthcoming DOE implementing regulations;
- preparing documentation that may support future DOE reviews;
- evaluating potential impacts on planned procurements and capital projects; and
- alignment with North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards and emerging DOE cybersecurity requirements.

Looking Ahead

The DOE has been directed to issue rules implementing the EO, to identify equipment that may warrant particular scrutiny, and to determine the scope of Covered Foreign Entities and persons owned, controlled by, or subject to the jurisdiction or direction of such Entities for purposes of the EO.

In the meantime, owners, operators, and developers of energy infrastructure should begin assessing the provenance, cybersecurity posture, and operational dependencies associated with critical grid equipment. Organizations that proactively evaluate their supply chains and OT cybersecurity programs will be better positioned to respond to future regulatory requirements and potential equipment review or replacement mandates.

If you have questions about these developments or would like to discuss the potential impact on your business, please contact a member of Baker Donelson's [Energy Group](#), [Renewable Energy Team](#), or [Cybersecurity and Incident Response Team](#).