



Rainey
Center

Securing the Grid While Growing the Grid

October 2026







Key Takeaways

The rules are being written now.

Executive Order 14421 has the Department of Energy writing implementing rules by December 24, 2026, with comments on its Request for Information due October 9. A parallel FCC action already restricts foreign-made, remotely connected inverters.

Neither track is a blanket ban.

The order applies only where a transaction has a Covered Foreign Entity nexus and the Department finds undue or unacceptable risk, and it allows mitigation, licensing, and prequalification. The FCC has run a case-by-case approval path from the start.

Origin is a signal, not a safeguard.

The risks the order names travel through code, connections, and control, and they work the same whether a device is built abroad or at home. A ban governs geography; a standard governs the risk, on every device.

The standard does not need to be invented.

NERC, NIST, IEEE, UL, and IEC already define measurable security requirements, and the FCC already clears compliant equipment case by case. Voters are there too: by 69% to 19% they say how equipment is built, tested, and controlled matters more than where it was made.

The recommendation.

Define risk by a verifiable, technology-neutral standard built on those existing controls, prequalify through independent U.S. testing aligned with the FCC, mitigate installed equipment before removing it, and keep the cost to ratepayers in view.



The Security Standards Already Exist: A Case for Regulation, Not a Blanket Ban

Executive Order 14421 directs the Department of Energy to secure the bulk-power system from foreign-produced equipment tied to Covered Foreign Entities. Implementing rules are due December 24, 2026, and comments on the Department's Request for Information close October 9.^{1,2} The concern behind the order is real. In 2025, analysts reported undocumented cellular radios in Chinese-made solar inverters, and federal agencies have documented state-sponsored access inside United States critical infrastructure.^{3,4} Ownership compounds the risk: China's National Intelligence Law obliges companies to assist state intelligence work.⁵ The Department must now define undue or unacceptable risk, and the definition it chooses will decide whether the rule measures security or mostly measures geography.

One answer would key the rule to where equipment is made. This brief examines a different one: a verifiable, technology-neutral standard applied to every grid device, whatever its origin. The two are not opposites. Where a device is made is worth knowing, and a Covered Foreign Entity nexus is a sound reason to look harder, but the risks that the order names reach the grid through code, connections, and control rights, and those pathways work the same way whether a device is assembled abroad or at home.



Demand Is Rising While Supply Concentrates Abroad

Demand is climbing: the North American Electric Reliability Corporation projects summer peak demand will grow 224 gigawatts, or 24%, over the next ten years.⁶ Supply is concentrated abroad: about 80% of large transformers and more than 90% of the power inverters installed over the past decade were imported, Chinese suppliers held close to half the United States inverter market in 2024 and 2025, and China makes more than 80% of the world's battery cells.^{7,8,9} New domestic plants help, but they reach production only late in the decade.¹⁰ A rule that stalls the build-out carries a reliability cost. A rule that leaves foreign control pathways open carries a security cost. The task is to meet record demand without doing either.



Origin Is a Signal, Not a Safeguard

A rule keyed to assembly location regulates geography. It does not test the controls that decide whether a device can be trusted on the grid, and it misses risks that have nothing to do with a foreign factory: a domestically assembled device with an insecure cloud connection, or a credentialed insider. The better principle is to regulate the risk, not the nameplate. It asks three things of any device, foreign or domestic: whether anyone outside the United States can reach it, whether its software can be verified, and whether its data stays home. A verifiable standard answers all three. An origin rule answers none of them (Table 1).



TABLE 1

What Each Approach Actually Tests

Risk Pathway	An Origin Rule	A Verifiable Standard
Remote access by the maker	Caught only if the maker is foreign	Off by default and owner-controlled, foreign or domestic
Software integrity	Not tested	Verified software, with owner-approved updates
Where the data goes	Not addressed	Kept in the United States
A domestic or relabeled device with hidden connectivity	Passes as domestic	Tested like any other device

A ban also misses the way many attacks actually happen. A growing share of intrusions into critical infrastructure never touch a hardware backdoor; they exploit people, through phishing and impersonation that turn a trusted employee into the way in, no matter who built the equipment.¹¹ A standard can require the operator-side controls a ban never reaches, such as multifactor access, session logging, and the ability to revoke remote access, which raise the floor for every system on the grid, domestic ones included.



The Standard Already Exists

The Department does not have to invent a security standard, and industry already speaks its language. NERC's Critical Infrastructure Protection standards set mandatory supply-chain, access, and monitoring requirements for bulk-system operators.¹² The National Institute of Standards and Technology supplies measurable controls for supply-chain risk, operational technology, device security, and secure software development.^{13,14} IEEE 1547.3 covers cybersecurity for distributed energy resources, UL 1741 already defines the inverter class the FCC restricts, and IEC 62443 is the international baseline for industrial control systems.¹⁵ Expressing the rule in that vocabulary tells a manufacturer exactly what it must prove, and lets the Department tier requirements by consequence, so the heaviest scrutiny falls on the equipment whose failure would matter most, such as utility-scale inverters and substation control systems.¹⁶

The federal government has also already built the enforcement model. The FCC placed foreign-made, remotely connected inverters on its Covered List, which keeps them out of the United States market, and it clears compliant devices through a case-by-case Conditional Approval.^{17,18} On August 20 it narrowed the entry to inverters that can actually be reached remotely, the same connectivity test a security standard would apply, and it kept security updates flowing to installed units so that cutting them off did not make them less safe.¹⁹ The Department should build on that regime rather than beside it: shared criteria, one evidence package, and recognition of matching determinations, so a manufacturer files once instead of twice.





What a Verifiable Standard Would Require

In practice, a device would have to meet a short list of requirements, each of which can be tested:

U.S.-Controlled Operation

No remote access or control from outside the United States. Remote functions are off by default, under the owner's control, and can be disabled without impairing safe operation.

Verified Software

Signed firmware and verified boot, a list of what is in the software, and owner review of updates before they install.

Independent Testing

Penetration testing and a hardware teardown by an accredited United States laboratory, with re-testing after major updates.

Data Kept Home

Operational data stays in the United States, and vendor access to it is logged and limited.

Equipment that cannot meet the standard, or that hides communication hardware, stays off the grid. The point of a standard is that some equipment fails it.



Build It Here, and Verify Everything

Securing the grid and building more of it at home are complementary goals, and the order pursues both. To decide what counts as American-made, the Department should use tests that already exist: the Buy American Act's domestic-content threshold or the substantial-transformation standard from customs law, both of which reward real manufacturing rather than relabeling.^{20,21} The FCC took the same path when it exempted inverters eligible for the Section 45X manufacturing credit.¹⁷ Domestic production is worth encouraging, and it addresses supply concentration and lead times. It is not, by itself, a security test. A device assembled in the United States with an unsecured foreign cloud connection is still a way into the grid.





Fix Installed Equipment Before Pulling It Out

The order also lets the Department act on equipment already on the grid, and this is where a heavy hand would do the most harm. Replacement lead times run years, so pulling working equipment can create the very reliability risk the order is trying to prevent. The Department should mitigate first, by segmenting networks, monitoring, restricting remote access, and controlling updates, and reserve removal for risks that cannot be mitigated.¹ Keeping security patches flowing to installed equipment is part of that work, as the FCC's own waiver recognizes.¹⁹

When the Department does order equipment off the grid as a matter of policy rather than for demonstrated cause, it should do so with discipline. The Rainey Center's work on permitting durability shows what happens when the government reverses its own authorizations: the cost of capital rises, and ratepayers and retirement savers ultimately pay it.²² The same safeguards apply to a removal order. It should rest on specific written findings, be certified by the head of the responsible security agency, expire unless it is renewed on current facts, and carry compensation for lawfully installed equipment removed as policy. These safeguards do not weaken the Department's hand against a real threat. They make its orders credible and its rule durable.



The Honest Counterargument

Testing captures a device at one moment. An update can change its behavior later. A capable adversary can hide a function, and a foreign government can compel a vendor. For the highest-consequence equipment, some conclude that only exclusion is reliable until domestic capacity grows. A standard does not erase that risk, but it narrows it: owner-controlled updates, United States-controlled communications, continuous monitoring, and the power to revoke approval address what changes after a test, and exclusion remains the answer where firmware cannot be verified. Exclusion is a tool the standard keeps. It is not the rule the standard replaces.



What Voters Already Believe

In Rainey Center's September Policy Survey, 81% are concerned that grid equipment could be remotely accessed or controlled by a foreign government or company, with both parties within two points.²³ By 69% to 19%, voters say how equipment is built, tested, and controlled matters more than where it was made, and majorities of both parties agree. Asked what a federal standard should require, they rank no remote access from outside the United States (44%) and testing by independent United States laboratories (41%) first, and 72% would accept higher costs for stronger standards.^{23,24} Support for a single standard is broad but not deep: 59% support it, only 20% strongly. Support will hold only if the standard is demanding, independently verified, and enforced.

ABOUT THE SURVEY

Rainey Center surveyed 1,004 registered voters online, September 10-14, 2026, weighted by age, gender, race, education, 2024 vote recall, and region. The margin of error is plus or minus 4.9 percentage points and is larger for subgroups.



What the Department Should Do

The December rules and the February procurement recommendations are where this becomes policy. The Department can take four steps, and weigh cost at each. Every restriction has a price that reaches electricity bills, and it falls hardest on rural and cooperative utilities, which have the least purchasing power.



Define risk by what can be tested.

The Department should define undue or unacceptable risk by published, testable criteria, treat a Covered Foreign Entity nexus as a reason for heightened scrutiny rather than an automatic verdict, and reserve exclusion for equipment that fails the standard or cannot be mitigated.^{1,25}

Build on existing standards, and test independently.

The Department should ask the National Institute of Standards and Technology, with the North American Electric Reliability Corporation and the national laboratories, to express the standard in controls that already exist, then prequalify equipment and vendors through accredited United States laboratories on a published clock, for example 90 days for a complete application, so compliant projects are not stranded.^{2,12}

File once, not twice.

The Department should align its prequalification evidence and criteria with the FCC's Conditional Approval process so a manufacturer can file one package and get consistent answers, and work with FERC, NERC, and state regulators so distribution-level devices meet the same baseline through procurement and interconnection.¹⁷

Remediate before removing, and discipline removal orders.

For equipment already installed, the Department should prefer monitoring, segmentation, and controlled updates to removal, and when it does order removal as policy, rest it on written findings, security-agency certification, automatic expiration, and compensation for lawfully installed equipment.²²



Secure the Grid, and Keep Building It

A ban is the easiest rule to write and the least it can accomplish. It draws a line at the border, not around the risk, and leaves the country no better able to tell a secure device from a dangerous one. A verifiable standard asks more, and the standards to build it already exist. The real question is not where a device was made. It is whether its controls can be trusted. A ban is the easy answer. A standard is the leadership the grid requires.





Endnotes

1. Exec. Order No. 14421, “Declaring a National Emergency to Secure the United States Bulk-Power System,” 91 Fed. Reg. 55995 (Aug. 31, 2026) (signed Aug. 26, 2026), <https://www.federalregister.gov/documents/2026/08/31/2026-17843/declaring-a-national-emergency-to-secure-the-united-states-bulk-power-system>.
2. U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response (CESER), “Securing the United States Bulk-Power System,” Request for Information, 91 Fed. Reg. 57322 (Sept. 9, 2026), Docket No. DOE-HQ-2026-1123, RIN 1901-AB79, <https://www.federalregister.gov/documents/2026/09/09/2026-18370/securing-the-united-states-bulk-power-system>
3. S. McFarlane, “Rogue communication devices found in Chinese solar power inverters,” Reuters (May 14, 2025), <https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/>; J. Winter and R. Satter, “US warns hidden radios may be embedded in solar-powered highway infrastructure,” Reuters (Sept. 10, 2025) (reporting a Federal Highway Administration advisory dated Aug. 20, 2025), <https://www.reuters.com/legal/government/us-warns-hidden-radios-may-be-embedded-solar-powered-highway-infrastructure-2025-09-10/>
4. CISA, NSA, FBI, et al., “PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure,” Cybersecurity Advisory AA24-038A (Feb. 7, 2024) (Volt Typhoon), <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>
5. National Intelligence Law of the People’s Republic of China (2017, amended 2018), art. 7, trans. China Law Translate, <https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/>
6. North American Electric Reliability Corporation, 2025 Long-Term Reliability Assessment (Jan. 2026), https://www.nerc.com/globalassets/our-work/assessments/nerc_ltra_2025.pdf.
7. S. Chopra and B. Boucher, “Supply shortages and an inflexible market give rise to high power transformer lead times,” Wood Mackenzie (Apr. 2, 2024), <https://www.woodmac.com/news/opinion/supply-shortages-and-an-inflexible-market-give-rise-to-high-power-transformer-lead-times/>; Wood Mackenzie, “Power transformers and distribution transformers will face supply deficits of 30% and 10% in 2025,” press release (Aug. 14, 2025), <https://www.woodmac.com/press-releases/power-transformers-and-distribution-transformers-will-face-supply-deficits-of-30-and-10-in-2025/>.
8. Pilar Sánchez Molina and Tristan Rayner, “US Could Surpass 100 GW of Annual Inverter and PCS Manufacturing Capacity by 2027,” ESS News (Aug. 11, 2026) (reporting Wood Mackenzie data that more than 90% of U.S. PV inverters were imported over the past decade and that Chinese



suppliers held close to 50% of the U.S. market in 2024 and 2025), <https://www.ess-news.com/2026/08/11/us-could-surpass-100-gw-of-annual-inverter-and-pcs-manufacturing-capacity-by-2027/>.

9. IEA, Global EV Outlook 2026 (2026), <https://www.iea.org/reports/global-ev-outlook-2026>, and Global Critical Minerals Outlook 2025 (2025), <https://www.iea.org/reports/global-critical-minerals-outlook-2025>; U.S. Energy Information Administration, “China dominates global trade of battery minerals,” Today in Energy (May 21, 2025), <https://www.eia.gov/todayinenergy/detail.php?id=65305>.
10. Hitachi Energy, “Hitachi deepens commitment to U.S. manufacturing with \$528 million Mississippi transformer factory,” press release (Sept. 15, 2026), <https://www.hitachienergy.com/news-and-events/press-releases/2026/09/hitachi-deepens-commitment-to-u-s-manufacturing-with-528-million-mississippi-transformer-factory>.
11. L. Overby, “Human Hacking in the Digital Battlefield,” Rainey Center (Apr. 22, 2026). AI-augmented social engineering against critical infrastructure; the case for defense and resilience over restriction.
12. NERC Critical Infrastructure Protection (CIP) Reliability Standards CIP-013, CIP-005, CIP-010, CIP-014, and CIP-015 (FERC-approved supply-chain, access, and monitoring standards), <https://www.nerc.com/standards/reliability-standards/cip>.
13. NIST, The NIST Cybersecurity Framework (CSF) 2.0, CSWP 29 (Feb. 2024), <https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-csf-20/final>; NIST SP 800-161 Rev. 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (May 2022), <https://csrc.nist.gov/pubs/sp/800/161/r1/upd1/final>; NIST IR 8259, Foundational Cybersecurity Activities for IoT Device Manufacturers (May 2020), <https://csrc.nist.gov/pubs/ir/8259/final>, and NIST IR 8259A, IoT Device Cybersecurity Capability Core Baseline (May 2020), <https://csrc.nist.gov/pubs/ir/8259/a/final>; NIST IR 8320, Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases (May 2022), <https://csrc.nist.gov/pubs/ir/8320/final>.
14. NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (Sept. 2023), <https://csrc.nist.gov/pubs/sp/800/82/r3/final>; NIST SP 800-218, Secure Software Development Framework (SSDF) Version 1.1 (Feb. 2022), <https://csrc.nist.gov/pubs/sp/800/218/final>.
15. IEEE Std 1547.3-2023, Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems, <https://standards.ieee.org/ieee/1547.3/10173/>; UL 1741, Inverters, Converters, Controllers and Interconnection System Equipment for Use with Distributed Energy Resources, <https://www.shopulstandards.com/ProductDetail.aspx?productid=UL1741>; ISA/IEC 62443 series, Security for Industrial Automation and Control Systems, <https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards>.



16. Idaho National Laboratory, Center for Securing Digital Energy Technology (CSDet), “Battery Energy Storage System (BESS) Supply Chain Analysis” (Feb. 2025), https://csdet.inl.gov/content/uploads/45/2025/03/02_SupplyChainAnalysis_02132025.pdf, summarizing Idaho National Laboratory, Battery Energy Storage Systems Report (Nov. 1, 2024) (component criticality ratings).
17. FCC Public Safety and Homeland Security Bureau, Public Notice DA 26-786 (July 28, 2026) (adding foreign-produced power inverters to the Covered List), <https://docs.fcc.gov/public/attachments/DA-26-786A1.pdf>, and Public Notice DA 26-870 (Aug. 20, 2026) (modifying the entry after a second Department of War national security determination), <https://docs.fcc.gov/public/attachments/DA-26-870A1.pdf>.
18. FCC, “List of Equipment and Services Covered by Section 2 of the Secure Networks Act” (Covered List) (updated Aug. 20, 2026), <https://www.fcc.gov/supplychain/coveredlist>.
19. FCC Office of Engineering and Technology, Public Notice DA 26-789 (July 28, 2026) (waiver permitting software and firmware updates that mitigate harm to U.S. consumers for previously authorized covered inverters, through at least Jan. 1, 2029), <https://docs.fcc.gov/public/attachments/DA-26-789A1.pdf>.
20. 41 U.S.C. §§ 8301 to 8305 (Buy American Act); 48 C.F.R. §§ 25.003, 25.101 (domestic-content threshold for a U.S.-made end product, rising to 75% for items delivered beginning in 2029).
21. 19 U.S.C. § 2518(4)(B) (substantial transformation under the Trade Agreements Act); see *Energizer Battery, Inc. v. United States*, 190 F. Supp. 3d 1308 (Ct. Int’l Trade 2016).
22. Sarah E. Hunt, When Permits Aren’t Permanent: How Permitting Instability Reaches the American Retirement Portfolio and the Statutory Reforms That Will Restore Investor Confidence, Joseph Rainey Center for Public Policy (Sept. 2026).
23. Rainey Center, September Policy Survey, grid-equipment security questions Q65 to Q69 (fielded Sept. 10 to 14, 2026; 1,004 registered voters; plus or minus 4.9 points). Topline and party results as reported by the survey team.
24. Rainey Center, September Policy Survey: Topline Results and Demographic Crosstabs (fielded Sept. 10 to 14, 2026), published with “September Policy Survey: Summary of Findings,” <https://www.raineycenter.org/polling/september-policy-survey-summary-of-findings>.
25. U.S. Department of Energy, CESER, “Declaring a National Emergency to Secure the United States Bulk-Power System Executive Order” (implementation page, accessed Sept. 28, 2026), <https://www.energy.gov/ceser/declaring-national-emergency-secure-united-states-bulk-power-system-executive-order>.





**Rainey
Center**

info@raineycenter.org
raineycenter.org