

Department of Energy

Securing the United States Bulk-Power System

Docket: DOE-HQ-2026-1123

AUTHORS

Annie Fixler

Director and Senior Fellow

FDD's Center on Cyber and Technology Innovation

Zoe Rice

Research Intern

FDD's Center on Cyber and Technology Innovation

Craig Singleton

Senior Director and Senior Fellow

FDD's China Program

Jack Burnham

Senior Research Analyst

FDD's China Program

Sophie McDowall

Research Associate

FDD's Center on Cyber and Technology Innovation

RADM (Ret.) Mark Montgomery

Senior Director and Senior Fellow

FDD's Center on Cyber and Technology Innovation

Washington, DC

October 9, 2026

Introduction

The United States is entering a time of essential power grid buildout. Driven by artificial intelligence's datacenter demands and the broader electrification of the U.S. economy, as well as the need to replace aging infrastructure, the government faces the task of meeting growing needs for generation, transmission, and distribution of electricity while ensuring the security and reliability of the bulk-power system (BPS). The technologies necessary for this buildout — such as battery energy storage systems and inverters and the software and firmware that control them — are increasingly “smart,” connected, and remotely updatable. Connectivity makes the grid more flexible, but it also creates new opportunities for adversaries.¹ If not properly secured, these new technologies pose a significant risk to the U.S. public and national defense.

Foreign adversaries have repeatedly shown both the intent and ability to disrupt U.S. and allied electric infrastructure. In 2015, Russian military intelligence remotely opened breakers at three Ukrainian distribution utilities, cutting power to roughly 225,000 people.² A year later, the same actors struck a transmission substation. More recently, Russian actors disrupted operations at Polish energy companies but luckily failed to cause large-scale grid disruption.³ Meanwhile, for at least the past five years, China has been prepositioning capabilities within U.S. critical infrastructure — including energy infrastructure — to disrupt normal operations at the time of Beijing's choosing.⁴

Against this backdrop, President Donald Trump issued Executive Order 14421 to protect U.S. electric infrastructure from threats posed by foreign-made equipment.⁵ Adversaries are seeking access to the U.S. electric grid. America need not make it easy for them by installing equipment that may have preset access points. The growing dependence on “smart” components and movement toward greater grid interconnection makes the issue increasingly urgent for national security.

Every foreign-produced component, however, does not carry the same risk. Components that can perform only a single function because of chemistry or physics constraints do not pose the same risk that digital control systems pose. This reality demands a tiered, risk-informed approach to identifying the devices and individual components that must be sourced domestically, those that

¹ Phoebe Benich, Emma Stewart, and Harry Krejsa, “Electrotech Moneyball: An Industrial Strategy for Ranking Risk and Opportunity in Energy & AI Supply Chains,” *Carnegie Mellon Institute for Strategy & Technology and Foundation for Defense of Democracies*, May 2026. (<https://www.cmu.edu/cmist/tech-and-policy/electrotech-moneyball/electrotech-moneyball-cmist-white-paper-may-2026.pdf>)

² Brian E. Humphreys, “Attacks on Ukraine's Electric Grid: Insights for U.S. Infrastructure Security and Resilience,” *Congressional Research Service*, September 30, 2026. (<https://www.congress.gov/crs-product/R48067>)

³ “ELECTRUM: Cyber Attack on Poland's Electric System 2025,” *Dragos*, January 2026. (<https://5943619.hs-sites.com/hubfs/Reports/dragos-2025-poland-attack-report.pdf?hsCtaAttrib=205962111494>); Daryna Antoniuk and Alexander Martin, “Russia's FSB blamed for Poland grid attack as UK and EU impose first joint cyber sanctions,” *The Record*, July 12, 2026. (<https://therecord.media/russia-blamed-for-poland-grid-cyberattack-in-joint-uk-eu-sanctions-package>)

⁴ U.S. Cybersecurity & Infrastructure Security Agency, “PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure,” Advisory AA24-038A, February 7, 2024. (<https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>)

⁵ U.S. Executive Order 14421, “Declaring a National Emergency to Secure the United States Bulk-Power System,” August 26, 2026. (<https://www.federalregister.gov/d/2026-17843>)

can be sourced from trusted foreign partners, and those that carry little digital risk and could be purchased from any supplier.

The following response outlines how the Department of Energy (DOE) can take a risk-based approach to securing the bulk-power system in response to Docket No. DOE-HQ-2026-1123. In the aggregate, the response outlines four recommendations:

1. Classify bulk-power system (BPS) equipment through a tiered system based on function, connectivity, and location in the technology stack and place the most rigorous requirements on the active control layer. (C-1 and A-3)
2. Secure Tier 1 components as “firebreaks” in the existing grid while trusted alternatives are developed, and prioritize strategic substitution of adversary-origin control components in the highest-consequence locations. (A-6, D-2, D-3)
3. Require standardized and updated hardware and software bills of material (HBOMs and SBOMs) so that origin and risk indicators of components with smart capabilities can be traced. (B-2, A-5)
4. Pair near-term security measures with a long-term industrial strategy, including durable demand commitments, allied mutual recognition agreements, and focused investment in linchpin technologies. (F-1 through F-5, G-5)

Scope and Definitions

[A-1] The Foundation for Defense of Democracies (FDD) is a nonprofit, nonpartisan research institute based in Washington, DC. FDD does not accept funding from any foreign government or corporation. It is an institutional stakeholder that will address the policy, cost, implementation, and public-interest perspective. The recommendations contained in this response stem from work by FDD’s three centers on American power: the Center on Military and Political Power, Center on Economic and Financial Power, and Center on Cyber and Technology Innovation. Additionally, the recommendations leverage the expertise of FDD’s China Program.

In particular, the response draws on research and recommendations contained within FDD publications, “Electrotech Moneyball: An Industrial Strategy for Ranking Risk and Opportunity in Energy & AI Supply Chains,”⁶ “Laser Focus: Countering China’s Lidar Threat,”⁷ and

⁶ Phoebe Benich, Emma Stewart, and Harry Krejsa, “Electrotech Moneyball: An Industrial Strategy for Ranking Risk and Opportunity in Energy & AI Supply Chains,” *Carnegie Mellon Institute for Strategy & Technology and Foundation for Defense of Democracies*, May 2026. (<https://www.cmu.edu/cmist/tech-and-policy/electrotech-moneyball/electrotech-moneyball-cmist-white-paper-may-2026.pdf>)

⁷ Craig Singleton and RADM (Ret.) Mark Montgomery, “Laser Focus: Countering China’s LidAR Threat to U.S. Critical Infrastructure and Military Systems,” *Foundation for Defense of Democracies*, December 2, 2024. (<https://www.fdd.org/wp-content/uploads/2024/12/fdd-memo-laser-focus-countering-chinas-lidar-threat-to-u.s.-critical-infrastructure-and-military-systems.pdf>)

“Beijing’s Power Play.”⁸ These works are referenced throughout the response. FDD scholars cannot, however, provide installed-base data, cost data, or proprietary supply-chain records that would be vendor, owner, or operator specific. FDD has therefore only answered the questions most relevant to its expertise.

[A-3] DOE should judge the component based on the technical capabilities and location of the equipment within the network architecture. The capability is its “smart” or “dumb” profile (see C-1). A smart component is one that can connect across the bulk-power system and is positioned within the architecture such that it can reach across and throughout the system. With malicious access to smart components, an adversary could have a widespread impact.

[A-3.a] The definition of “associated with” the bulk-power system should focus on whether the equipment, component, or service can affect operation, control, configuration, integrity, confidentiality, and safety of the BPS. Cellular radios and other communications components within pieces of equipment, for example, are the “smart” capability that should be designated as associated with the BPS. According to public reporting, there have been instances in which foreign manufacturers have failed to document these communications systems.⁹ Idaho National Laboratory (INL) recommends segmenting vendor monitoring from command and control so that consequential functions are protected.¹⁰ Even if a manufacturer installs monitoring capabilities for safe operation of the equipment, an adversary could use the pathways to disrupt operations if there is insufficient segmentation.¹¹

In November 2024, for example, Chinese inverter manufacturer Deye reportedly used its remote management tools to disable inverters sold in the United States over a commercial dispute with U.S. distributor Sol-Ark.¹² While Deye disputes the accusation,¹³ the scenario is plausible and concerning. Reuters reported in a separate incident that from around October 2024 to May 2025, there were cases of undisclosed communication devices in the power inverters of batteries from multiple Chinese suppliers.¹⁴ The concern was similar: The manufacturer could use this

⁸ Craig Singleton, “Beijing’s Power Play: Safeguarding U.S. National Security in the Electric Vehicle and Battery Industries,” *Foundation for Defense of Democracies*, October 23, 2023. (<https://www.fdd.org/wp-content/uploads/2023/10/fdd-memo-beijings-power-play.pdf>)

⁹ Robert Freedman, “‘Rogue’ Communication Devices Found on Chinese-Made Solar Power Inverters,” *Utility Dive*, May 15, 2025. (<https://www.utilitydive.com/news/rogue-communication-devices-found-on-chinese-made-solar-power-inverters/748242>)

¹⁰ U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, Idaho National Laboratory, “Battery Energy Storage Systems Report,” November 1, 2024, page 76. (https://www.energy.gov/sites/default/files/2025-01/BESSIE_supply-chain-battery-report_111124_OPENRELEASE_SJ_1.pdf)

¹¹ RADM (Ret.) Mark Montgomery and Jack Burnham, “The Risk of Chinese-Produced Cellular Modules,” *Foundation for Defense of Democracies*, April 2026. (<https://www.fdd.org/analysis/2026/04/15/the-risks-of-chinese-produced-cellular-modules>)

¹² Dave Soulia, “The November 2024 Inverter Shutdown Was Real—and It Came from China,” *FYIVT*, May 23, 2025. (<https://fyivt.com/the-november-2024-inverter-shutdown-was-real-and-it-came-from-china>)

¹³ Dirk Knop, “Photovoltaics: Deactivated Deye and Sol-Ark inverters in the USA,” *Heise* (Denmark), November 30, 2024. (<https://www.heise.de/en/news/Photovoltaics-Deactivated-Deye-and-Sol-Ark-inverters-in-the-USA-10183716.html>)

¹⁴ Sarah 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>)

communication pathway to destabilize power generation. More broadly, if companies in adversary jurisdictions produce and maintain communication with equipment sold in the United States, those nation states could use communication and control systems to affect the safe operation of America's electric grid.

[A-3.b] DOE should consider general purpose components associated with the BPS when they provide access pathways to other Tier 1 or Tier 2 components. This includes VPNs and firewalls at the boundary of operational technology networks and cloud-hosted services that have control over grid equipment. In the December 2025 Poland attack, Russian state-directed actors targeted the VPN infrastructure which enabled management of remote terminal units and firmware.¹⁵ General purpose network equipment can be the entry point to the digital control layer. Risks posed by associated general purpose items should be addressed through digital and engineered controls and monitoring, as discussed in A-6 and D-2, and through HBOM and SBOM requirements discussed in B-2.

[A-4] As established in A-3, the function and connectivity test is what determines association. For those items with broader application beyond BPS, DOE should align definitions with other agencies that have authority to restrict foreign-made equipment. The Federal Communications Commission (FCC), for example, has a series of steps to restrict the importation and authorization of foreign-produced equipment. For power inverters, the FCC limited its Covered List entry to inverters designed to operate in parallel with the electricity grid and those designed to enable connection and communication, while excluding inverters that cannot connect to the grid.¹⁶ Alignment across DOE, FCC, Commerce Department Bureau of Industry and Security, and the Cybersecurity and Infrastructure Security Agency will help ensure that adversary-produced equipment cannot slip through the cracks of different authorities.

[A-5] DOE should consider the FCC definition of "foreign produced." For its action to prohibit foreign produced power inverters and advanced robotic devices, the FCC used the definition outlined in the Buy American Act, defining foreign produced as any product where the value of foreign produced components exceeds 35 percent of the total cost of all components.¹⁷

¹⁵ Phoebe Benich, Emma Stewart, and Harry Krejsa, "Electrotech Moneyball: An Industrial Strategy for Ranking Risk and Opportunity in Energy & AI Supply Chains," *Carnegie Mellon Institute for Strategy & Technology and Foundation for Defense of Democracies*, May 2026, page 15. (<https://www.cmu.edu/cmist/tech-and-policy/electrotech-moneyball/electrotech-moneyball-cmist-white-paper-may-2026.pdf>)

¹⁶ Devin DeBacker, Yaron Dori, Matthew DelNero, and Corey Walker, "FCC Narrows Covered List Definition of 'Power Inverters' and Clarifies Meaning of 'Foreign-Produced,'" *Covington & Burling: Global Policy Watch*, August 21, 2026. (<https://www.globalpolicywatch.com/2026/08/fcc-narrows-covered-list-definition-of-power-inverters-and-clarifies-meaning-of-foreign-produced/>)

¹⁷ Brooks E. Allen, Brian J. Egan, Jennifer Permesly, Tatiana O. Sullivan, Ellie M. Fain, Sholom Licht, Jake O. Seaboch, and Patrick Stewart, "FCC Updates Covered List to Include Foreign-Produced Advanced Robotic Devices and Power Inverters on National Security Grounds," *Skadden, Arps, Slate, Meagher & Flom LLP and Affiliates*, August 5, 2026. (<https://www.skadden.com/insights/publications/2026/08/fcc-updates-covered-list-to-include-foreign-produced-advanced-robotic-devices>); Howard W. Waltzman, Mickey Leibner, Rajesh De, Adam S. Hickey, Aiysha Hussain, Timothy J. Keeler, and Thea Kendler, "FCC Adds Foreign-Produced Power Inverters and Advanced Robotic Devices to Covered List," *Mayer Brown*, July 29, 2026. (<https://www.mayerbrown.com/en/insights/publications/2026/07/fcc-adds-foreign-produced-power-inverters-and-advanced-robotic-devices-to-covered-list>)

However, DOE cannot simply apply the definition at the product level. The most important components of devices are not necessarily the most expensive. DOE should examine equipment to assess whether critical components are “foreign produced.” DOE can use the same 35 percent metric, but assess the value of foreign inputs to the firmware, software, and control layers of the equipment. The origin of the digital components and the location of service providers and manufacturers that retain access to those digital components for the purpose of providing software updates affect the digital risk more substantially than, for example, the physical packaging of the device.

[A-5.c] To ascertain the origin of a component, the DOE should require that manufacturers furnish importers, distributors, and purchasers with HBOMs and SBOMs. These bills of materials should document the origin of each component part, including its supplier (or author) name and location, version number, unique identifiers and all other required minimum elements.¹⁸

[A-6] DOE should prioritize for early implementation those components that reach Tier 1 status as outlined in C-1. That is, technology that is most urgent in its deployment and imminent in its lock-in; has the greatest systemic reach across a network; and would grant the most cross-sector industrial competitive advantage if produced domestically.¹⁹ An assessment using these criteria will likely result in DOE prioritizing smart inverters, battery management systems, and communication modules in high-consequence locations.

Focusing on addressing control layer technologies can create “firebreaks” against risks further down the stack, and so early implementation of secure components in this area would reduce the risk in the existing stack. Firebreaks — that is, security measures like segmentation, isolation, and one-way communications — can be a mechanism to control risk while domestic and allied supply chains build out to meet demand.²⁰

For those classified as Tier 2, DOE should require cybersecurity and engineering controls that mitigate risks that adversaries may exploit these devices to cause disruption. DOE should consider existing standards and guidance including the Cybersecurity and Infrastructure Security Agency’s (CISA’s) Zero Trust Maturity Model,²¹ the National Institute of Standards and

¹⁸ U.S. Cybersecurity & Infrastructure Security Agency, “2026 Minimum Elements for a Software Bill of Materials (SBOM),” July 29, 2026. (<https://www.cisa.gov/resources-tools/resources/2026-minimum-elements-software-bill-materials-sbom>); Georgianna Shea, “A Software Bill of Materials Is Critical for Comprehensive Risk Management,” *Foundation for Defense of Democracies*, September 29, 2021. (<https://www.fdd.org/analysis/2021/09/29/a-software-bill-of-materials-is-critical-for-comprehensive-risk-management>)

¹⁹ Phoebe Benich, Emma Stewart, and Harry Krejsa, “Electrotech Moneyball: An Industrial Strategy for Ranking Risk and Opportunity in Energy & AI Supply Chains,” *Carnegie Mellon Institute for Strategy & Technology and Foundation for Defense of Democracies*, May 2026. (<https://www.cmu.edu/cmist/tech-and-policy/electrotech-moneyball/electrotech-moneyball-cmist-white-paper-may-2026.pdf>)

²⁰ Phoebe Benich, Emma Stewart, and Harry Krejsa, “Electrotech Moneyball: An Industrial Strategy for Ranking Risk and Opportunity in Energy & AI Supply Chains,” *Carnegie Mellon Institute for Strategy & Technology and Foundation for Defense of Democracies*, May 2026, page 28. (<https://www.cmu.edu/cmist/tech-and-policy/electrotech-moneyball/electrotech-moneyball-cmist-white-paper-may-2026.pdf>)

²¹ U.S. Cybersecurity & Infrastructure Security Agency, Cybersecurity Division, “Zero Trust Maturity Model: Version 2.0,” April 2023. (https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf)

Technology's Internet-of-Things Cybersecurity Guidelines²² and project on secure software development and operation, and other relevant existing national and international technical standards.²³

Covered Foreign Entities and Supply Chain Risk Management

[B-2] DOE should leverage existing HBOM and SBOM standards and develop BPS supplemental minimum elements as necessary to clarify the applicability of existing standards to electric infrastructure needs. It should disclose the component's producer, the location of its production, and the percentage of component value associated with each production.²⁴ The reporting would support the recommendations made in C-1, C-2, and D-4.

When every vendor discloses the same information in the same format, DOE and asset owners can compare products and assess indicators of risk within product classes. FDD has recommended this approach to the FCC in the past, urging that applicants submit an HBOM and SBOM in order to receive equipment authorization and provide regular updates to the commission to maintain that authorization.²⁵ DOE should build on existing federal baselines, such as CISA's 2025 SBOM Minimum Elements²⁶ and 2023 HBOM Framework²⁷ so that vendors serving multiple federal programs can report once across the different reporting regimes.

Since Tier 1 and Tier 2's risk profile depends on the smart capabilities of the component, DOE should prioritize bills of materials that illuminate the components creating these capabilities. This means tracing to the control board, communications module, and firmware image origin. Because firmware and software receive updates after installation, manufacturers must continuously update these records. An SBOM generated once and stored "...is not a defense. It is a false assurance," FDD research has revealed.²⁸

²² Michael Fagan, Katerina Megas, Jeffrey Marron, Kevin Brady, and Barbara Cuthill, "IoT Product Cybersecurity Guidelines for the Federal Government: Establishing IoT Product Cybersecurity Requirements," *National Institute of Standards and Technology*, June 2026. (<https://doi.org/10.6028/NIST.SP.800-213r1.ipd>)

²³ U.S. National Institute of Standards and Technology, National Cybersecurity Center of Excellence, "Secure Software Development, Security, and Operations (DevSecOps) Practices: Executive Summary," March 2026. (<https://pages.nist.gov/nccoe-devsecops/executive-summary.html>)

²⁴ Jack Burnham, "Protecting Against National Security Threats in Domestic Telecommunications Service," *Foundation for Defense of Democracies*, July 6, 2026. (<https://www.fdd.org/analysis/2026/07/06/protecting-against-national-security-threats-in-domestic-telecommunications-service>)

²⁵ Jack Burnham, "Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program," *Foundation for Defense of Democracies*, August 7, 2026. (<https://www.fdd.org/analysis/2026/08/07/protecting-against-national-security-threats-to-the-communications-supply-chain-through-the-equipment-authorization-program-3>)

²⁶ U.S. Cybersecurity and Infrastructure Security Agency, "2025 Minimum Elements for a Software Bill of Materials (SBOM)," August 22, 2025. (<https://www.cisa.gov/resources-tools/resources/2025-minimum-elements-software-bill-materials-sbom>)

²⁷ U.S. Cybersecurity and Infrastructure Security Agency, "A Hardware Bill of Materials (HBOM) Framework for Supply Chain Risk Management," September 25, 2023. (<https://www.cisa.gov/resources-tools/resources/hardware-bill-materials-hbom-framework-supply-chain-risk-management>)

²⁸ Georgianna Shea, "From Static Inventory to Real-Time Defense: Why the SBOM Conversation Has to Change Now," *Foundation for Defense of Democracies*, April 9, 2026. (<https://www.fdd.org/analysis/2026/04/09/from-static-inventory-to-real-time-defense-why-the-sbom-conversation-has-to-change-now>)

[B-7.a] BPS regulations already require vulnerability testing and mitigation. Where these regulations do not apply to equipment covered under Executive Order 14421, DOE should work with relevant regulators to expand the requirements.

[B-7.e] As the sector risk management agency for the energy sector, DOE offers numerous, effective programs for information sharing and testing. Of particular relevance to Executive Order 14421, DOE's sponsorship of the CyTRICS program and Energy Threat Analysis Center (ETAC) provide valuable mechanisms for stakeholder participation.

CyTRICS is part of the Energy Cyber Sense program, a national program to enhance the cyber resilience of energy infrastructure.²⁹ The program is a partnership between federal agencies, national laboratories, and private companies to test hand-picked technologies that, if compromised, would have the greatest impact across the energy sector.³⁰ CyTRICS's ability to reduce time from discovery to mitigation to notification of impacted asset owners should be considered a great success. While the program relies on voluntary partnerships, DOE could explore requiring CyTRICS or similar testing as criteria for treating a foreign produced component as a domestic component for the purposes of Executive Order 14421.

Risk Evaluation and Transaction Review

[C-1] DOE should determine consequence and system criticality by assessing a technology or component based on cyber risk and industrial policy impact. Collectively, these two variables can determine national security prioritization.

First, DOE should assess a technology based on 1) its level of digital connectivity, systemic reach across a network, and to whom it grants that access; and 2) the severity of the impact of its compromise and, conversely, the value of the risk mitigation it could provide. These questions will determine the cyber risk associated with the technology and what an adversary could do with it.

Next, DOE should determine 3) the urgency of the technology's deployment and imminence of vendor lock-in; and 4) the significance of the cross-sector industrial competitive advantage if produced domestically.³¹

DOE should then restrict those components (Tier 1) to only domestic sources where the cyber risks and therefore national security risk is highest and where the industrial policy risks and rewards are greatest. Where components have meaningful security risk but lack cross-sector

²⁹ U.S. Department of Energy, Cyber Testing for Resilient Industrial Control System (CyTRICS), "CyTRICS Program Fact Sheet," November 2025. (https://www.energy.gov/sites/default/files/2025-11/CyTRICS_One-Pager_delivered-11042025.pdf)

³⁰ U.S. Department of Energy, Action Plan, "Energy Sector Cybersecurity," January 2024. (https://assets.performance.gov/APG/files/2024/january/FY2024_January_DOE_Progress_Energy_Sector_Cybersecurity.pdf)

³¹ Phoebe Benich, Emma Stewart, and Harry Krejsa, "Electrotech Moneyball: An Industrial Strategy for Ranking Risk and Opportunity in Energy & AI Supply Chains," *Carnegie Mellon Institute for Strategy & Technology and Foundation for Defense of Democracies*, May 2026. (<https://www.cmu.edu/cmist/tech-and-policy/electrotech-moneyball/electrotech-moneyball-cmist-white-paper-may-2026.pdf>)

advantage (Tier 2), DOE should permit sourcing from trusted ally supply chains with certain caveats. For the purpose of Tier 2 equipment, DOE should treat equipment sourced from Five Eyes nations, Japan, South Korea, Taiwan, Israel, and the European Union as safe assuming the equipment passes cybersecurity standards, undergoes robust testing as outlined in B-7.e, and is provided with HBOMs and SBOMs to ensure that critical components are not sourced from U.S. adversaries. DOE should continue to develop standards with these allies to ensure a common understanding of cybersecurity and engineering safety requirements. Only commodity hardware with limited security exposure (Tier 3) should receive an exception to requirements to purchase and maintain BPS associated equipment from domestic and trusted ally sources.³²

This tiering will help establish which components DOE should prioritize, aiding in early implementation plans to focus on the necessary critical components.

DOE should also seek to assess and prioritize down to the component level. For example, battery management systems sit at the intersection of generation, storage, and grid dispatch. A compromise of the BMS could result in the destabilization of the larger ecosystem.³³ As a result, an integrated battery energy storage system should be treated as a Tier 1 product.

However, even critical products contain components that have a less significant reach. The BMS and its associated firmware and cloud connectivity should be classified as Tier 1, as they govern how the battery functions and communicates with the grid.³⁴ If those systems can be separated from the electrochemical cells beneath them, which have a cybersecurity profile closer to passive commodity hardware, the electrochemical cells can be treated as Tier 3.³⁵ That is, a component of a Tier 1 product should be categorized as Tier 3 only if the commodity hardware can be segmented from the critical systems. If not, the component must also be categorized as Tier 1 to ensure proper security.

The location of a component within the technology stack and network architecture can determine the impact an affected component will have, which can be pictured as its “blast” radius. If the component’s failure would cause cascading effects and a larger grid failure, then it has a high security consequence, and must be treated as a higher-tier component. However, if that

³² Phoebe Benich, Emma Stewart, and Harry Krejsa, “Electrotech Moneyball: An Industrial Strategy for Ranking Risk and Opportunity in Energy & AI Supply Chains,” *Carnegie Mellon Institute for Strategy & Technology and Foundation for Defense of Democracies*, May 2026, page 22. (<https://www.cmu.edu/cmist/tech-and-policy/electrotech-moneyball/electrotech-moneyball-cmist-white-paper-may-2026.pdf>)

³³ Phoebe Benich, Emma Stewart, and Harry Krejsa, “Electrotech Moneyball: An Industrial Strategy for Ranking Risk and Opportunity in Energy & AI Supply Chains,” *Carnegie Mellon Institute for Strategy & Technology and Foundation for Defense of Democracies*, May 2026, page 24. (<https://www.cmu.edu/cmist/tech-and-policy/electrotech-moneyball/electrotech-moneyball-cmist-white-paper-may-2026.pdf>)

³⁴ Phoebe Benich, Emma Stewart, and Harry Krejsa, “Electrotech Moneyball: An Industrial Strategy for Ranking Risk and Opportunity in Energy & AI Supply Chains,” *Carnegie Mellon Institute for Strategy & Technology and Foundation for Defense of Democracies*, May 2026, page 24. (<https://www.cmu.edu/cmist/tech-and-policy/electrotech-moneyball/electrotech-moneyball-cmist-white-paper-may-2026.pdf>)

³⁵ Phoebe Benich, Emma Stewart, and Harry Krejsa, “Electrotech Moneyball: An Industrial Strategy for Ranking Risk and Opportunity in Energy & AI Supply Chains,” *Carnegie Mellon Institute for Strategy & Technology and Foundation for Defense of Democracies*, May 2026, page 24. (<https://www.cmu.edu/cmist/tech-and-policy/electrotech-moneyball/electrotech-moneyball-cmist-white-paper-may-2026.pdf>)

component's blast can be controlled by creating firebreaks around it, preventing cascading failures, it presents lower risk — if firebreaks are used.

DOE should also develop requirements for vendors and customers that are seeking to have their products treated as a lower-tier product for the purpose of sourcing requirements.

[C-2] The DOE should consider the legal regimes of the jurisdictions where providers, suppliers, developers, and manufacturers are domiciled. DOE should evaluate vendor history and ownership to ascertain whether the vendor is subject to invasive legal requirements. China, for example, has invasive national security laws, such as National Intelligence Law Article 7, which states that organizations and citizens shall support and cooperate with intelligence work.³⁶ Chinese law also requires that vulnerabilities found in network products produced in China be reported to the Ministry of Industry and Information Technology.³⁷ Microsoft has assessed that the rule likely enables Chinese state actors to stockpile and use zero-day vulnerabilities before they are patched.³⁸

To address the full scope of risk, the DOE should consider a product's architecture, mode of receiving software and firmware updates, inclusion of components whose contents and operation cannot be practically inspected, and whether the provider retains cloud-side custody of operational data.³⁹

For example, CATL states publicly that after a project enters operation, the company continues to monitor operational states throughout the product's life cycle.⁴⁰ The practice requires operational data to leave the utility's, or integrator's network. DOE should treat this kind of vendor-retained data as evidence in its risk evaluation, as the vendor's legal environment governs the data once it leaves U.S. control. INL found in its 2024 Battery Energy Storage System Report that some of the risk can be mitigated by separating vendor monitoring from command and control, which is why the DOE should assess not only whether a vendor collects operational data, but whether that data path is segmented from control functions (see D-2).⁴¹

³⁶ "National Intelligence Law of the P.R.C. (2017)," *China Law Translate*, June 27, 2017, Article 7.

(<https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017>)

³⁷ "Provisions on the Management of Network Product Security Vulnerabilities," *China Law Translate*, July 12, 2021, Article 7(2). (<https://www.chinalawtranslate.com/en/product-security-vulnerabilities>)

³⁸ Jonathan Greig, "Microsoft Accuses China of Abusing Vulnerability Disclosure Requirements," *The Record*, November 4, 2022. (<https://therecord.media/microsoft-accuses-china-of-abusing-vulnerability-disclosure-requirements>)

³⁹ Craig Singleton and RADM (Ret.) Mark Montgomery, "Laser Focus: Countering China's LiDAR Threat to U.S. Critical Infrastructure and Military Systems," *Foundation for Defense of Democracies*, December 2, 2024, page 7. (<https://www.fdd.org/wp-content/uploads/2024/12/fdd-memo-laser-focus-countering-chinas-lidar-threat-to-u.s.-critical-infrastructure-and-military-systems.pdf>)

⁴⁰ U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, Idaho National Laboratory, "Battery Energy Storage Systems Report," November 1, 2024, pages 54-55. (https://www.energy.gov/sites/default/files/2025-01/BESSIE_supply-chain-battery-report_111124_OPENRELEASE_SJ_1.pdf)

⁴¹ U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, Idaho National Laboratory, "Battery Energy Storage Systems Report," November 1, 2024, pages 54-55. (https://www.energy.gov/sites/default/files/2025-01/BESSIE_supply-chain-battery-report_111124_OPENRELEASE_SJ_1.pdf)

INL's 2024 BESS Report noted that China has been accused of tampering with computing equipment meant for U.S. implementation in military and power systems, asserting that the tampering went as far as installing backdoors on chips.⁴² Therefore, while an HBOM should be required of all domestic- and foreign-produced equipment, if the vendor is apt to lie about component parts or prevent their inspection, no amount of documentation will ensure a product's security.

The right to inspect is essential. INL found that many critical components sourced in the United States are governed by supplier contracts that forbid integrators from inspecting, reverse engineering, or evaluating the internal components of a device.⁴³ Purchasers of this equipment then have only a limited ability to identify or manage vulnerabilities. DOE should require manufacturers and distributors of equipment the department deems to be Tier 1 to provide the purchaser with authorization to inspect and test hardware, firmware, and software, including by independent laboratories (see D-4).

[C-3] The significance of supply chain risk is best measured by how quickly an input shortage converts into an operational problem. A supply chain disruption does not necessarily mean an immediate operational challenge. DOE should consider existing stress in the system, how much can be reasonably stored, production lead times on replacement systems, and alternate supplies if a source of production is cut off.

For example, transformer lead times are over two years, and utilities currently have lower inventories of necessary distribution transformers than in 2018.⁴⁴ The National Infrastructure Advisory Council warned in 2024 that the limited inventory is the result of a lack of skilled labor and supply chain shortages, which are further exacerbated by a demand for greater distribution of electricity.⁴⁵ In this case, a further supply chain disruption might quickly begin to cause operational problems.

The concentration of sources of critical components raises additional concerns. Supply chains for grid-scale batteries, cellular chipsets and modules, and power inverters are dominated by Chinese companies. As of 2024, DOE Office of Manufacturing & Energy Supply Chains reported that for battery supply chains, China held more than 60 percent of the market share of the critical

⁴² U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, Idaho National Laboratory, "Battery Energy Storage Systems Report," November 1, 2024, pages 54-55. (https://www.energy.gov/sites/default/files/2025-01/BESSIE_supply-chain-battery-report_111124_OPENRELEASE_SJ_1.pdf)

⁴³ U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, Idaho National Laboratory, "Battery Energy Storage Systems Report," November 1, 2024, pages 49-50. (https://www.energy.gov/sites/default/files/2025-01/BESSIE_supply-chain-battery-report_111124_OPENRELEASE_SJ_1.pdf)

⁴⁴ American Public Power Association, "Critical Electric Infrastructure and Supply Chain Constraints," June 2024. (https://www.publicpower.org/system/files/documents/70%202024%20PMC%20Issue%20Briefs_Supply%20Chain_FINAL.pdf)

⁴⁵ U.S. National Infrastructure Advisory Council, "Addressing the Critical Shortage of Power Transformers to Ensure Reliability of the U.S. Grid," June 2024, page 10. (https://www.cisa.gov/sites/default/files/2024-06/DRAFT_NIAC_Addressing%20the%20Critical%20Shortage%20of%20Power%20Transformers%20to%20Ensure%20Reliability%20of%20the%20U.S.%20Grid_Report_06052024_508c.pdf)

midstream production.⁴⁶ Other estimates assess that Chinese vendors control as much as 90 percent of the IoT module market, 85 percent of the cellular chipset market, and two-thirds of all inverter shipments globally.⁴⁷ The current supply chain risks necessitate the implementation plans to stimulate manufacturing and the development of domestic supply chains in F-3, F-4, and F-5.

Existing Equipment and Mitigation

[D-2] DOE should approach existing foreign equipment in the bulk-power system using the same risk assessment criteria as used for new equipment, as outlined in C-1 and C-2. Ensuring proper tiering designation allows for prioritization of risk mitigations for the most consequential equipment.

It is more important to replace adversary-origin Tier 1 components in high-consequence locations than Tier 3 commodity hardware. However, if the removal of Tier 1 foreign equipment would create reliability concerns, DOE should establish firebreak requirements to prevent or mitigate the impact of an adversarial exploitation of that equipment to cause grid disruption. Firebreaks should include procedures like disabling or tightly controlling remote access for the manufacturer and vendors, and controlling traffic across and between components as well as independent testing and logging.

Imposing firebreaks quickly would then buy DOE and the asset owners time to determine whether to replace concerning equipment with domestically produced component or allied-manufactured equipment. In rare cases, the firebreak may be sufficient to remove the national security risk associated with the equipment. However, DOE should view these scenarios with caution lest the department allow a national security risk to persist because of the difficulty of replacing previously installed equipment.

Cybersecurity measures and engineering can help secure the BPS during the search for alternative equipment and secure the system in the long run. DOE should develop requirements, standards, or guidelines using the knowledge it has already developed through the Cyber-Informed Engineering approach and Consequence-Driven Cyber-Informed Engineering methodology.⁴⁸

⁴⁶ U.S. Department of Energy, Office of Manufacturing and Energy Supply Chains, “Supply Chain Readiness Level Preliminary Analysis: Batteries Summary,” November 2024, slide 14. (https://www.energy.gov/sites/default/files/2024-12/Supply_Chain_Readiness_Level_SCRL_Analysis_Nov-2024_2024.12.20.pdf)

⁴⁷ Phoebe Benich, Emma Stewart, and Harry Krejsa, “Electrotech Moneyball: An Industrial Strategy for Ranking Risk and Opportunity in Energy & AI Supply Chains,” *Carnegie Mellon Institute for Strategy & Technology and Foundation for Defense of Democracies*, May 2026, page 13. (<https://www.cmu.edu/cmist/tech-and-policy/electrotech-moneyball/electrotech-moneyball-cmist-white-paper-may-2026.pdf>); RADM (Ret.) Mark Montgomery and Jack Burnham, “The Risk of Chinese-Produced Cellular Modules,” *Foundation for Defense of Democracies*, April 2026. (<https://www.fdd.org/analysis/2026/04/15/the-risks-of-chinese-produced-cellular-modules>)

⁴⁸ Idaho National Laboratory, “Consequence-Driven Cyber-Informed Engineering (CCE),” accessed October 8, 2026. (<https://inl.gov/national-security/cce>); Idaho National Laboratory, “Cyber-Informed Engineering,” accessed October 8, 2026. (<https://inl.gov/national-security/cie>)

The DOE and its national laboratories currently recommend firebreak-style mitigation for existing equipment. INL found that while rip-and-replace is unrealistic in the immediate, short, and long term, and that, for existing systems, it is possible to reduce the scope and scale of the risk using engineered controls.⁴⁹ These measures would allow the DOE to secure deployed Tier 1 equipment sourced from foreign suppliers while trusted replacements are developed (see A-6 and D-3).

[D-3] DOE needs to evaluate reliability and safety of removing and replacing deployed equipment. Where there are concerns about the availability of domestic alternatives, or where the removal and reinstallation of equipment would cause reliability or safety concerns, DOE should require the deployment of firebreaks, as noted in D-2.

[D-4] DOE should expand upon existing testing bodies to facilitate ongoing, regular testing to ensure compliance with sourcing and security requirements. The current process of relying on self-attestation is insufficient, as hidden components have emerged.⁵⁰ Instead, DOE's national laboratories have existing programs that could be expanded or used as models to create additional testing bodies.⁵¹ As mentioned in B-7.e, DOE currently sponsors the CyTRICS program which does a comprehensive assessment of the security of tested equipment. However, CyTRICS only assesses the equipment itself, not its deployment in unique architectures of individual asset owners. Determining continued effectiveness of security and engineering measures may require the creation of a new testing program. Before doing so, however, DOE should assess existing programs sponsored by the department and other federal agencies to determine where efficiencies can be gained.⁵²

The need to test consistently is key to ensuring continued security, especially if foreign components cannot be immediately replaced. Testing standards should mirror the tiering structure introduced in C-1, with an emphasis on testing of critical components with high connectivity and strategic location in the grid architecture.

Domestic Manufacturing, Secure Replacements, and Federal Procurement

⁴⁹ U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, Idaho National Laboratory, "Battery Energy Storage Systems Report," November 1, 2024, page 57. (https://www.energy.gov/sites/default/files/2025-01/BESSIE_supply-chain-battery-report_111124_OPENRELEASE_SJ_1.pdf)

⁵⁰ Craig Singleton and RADM (Ret.) Mark Montgomery, "Laser Focus: Countering China's LiDAR Threat to U.S. Critical Infrastructure and Military Systems," *Foundation for Defense of Democracies*, December 2, 2024, page 12. (<https://www.fdd.org/wp-content/uploads/2024/12/fdd-memo-laser-focus-countering-chinas-lidar-threat-to-u.s.-critical-infrastructure-and-military-systems.pdf>)

⁵¹ Craig Singleton and RADM (Ret.) Mark Montgomery, "Laser Focus: Countering China's LiDAR Threat to U.S. Critical Infrastructure and Military Systems," *Foundation for Defense of Democracies*, December 2, 2024, page 15. (<https://www.fdd.org/wp-content/uploads/2024/12/fdd-memo-laser-focus-countering-chinas-lidar-threat-to-u.s.-critical-infrastructure-and-military-systems.pdf>)

⁵² Programs the DOE should assess include INL's Cybercore Integration Center's Operational Technology Cybersecurity program, Cyber-Informed Engineering, the Grid Deployment Office's technical assistance for Grid Resilience and Innovation Partnerships, and others. Idaho National Laboratory, "Operational Technology: Cybersecurity Capabilities Catalog," October 30, 2025. (<https://inl.gov/flipbook/ot-cybersecurity-catalog>)

[F-1] BPS equipment categories of greatest concern are not those with the highest import dependence, but those where supply is concentrated in adversary jurisdictions and the equipment performs control or communication functions, as addressed in C-1.

Dependence on trusted ally sources poses a marginal security risk compared to the national security and grid reliability risk posed by dependence on adversarial supply chains for critical components. According to the DOE, 82 percent of large power transformers used in the United States were imported. As it stands, lead times commonly reach 36 months and can run up to 60 months.⁵³ The United States imports the majority of this equipment from non-adversary suppliers. Banning the importation of transformers from allies could exacerbate limited supplies and turn supply chain constraints into a reliability crisis.

Current dependencies and supply chain concentrations in foreign adversary markets are due to historic industry positioning, which emphasized market hegemony in critical components, as mentioned in C-3. China has operated a multidecade strategy to acquire intellectual property, scale manufacturing, drive domestic adoption, and lock in market share across key sectors of the stack.⁵⁴ The success of its national champions is the result of state support and interventions, including subsidies, tax incentives, and favorable procurement deals. For example, from 2015 to 2019, a Chinese Ministry of Industry and Information Technology “whitelist” of approved battery suppliers helped promote Chinese manufacturers over foreign competitors.⁵⁵ In order to combat these supply chain concentrations, the DOE should consider using government economic levers to stimulate domestic development of Tier 1 technology.

[F-3] DOE has programs that can help expand domestic sources of critical technologies and the development of alternatives. DOE’s Transformer Resilience and Advanced Components (TRAC) program, for example, helps develop new technologies that aim to meet necessary grid modernization and securitization. DOE is also financing grid improvements under its new SPARK program.⁵⁶ The program pays for reconductoring of more than 1,500 miles of transmission lines and deploying grid-enhancing technologies. Many of these technologies fall under the Tier 1 categorization, as they include networked sensors and control devices, and so DOE may be able to leverage this and other existing programs to support the implementation of Executive Order 14421.

⁵³ Idaho National Laboratory, “Operational Technology: Cybersecurity Capabilities Catalog,” October 30, 2025. (<https://inl.gov/flipbook/ot-cybersecurity-catalog>)

⁵⁴ Phoebe Benich, Emma Stewart, and Harry Krejsa, “Electrotech Moneyball: An Industrial Strategy for Ranking Risk and Opportunity in Energy & AI Supply Chains,” *Carnegie Mellon Institute for Strategy & Technology and Foundation for Defense of Democracies*, May 2026, page 13. (<https://www.cmu.edu/cmist/tech-and-policy/electrotech-moneyball/electrotech-moneyball-cmist-white-paper-may-2026.pdf>)

⁵⁵ Craig Singleton, “Beijing’s Power Play: Safeguarding U.S. National Security in the Electric Vehicle and Battery Industries,” *Foundation for Defense of Democracies*, October 23, 2023, page 4. (<https://www.fdd.org/wp-content/uploads/2023/10/fdd-memo-beijings-power-play.pdf>)

⁵⁶ U.S. Department of Energy, Office of Electricity, “Speed to Power through Accelerated Reconductoring and other Key Advanced Transmission Technology Upgrades (SPARK),” February 25, 2026. (<https://www.energy.gov/oe/speed-power-through-accelerated-reconductoring-and-other-key-advanced-transmission-technology>); U.S. Department of Energy, Press Release, “Energy Department Announces Speed to Power Investments Across 26 States to Lower Electricity Costs and Improve Grid Reliability,” September 24, 2026. (<https://www.energy.gov/articles/energy-department-announces-speed-power-investments-across-26-states-lower-electricity>)

Allied countries also provide viable alternative sources of equipment that are currently being obtained from other foreign countries. These partnerships have the opportunity to reduce duplicate costs, as well as ensure interoperability.⁵⁷ The alignment is already happening, as the European Union has decided to restrict EU funding for energy storage projects using inverters from high-risk countries.⁵⁸ It is a similar recognition of the need to secure the European power grid and indicates that the EU is in a position to look for buildout of industry as well. During the 2026 summit in France, the G7 countries also announced commitments to reduce their dependency on certain supply chains — that is, Chinese supplies — of critical minerals.⁵⁹

DOE also already partners with allied vendors. CyTRICS partners include Hitachi Energy, Schneider Electric, Schweitzer Engineering Labs, GE Vernova, and Westinghouse.⁶⁰ Nine firms of allied country origin have supported the DOE's Supply Chain Cybersecurity Principles.⁶¹

Collaboration with allied partners should continue, and mutually supported manufacturing buildout could be an essential part of implementation plans. Standards developed with allied partners would ensure allied-sourced components can integrate seamlessly with domestically produced Tier 1 control layers.

[F-4] Federal procurement should prioritize long-term measures to build out the domestic supply chain, with measures stimulating domestic development and investment. To successfully do this, the DOE should use the recommendations set forth in A-6, D-2, and D-4 to shore up cybersecurity of the BPS while domestic manufacturing is prioritized. Federal procurement should ensure that “Buy America”-style provisions and congressional intent are honored. Previously, policymakers have waived these requirements in efforts to stimulate new technology adoption.⁶² However, this undermines domestic sourcing objectives and would flout objectives of the executive order. Domestic content requirements should be strictest for Tier 1 control layers,

⁵⁷ Phoebe Benich, Emma Stewart, and Harry Krejsa, “Electrotech Moneyball: An Industrial Strategy for Ranking Risk and Opportunity in Energy & AI Supply Chains,” *Carnegie Mellon Institute for Strategy & Technology and Foundation for Defense of Democracies*, May 2026, page 32. (<https://www.cmu.edu/cmist/tech-and-policy/electrotech-moneyball/electrotech-moneyball-cmist-white-paper-may-2026.pdf>)

⁵⁸ Tristan Rayner, “EU Funding Ban on High-Risk Inverters, Including Chinese Suppliers, Extends to BESS,” *PV Magazine*, May 4, 2026. (<https://www.pv-magazine.com/2026/05/04/eu-funding-ban-on-high-risk-inverters-including-chinese-suppliers-extends-to-bess/>)

⁵⁹ G7 Leaders, “G7 Leaders’ Declaration on Securing Supply Chains for Critical Minerals,” Evian, June 17, 2026. (https://g7documents.org/fileadmin/G7G20_documents/2026/G7/France/Leaders/1%20Leaders'%20Language/G7%20Leaders'%20Declaration%20on%20securing%20supply%20chains%20for%20critical%20minerals_20260617.pdf)

⁶⁰ Daniel Lagraffe and Stephanie Johnson, “Agency Priority Goal Action Plan: Energy Sector Cybersecurity, FY 2023, Q4,” *U.S. Department of Energy*, January 2024, slide 5. (https://assets.performance.gov/APG/files/2024/january/FY2024_January_DOE_Progress_Energy_Sector_Cybersecurity.pdf)

⁶¹ U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, “Supply Chain Cybersecurity Principles,” August 16, 2024. (<https://www.energy.gov/ceser/supply-chain-cybersecurity-principles>)

⁶² Craig Singleton, “Beijing’s Power Play: Safeguarding U.S. National Security in the Electric Vehicle and Battery Industries,” *Foundation for Defense of Democracies*, October 23, 2023, page 14. (<https://www.fdd.org/wp-content/uploads/2023/10/fdd-memo-beijings-power-play.pdf>)

while Tier 3 commodity components should face transparency and testing requirements rather than sourcing restrictions.⁶³

DOE may benefit from assessing effective programs with similar intent at the state level. For example, Texas passed the 2021 Lone Star Infrastructure Protection Act, which prohibited Texas businesses and governments from contracting with entities owned or controlled by individuals from adversarial nations if contracting related to “critical infrastructure.”⁶⁴ The law applies where the arrangement would give the foreign entity direct or remote access to, or control of, critical infrastructure, including the electric grid. DOE should consider coordination with state governments to address standardization of requirements where local governments (rather than DOE) have relevant jurisdiction.

[F-5] To improve the availability and resilience of secure supply, the DOE should explore durable demand commitments for domestic and allied Tier 1 and Tier 2 manufacturers. DOE should assess where its authorities leave gaps regarding the deployment of smart components in electricity distribution systems. The existing bodies that regulate cybersecurity standards for the BPS are the North American Electric Reliability Corporation and the Federal Energy Regulatory Commission.⁶⁵ Their authority, however, does not extend to behind-the-meter deployments of smart technology that might otherwise be covered under Executive Order 14421. DOE coordination and outreach to state governments is necessary to address this gap. Additionally, DOE could work with utilities to create an industry consortium establishing shared baselines for secure integration of digitally active electrotech across diverse utility environments.

DOE should also work with industry partners to identify a small number of linchpin technologies where strategic investment could unlock systemic hurdles hindering the development of domestic supplies. Specialized supply chains would reduce the wait time and implementation of technology. Strategic investment could reverse dependence on foreign supply chains and create secure supplies of critical components. The technologies that DOE should assess include battery management systems, power electronics, grid-edge software, and actuators.⁶⁶

Economic and Regulatory Analysis

⁶³ Phoebe Benich, Emma Stewart, and Harry Krejsa, “Electrotech Moneyball: An Industrial Strategy for Ranking Risk and Opportunity in Energy & AI Supply Chains,” *Carnegie Mellon Institute for Strategy & Technology and Foundation for Defense of Democracies*, May 2026, page 31. (<https://www.cmu.edu/cmist/tech-and-policy/electrotech-moneyball/electrotech-moneyball-cmist-white-paper-may-2026.pdf>)

⁶⁴ Robert Soza, “Texas and Federal Government Seek to Protect U.S. Infrastructure from Disruption by Foreign Adversaries,” *Jackson Walker*, January 11, 2022. (<https://www.jw.com/news/insights-texas-lone-star-infrastructure-protection-act>)

⁶⁵ Phoebe Benich, Emma Stewart, and Harry Krejsa, “Electrotech Moneyball: An Industrial Strategy for Ranking Risk and Opportunity in Energy & AI Supply Chains,” *Carnegie Mellon Institute for Strategy & Technology and Foundation for Defense of Democracies*, May 2026, page 29. (<https://www.cmu.edu/cmist/tech-and-policy/electrotech-moneyball/electrotech-moneyball-cmist-white-paper-may-2026.pdf>)

⁶⁶ Phoebe Benich, Emma Stewart, and Harry Krejsa, “Electrotech Moneyball: An Industrial Strategy for Ranking Risk and Opportunity in Energy & AI Supply Chains,” *Carnegie Mellon Institute for Strategy & Technology and Foundation for Defense of Democracies*, May 2026, page 32. (<https://www.cmu.edu/cmist/tech-and-policy/electrotech-moneyball/electrotech-moneyball-cmist-white-paper-may-2026.pdf>)

[G-5] DOE should consider the benefits of positive industrial returns on domestic and allied supply buildout. Technologies covered by the executive order are not just energy technologies. Semiconductors, battery cells, wireless communication modules, sensors, and power management systems are driving an overall electrification and technological advancement of the U.S. economy.⁶⁷ Efforts to secure the bulk-power system will lay the commercial foundation for other industries. Power electronics, which govern grid-scale battery dispatch, share lineage with defense-sector and electric vehicle components, and the firmware that orchestrates battery fleets applies across autonomous systems and industrial robotics.⁶⁸ Domestic leadership in these components generates manufacturing multipliers across industries.⁶⁹

Meanwhile, the expansion of domestic and allied supplies of critical technologies will support Pentagon requirements. Beginning next year, for example, the Department of Defense is barred from procuring equipment from CATL, BYD, and other named Chinese suppliers.⁷⁰

Conclusion

Executive Order 14421 gives the DOE an opportunity to secure the bulk-power system at the moment it is being expanded. DOE should use a tiered approach focusing on connectivity where compromise would have the greatest consequence. Success in energy sector applications could unlock other security and manufacturing benefits. A deliberate, prioritized approach will allow the United States to meet threats without stalling the buildout its future depends on.

⁶⁷ Phoebe Benich, Emma Stewart, and Harry Krejsa, “Electrotech Moneyball: An Industrial Strategy for Ranking Risk and Opportunity in Energy & AI Supply Chains,” *Carnegie Mellon Institute for Strategy & Technology and Foundation for Defense of Democracies*, May 2026, page 5. (<https://www.cmu.edu/cmist/tech-and-policy/electrotech-moneyball/electrotech-moneyball-cmist-white-paper-may-2026.pdf>)

⁶⁸ Phoebe Benich, Emma Stewart, and Harry Krejsa, “Electrotech Moneyball: An Industrial Strategy for Ranking Risk and Opportunity in Energy & AI Supply Chains,” *Carnegie Mellon Institute for Strategy & Technology and Foundation for Defense of Democracies*, May 2026, page 25. (<https://www.cmu.edu/cmist/tech-and-policy/electrotech-moneyball/electrotech-moneyball-cmist-white-paper-may-2026.pdf>)

⁶⁹ Phoebe Benich, Emma Stewart, and Harry Krejsa, “Electrotech Moneyball: An Industrial Strategy for Ranking Risk and Opportunity in Energy & AI Supply Chains,” *Carnegie Mellon Institute for Strategy & Technology and Foundation for Defense of Democracies*, May 2026, page 33. (<https://www.cmu.edu/cmist/tech-and-policy/electrotech-moneyball/electrotech-moneyball-cmist-white-paper-may-2026.pdf>)

⁷⁰ National Defense Authorization Act for Fiscal Year 2024, Pub. L. 118-31, U.S.C. §154, 137 Stat. 136. (<https://www.congress.gov/bill/118th-congress/house-bill/2670/text>)