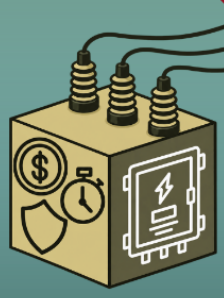
Carnegie Mellon Institute for Strategy & Technology

Carnegie Mellon University

Securing the Bulk-Power System While Advancing Speed and Affordability

A Prioritization Guide for Implementing Executive Order 14421



November 2026

By: Harry Krejsa & Phoebe Benich

Building on the Carnegie Mellon Institute for Strategy & Technology (CMIST) 2026 flagship report, *Electrotech Moneyball: An Industrial Strategy for Ranking Risk and Opportunity in Energy & AI Supply Chains*

Swift and secure grid expansion is a geopolitical imperative. Implementation of Executive Order 14421 on securing the bulk-power system should reduce adversary leverage over our grid while delivering the capacity, reliability, and affordability needed for defense, AI, and industrial growth. Our grid must be hardened against the risk of attack or coercion, but failing to build enough reliable power at a time of increased industrial and computational competition also poses serious national security peril.

The US Department of Energy (DOE) is pursuing faster grid expansion via its Speed to Power through Accelerated Reconductoring and other Key Advanced Transmission Technology Upgrades (SPARK) and Grid Resilience and Innovation Partnerships (GRIP) programs—while simultaneously tightening supply chain security through EO 14421. Implementation must reconcile the tension between these demands. Treating a diverse equipment list as one uniform emergency would spread scrutiny too thinly and delay projects where acceptable substitutes are unavailable. Policy should prioritize the components and connections through which compromise could cause the greatest harm.[1]

Distinguish the control software from the inert hardware

The smart-to-dumb spectrum makes this distinction visible within individual systems. A battery installation, generation project, or substation can contain all three layers:

- **Non-programmable hardware** (“dumb”) includes battery cells, passive PV modules, turbine machinery, transformer cores and windings, and transmission conductors. These physical components cannot receive or execute instructions. Clear them through country-of-origin disclosure, testing, and normal quality, integrity, and supply-assurance checks.
- **Containable electronics** (“smart-ish”) include hardware with embedded electronics whose behavior a trusted control layer can bound, such as inverter power stages, sensors, meters, and condition monitors. Use trusted-ally sourcing or prequalification, with disclosure of firmware and communications interfaces. A component that can issue control or trip commands on its own, for example, belongs in the control layer.

- **Control layers** ("smart") include the software, firmware, and services that can command, configure, or update equipment, such as plant and battery-management controllers, inverter control firmware, substation automation, grid and fleet orchestration, remote access, and software-update services. Reserve transaction review and the strictest sourcing limits for these systems, with the greatest cyber scrutiny where their functions can change the behavior of critical assets or many devices together.

Digital content is a starting point for review, but control authority, access, and scale determine the scope of urgency and consequence. A small controller can matter more to cyber risk than the large machine it operates.

Apply the "Electrotech Moneyball" framework to the parts that determine system behavior

Where technically feasible, secure the interfaces between digital control and physical hardware. An architectural "firebreak" combines controlled access, segmented communications, and appropriate protection to limit what a compromised component can affect. Its effectiveness must be tested against the installation's actual failure and attack paths. This can support broader hardware sourcing where the remaining risk is acceptable.[2]
To decide where these safeguards matter most, the "Electrotech Moneyball" framework considers three factors:

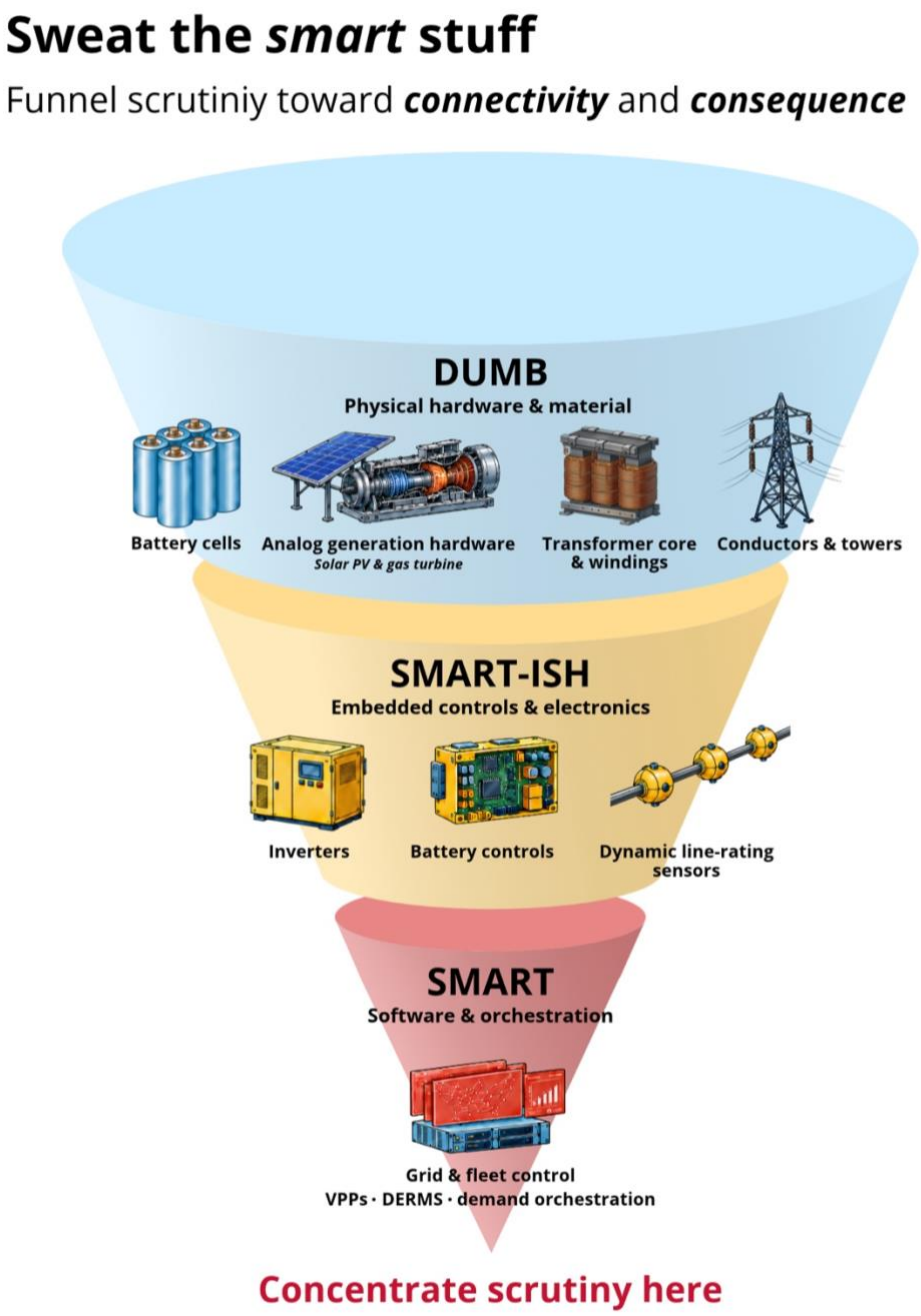
- Deployment urgency and lock-in determine which decisions cannot wait.
- Risk and blast radius determine where scrutiny and protective architecture matter most.
- Industrial spillovers help identify where investment in domestic and allied capability can also advance defense, AI, and other sectors.

Policymakers implementing EO 14421 should use the first two tests to prioritize near-term security decisions and the third to guide the capacity necessary for the United States' electricity ecosystem to remain competitive.[3]

Applying the Electrotech Moneyball framework to the order

The table below illustrates how policymakers might apply the Electrotech Moneyball framework to EO 14421's key provisions.[4]

EO provision	Proposed implementation approach
Implementing rules Section 3(b) · 120 days	Define review criteria for components and services, not whole undifferentiated systems. Examine control authority, remote access, firmware and update channels, and the consequences of coordinated compromise. Give lower-exposure hardware a clear route through review.
Risk inventory and response plan Section 3(c)	Start with critical facilities and purchases that would lock in long-lived equipment dependencies. Record the affected function, exposure, available safeguards, and the operational cost and timetable of any necessary substitution.
Equipment and vendor prequalification Section 2(e)	Use repeatable evidence requirements for equipment, suppliers, and configurations. Make the final guidance clear, including for software updates, outside vendor service dependencies, and maintenance needs. Reuse applicable evidence, such as FCC conditional approvals and accredited-laboratory testing, so manufacturers face one review rather than two.
Mitigation of otherwise prohibited transactions Section 2(c)	Where independent evidence shows the remaining risk is acceptable, define enforceable conditions on access, updates, monitoring, and operation. Verify that the safeguard addresses the relevant exposure and remains effective through maintenance and system changes.
Conditions on installed equipment Section 2(b)	Target consequential paths for digital control and isolate or replace components where feasible. Account for reliability, safety, replacement availability, and continuity before making disruptive changes. Phase this work where necessary to preserve essential service.
Federal procurement recommendations Section 4 · 180 days	Distinguish control layers from commodity inputs wherever the architecture permits. Align procurement requirements with the identified risk and a feasible supply base, while supporting domestic and allied capacity over time.



"Funnel" security scrutiny toward connectivity and consequence, and away from dumb metal

Policymakers should start with the system being purchased or operated, then separate its relevant components and services. Our funnel graphic illustrates how they can then assess the relative risk of those components or services, scoping its area of scrutiny down to only those components that are most consequential.

The "funneling questions" below apply the Electrotech Moneyball tests of urgency and blast radius to illustrative projects, and then prompt policymakers to identify safeguards that can let those projects proceed in the interim. Staying competitive in the race for advanced manufacturing and compute will require as much electricity as we can build as fast as we can build it, and securing our grid without paralyzing it will be the key balance to strike in the years ahead.

Ask three funneling questions

1. **What must this project deliver, and when?** Identify its role in capacity or reliability, the commitments being made now, and the consequences of delay or replacement.
2. **What can be accessed or controlled, and how far does that reach?** Identify remote connections, update authority, and shared dependencies. Distinguish a local device from a platform that can affect a plant or fleet.
3. **What can be secured or substituted while the project proceeds?** Assess specific controls, test their limits, and record the remaining exposure. Compare feasible alternatives and their effects on service and deployment.

Apply the distinction within each system

System or project	Focus digital review on	Distinguish the physical layer
Grid and fleet software	Dispatch, remote access, shared credentials and updates; include VPPs, DERMS and demand orchestration.	Software has no passive layer. Review its hosting and communications dependencies for integrity and continuity.
Utility-scale storage	Plant and fleet software, inverter controls, battery management, firmware and service access.	Cells, electrolyte and enclosures still require safety, quality and supply checks.
Solar and gas generation	Inverters, plant or turbine controls, protection, and any shared management service.	Passive PV modules and turbine machinery are distinct from the connected systems that operate the plant.
Transformers	Attached controllers, protection and remote interfaces where present.	Core, windings and insulation. Power and distribution applications can have different urgency, consequence and legal scope.
Transmission upgrades	Line-rating sensors and data paths, associated software, and connected control or protection equipment.	Conductors, towers and insulators. Assess the digital functions actually included in the project.

Verify *control* as well as *origin*

Country of assembly and ownership of licensed technology do not, by themselves, establish assurance against cyber risk. Identify who controls firmware, credentials, remote servicing, and updates. A battery system assembled in the United States can still take commands or updates from abroad if its software comes from a foreign vendor. Conversely, a licensed foreign design built here adds no remote-control risk when its control software comes from a trusted source and the licensor has no access to code or signing keys. Origin and foreign-entity tests for software and services should turn on who writes, signs, and updates the deployed code, not only on where hardware was assembled.

Clear, mitigate, or restrict

Answering the three funneling questions should lead to one of three outcomes, applied to each component or service rather than to the product as a whole:

- **Clear** hardware with no unacceptable exposure through proportionate quality and supply review.
- **Mitigate** where a digital risk can be contained: approve deployment or continued operation on enforceable conditions, and verify that they hold.
- **Restrict** or replace only the implicated component or service where unacceptable risk remains, with a workable transition for essential operations.

The practical objective is to secure consequential control functions while keeping needed infrastructure moving. Over time, invest in domestic and allied capabilities that reduce dependence and offer the largest industrial spillovers.

Sources

1. DOE, SPARK program overview; GRIP program overview.
2. NIST, Guide to Operational Technology Security, SP 800-82 Rev. 3, §§ 5.3.1 and 6.2.1.3.
3. Benich, Stewart, and Krejsa, *Electrotech Moneyball* (CMIST, May 2026), pp. 20–27.
4. Executive Order 14421, August 26, 2026, §§ 2–5.

Reach the authors at harrykrejsa@cmu.edu and pbenich@andrew.cmu.edu
Read the full report: www.cmu.edu/cmist/tech-and-policy/electrotech-moneyball