RESEARCH BRIEF

November 2026

Supply Chain Vulnerabilities May Worsen Critical Electrical Equipment Bottlenecks, Further Delaying the U.S. Ability to Power AI Energy Expansion

Artificial intelligence (AI) development is rapidly increasing electricity demand, especially through the growth of frontier data centers. Expanding the power supply depends on the availability of critical electrical equipment at the transmission and generation levels—much of which is sourced through complex global supply chains. In August 2026, the White House underscored the urgency of this issue in Executive Order 14421 by declaring a national emergency concerning threats to the U.S. bulk-power system associated with foreign-produced electrical equipment and explicitly linking those risks to rising electricity demand from AI and data centers.

RAND researchers examined how supply chain vulnerabilities could affect the equipment needed to power frontier AI data centers and, in turn, the U.S. power system's ability to meet AI demand by 2030. They assessed the components required for front-of-the-meter (FTM), behind-the-meter (BTM), and bridge-power (BP) energy systems; developed a composite indicator of supply chain vulnerability; and estimated how selected disruptions triggered by supply chain vulnerabilities could reduce available capacity.

What RAND Studied

To examine how supply chain vulnerabilities could affect energy expansion for AI, RAND researchers constructed an inventory of the electrical equipment needed across three broad system types:

- **FTM**—grid-connected generation and transmission infrastructure
- **BTM**—on-site systems, such as batteries and related equipment
- **BP**—interim on-site generation systems intended to provide power before full grid service is available.[1]

This research was independently initiated and made possible by RAND's own resources, including income from operations, unrestricted gifts from RAND supporters, and distributions from its long-term investment fund.

KEY FINDINGS

The research team found the following:

- The supply chains of critical electrical equipment at the generation and transmission levels needed to power AI energy expansion are vulnerable.
- Off-grid and BP strategies looking to bypass existing constraints on the power grid still rely on many of the same vulnerable components needed for grid-connected projects and therefore do not eliminate supply chain bottlenecks.
- In 2025, generation components generally appeared to be more vulnerable than transmission components, reflecting more-concentrated markets and greater exposure to supply disruptions.
- Vulnerability levels vary substantially across components, suggesting that policy responses should be targeted.
- Under illustrative threat scenarios, supply chain disruptions affecting key FTM components could reduce available net capacity by roughly 7 percent to 31 percent by 2030 relative to a no-additional-delay base case.[2]
- Supply chain disruptions affecting key BTM battery components could reduce available effective generation capacity by about 8 percent by 2030.

The researchers then evaluated the supply chain vulnerability of critical components using a composite indicator that incorporated several factors, including supplier concentration, number of importers, trade volatility, and evidence of declining imports. Finally, they used case studies and threat scenarios to estimate how supply chain–triggered equipment disruptions could affect available energy capacity by 2030.

Off-Grid Approaches Do Not Eliminate Supply Chain Constraints

One common assumption is that data center developers can avoid grid bottlenecks by moving off-grid or relying on BP solutions. But RAND's analysis suggests that this strategy does not remove supply chain constraints. Many of the same components required for FTM systems are also needed for BP and some BTM configurations, particularly generation-related equipment.

This means that off-grid approaches may help address some permitting, interconnection, or transmission constraints, but they do not fully avoid equipment shortages, import disruptions, or concentrated supplier markets. In some cases, they may simply shift dependence from one vulnerable set of components to another.

Generation Components Show Greater Supply Chain Vulnerability Than Transmission Components

Across the 2025 assessment, generation components generally ranked as more vulnerable than transmission components. This pattern appears to reflect the specialized nature of generation technologies, the smaller number of producers for some key inputs, and greater sensitivity to import volatility and supply disruptions.

By contrast, transmission-related components also face vulnerabilities, but these were generally less severe in the report's composite scoring. This distinction matters because many strategies for meeting AI-related electricity demand depend on generation equipment that may be harder to source quickly and reliably, regardless of grid integration status (see Table 1).

TABLE 1

Critical Components with Highest Supply Chain Vulnerability Rankings Across FTM Generation, FTM Transmission, and BTM Systems

System Category	Vulnerable Critical Components
FTM generation	Steam turbine, geothermal production wells,[a] solar panel parts, gas turbine, tower, steam generation system, hydraulic turbine, generator (wind), nacelle,[b] battery technologies and chemistries
FTM transmission	Conductors and wires, transmission lines,[c] reactive power compensation, static VAR compensators, support structures, spacers and space dampers, grounding system, large power transformers, ground wires or shield wires, circuit breakers
BTM systems	• Backup power: steam turbine, thermal storage tank, sodium drain valves, steam generator, argon, water heater, sodium, aeroderivative turbines, reciprocating gas generator • Power management: metering components, medium-voltage cables,[d] switchboards, static VAR compensators • Power transfer: cables,[d] control rods

[a] The Harmonized Tariff Schedule (HTS) code used for production wells is 8905.20.0000, which corresponds to drilling and production platforms. In practice, most geothermal production wells are likely imported on a component-by-component basis rather than as fully assembled platforms. Accordingly, this HTS code most closely captures a potentially complete platform, though it is not fully representative of all geothermal production well–related imports.

[b] The HTS codes used to define nacelles and other wind energy–related parts include shared classifications across related products.

[c] The HTS codes used to define conductors, wires, and transmission lines include shared classifications across related products.

[d] The HTS codes used to define cables and medium-voltage cables include shared classifications across related products.

Supply Chain Risks Could Materially Reduce Available Capacity by 2030

RAND researchers also examined how selected supply chain threats could affect the power system's ability to meet AI demand. They found that disruptions affecting key FTM generation components could reduce available net generation capacity by roughly 7 percent to 31 percent by 2030, depending on the scenario and assumptions used. For BTM systems, disruptions affecting battery-related components could reduce effective generation capacity by about 8 percent by 2030, relative to a no-additional-delay base case.

Supply chain disruptions could have system-level consequences large enough to matter for planning, siting, and timing decisions tied to AI infrastructure expansion.

Why Supply Chain Vulnerability Differs Across Components

Not all critical electrical equipment faces the same level or type of supply chain risk. Some components appear to be vulnerable because production is concentrated among a small number of suppliers or countries. Others are exposed to volatile import volumes, price spikes, or signs of declining availability.

This variation suggests that the problem is not a single, broad shortage that can be solved with one generic policy response. Some components may call for better market monitoring, others for diversification or stockpiling, and still others for substitution, standardization, or domestic industrial support.

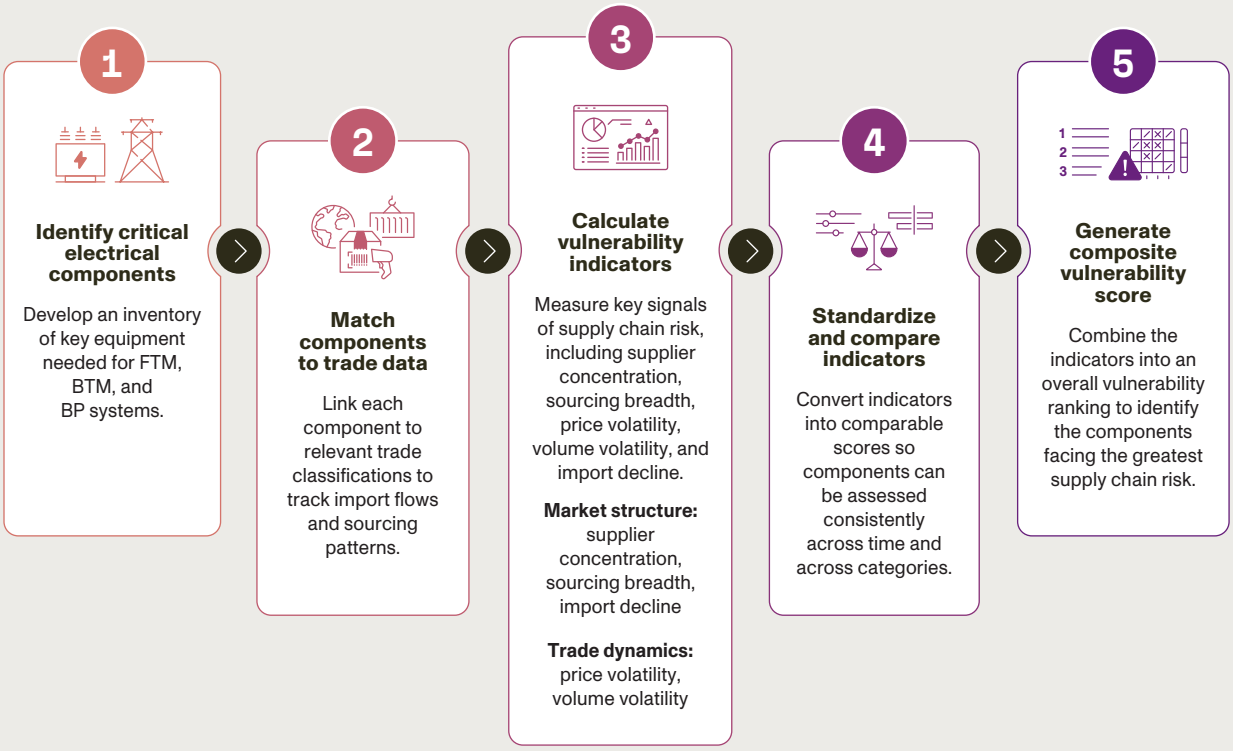
How RAND Measured Supply Chain Vulnerability

RAND researchers assessed each component using a composite indicator that combined several signals of supply chain stress, including

- supplier concentration
- number of importers
- downside volume volatility
- upside price volatility
- decline in imports over time.

This approach was designed to identify components that might be especially exposed to disruptions, delays, or shortages as the supply chain conditions change.

Research Steps



Policy Implications

Efforts to expand the energy supply for AI should address equipment bottlenecks as seriously as generation and transmission build-out. The research team's analysis led to the following policy implications:

- **Adopt a tiered response framework** so that policymakers can match interventions to the type, magnitude, and persistence of observed supply chain vulnerabilities.
- **Prioritize the most-vulnerable generation components,** which show higher supply chain risk than transmission equipment and affect both grid-connected and off-grid solutions.
- **Improve monitoring of critical equipment markets** by increasing the granularity of trade data for such components as turbines and transformers.
- **Enhance supply chain visibility** through reasonable reporting and mapping requirements for the sourcing and handling of key electrical equipment.
- **Consider developing strategic reserves for critical components** that combine high vulnerability with high system importance.
- **Promote greater standardization of key equipment** to reduce concentration risks and expand sourcing flexibility.
- **Improve coordination between utilities and large loads** so that demand forecasting and procurement planning better reflect emerging AI-related electricity needs.
- **Encourage the substitution of less vulnerable technologies** when alternative components or storage chemistries can reduce exposure to supply shocks.

Notes

[1] RAND researchers developed a comprehensive inventory of critical electrical equipment required to support frontier AI data centers, containing 220 inventoried components: 113 FTM items and 107 BTM items. The FTM side includes 52 transmission-related items and 61 generation-related items, while the BTM side includes transformers, thermal-management systems, internal power-management equipment, rack-level power-distribution equipment, power-transfer hardware, and 44 backup-power items. The inventory spans conventional grid infrastructure, on-site electrical distribution and conditioning systems, backup generation, battery systems, fuel cells, and emerging nuclear-based options. BP equipment was not inventoried as a separate category. Instead, BP is represented through components already listed under the BTM and, in some cases, FTM generation inventories. In practice, most BP equipment appears to map most directly onto the BTM backup-power category, although some FTM generation technologies may also serve BP roles.

In the report, the researchers discuss BP but do not provide named project case studies. Public reporting suggests that BP-style development is already emerging in the data center sector, including such examples as xAI's Colossus campus in Memphis and large Texas projects reportedly using on-site gas generation to begin operations ahead of full grid service.

[2] The *no-additional-delay base case* refers to an analytical scenario in which planned energy projects proceed without further supply chain–related delays beyond those already assumed in the existing deployment timeline.

This research brief describes work done in RAND Global and Emerging Risks and documented in *Supply Chain, Energy, and AI Nexus: Evaluating AI Energy Supply Chain Vulnerabilities*, by Ismael Arciniegas Rueda, Rahim Ali, Frank Andujar Lugo, Karishma V. Patel, and Robin Wang, RR-A4707-1, 2026 (available at www.rand.org/t/RRA4707-1). To view this research brief online, visit www.rand.org/t/RBA4707-1. RAND is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

RAND® is a registered trademark. © 2026 RAND Corporation

Limited Print and Electronic Distribution Rights

This publication and trademark(s) contained herein are protected by law. This representation of RAND intellectual property is provided for noncommercial use only. Unauthorized posting of this publication online is prohibited; linking directly to its webpage on rand.org is encouraged. Permission is required from RAND to reproduce, or reuse in another form, any of its research products for commercial purposes. For information on reprint and reuse permissions, please visit www. rand.org/about/publishing/permissions.