

**National Security Determination on the Threat Posed by
Foreign-Produced Power Inverters**
July 27, 2026

Summary of Determination

As President Trump’s National Security Strategy outlines, “[w]e want the world’s most robust industrial base“ and the “most robust, productive, and innovative energy sector—one capable not just of fueling American economic growth but of being one of America’s leading export industries in its own right.”¹ This theme is reiterated in America’s AI Action Plan, which states that “[t]he power grid is the lifeblood of the modern economy and a cornerstone of national security [...] Escalating demand driven by electrification and the technological advancements of AI are increasing pressures on the grid. The United States must develop a comprehensive strategy to enhance and expand the power grid designed not just to weather these challenges, but to ensure the grid’s continued strength and capacity for future growth.”² Executive Order 14262, “Strengthening the Reliability and Security of the United States Electric Grid,” observes that the U.S. “is experiencing an unprecedented surge in electricity demand driven by rapid technological advancements, including the expansion of artificial intelligence data centers and an increase in domestic manufacturing. This increase in demand, coupled with existing capacity challenges, places a significant strain on our Nation’s electric grid. Lack of reliability in the electric grid puts the national and economic security of the American people at risk. The United States’ ability to remain at the forefront of technological innovation depends on a reliable supply of energy from all available electric generation sources and the integrity of our Nation’s electric grid.”³

Power inverters, electronic devices that convert direct current (DC) electricity into alternating current (AC) electricity, facilitate the connection of DC energy generation sources, such as solar panels, to the predominately AC U.S. energy grid. Imported power inverters can introduce new vulnerabilities in the United States’ economy and energy infrastructure and exacerbate existing ones. It has been estimated that more than 46 GW of electric power—the equivalent of 46 nuclear power plants—on the U.S. grid currently relies on inverters, and some have projected that inverter-based resources will account for a large part of new U.S. electricity generation going forward.⁴ According to data from the U.S. Energy Information Administration (EIA), inverter-based resources are expected to supply a significant portion of new U.S. generating capacity in the short term. Between January 1 and November 30, 2025, utility-scale solar capacity increased by more than 22,237 MW while battery storage added 13,357 MW of new capacity. EIA foresees a combined 58,658 MW from these inverter-based resources being added in the next 12 months.⁵

¹ <https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf>

² <https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf>

³ <https://www.whitehouse.gov/presidential-actions/2025/04/strengthening-the-reliability-and-security-of-the-united-states-electric-grid/>

⁴ <https://www.marketscale.com/industries/energy/data-centers-drove-half-of-us-electricity-demand-growth-as-time-to-power-becomes-the-defining-constraint-2d609d>

⁵ <https://electrek.co/2026/01/28/eia-99-of-new-us-capacity-in-2026-will-be-solar-wind-storage/>

Any unanticipated manipulation or disruption of the supply of power inverters or of the inverters themselves would likely compromise the United States' electricity supply and by extension threaten the economic prosperity and national security of the United States. In response to this threat, the White House convened an executive branch interagency body with appropriate national security expertise, *see* 47 U.S.C. § 1601(c)(1). This body, including appropriate national security agencies, *id.* § 1601(c)(4), determined jointly and severally that power inverters produced in a foreign country, regardless of the nationality of the producer, pose an unacceptable risk to the national security of the United States and to the safety and security of U.S. persons and should be included on the FCC's Covered List, unless the Department of War or Department of Homeland Security makes a specific determination to the FCC that a given power inverter or class of power inverters do not pose such risks. The interagency group and the agencies comprising it determined that power inverters produced in a foreign country, regardless of the nationality of the producer, presented the specific unacceptable risks of facilitating a supply chain vulnerability that could disrupt U.S. economic security, including sectors critical to national security, and create a cybersecurity risk that threatens the security of critical infrastructure and the safety of U.S. persons.

To allow producers of inverters time to meet the standards set forth in this determination, entities that produce inverters in a foreign country are encouraged to apply for Conditional Approvals (Annex A) which, if approved, will allow such producers to continue to receive FCC authorization during the transition period.

Summary of Supporting Evidence

Inverters provide the interconnection between otherwise incompatible forms of electricity and directly enable precise control over the flow of electrical energy in a system. These devices allow the DC generated by certain forms of power to be converted into the AC, for which the majority of the U.S. electrical grid utilizes. The growing importance of inverters to the U.S. electrical grid and the increased sophistication of inverters creates new vulnerabilities that malicious actors can exploit either through cyber-attacks or manipulation of the supply chain.

Although there are several U.S.-based power inverter manufacturers, at present many inverters and inverter components used in the U.S. are procured from suppliers headquartered outside the United States or owned or controlled by non-U.S. entities. While “[t]he inverter supply chain varies by inverter type, [...] the domestic market relies heavily on inverters from companies headquartered [in foreign countries],” according to a DOE fact sheet.⁶ In 2020, only seven percent of U.S. inverter shipments came from U.S. headquartered manufacturers, with utility-scale applications dominated by foreign companies.⁷

The lack of a secure U.S. supply chain for inverters and the continuous inflow of foreign-produced or controlled inverters and inverter components poses threats to U.S. economic and national security. One Idaho National Laboratory analysis referencing “notable supply chain

⁶ <https://www.energy.gov/sites/default/files/2022-02/Solar%20Energy%20Supply%20Chain%20Fact%20Sheet.pdf>

⁷ <https://www.energy.gov/sites/default/files/2022-02/Solar%20Energy%20Supply%20Chain%20Report%20-%20Final.pdf> (pg. 61)

challenges [...] particularly pronounced with inverters” found that “security considerations from an unsecured supply chain may include hardware or software that could introduce backdoors or security flaws, counterfeit components in the manufacturing process, poor quality components that have potential for digital failure, lack of transparency regarding components and their origins, and weak vendor security practices.”⁸

Inverters’ remote connectivity introduces additional vulnerabilities which compound as inverter-based resources proliferate on the U.S. grid. These vulnerabilities could enable foreign firms to turn off the inverters or use them to collect and exfiltrate data, facilitate remote access and surveillance by foreign government actors, or be otherwise exploited through a cyberattack. In their 2025 report to Congress, the U.S.-China Economic and Security Review Commission noted that “inverters are increasingly internet connected, providing users with real-time data collection and remote access” and “are particularly vulnerable to cyberattacks,” echoing concerns from Idaho National Laboratory, which has also warned of inverters’ “remote connectivity and associated potential to be misused by malicious threat actors.”⁹¹⁰

Attacks targeting power inverters could have devastating effects for the U.S. In 2025, one security research group reported 46 vulnerabilities in solar inverters manufactured by three major firms, which they warned “could lead to grid disruption and potential blackouts.”¹¹¹² The U.S.-China Economic and Security Review Commission’s 2025 report stated that a “cyberattack on solar inverters could direct them to either cut off solar power generation assets or add more power to the grid, leading to voltage and stability issues in the local distribution system, damaged and tripped equipment, and possibly a power outage.”¹³ The Electric Reliability Council of Texas (ERCOT), which operates the state’s power grid, has said that inverter-based resources’ tripping offline and disconnecting from the grid could lead to a rapid collapse of the ERCOT system in a worst-case scenario.¹⁴

There is evidence to suggest foreign entities have the capability to access power inverters after their installation in the U.S. Following a dispute between one non-U.S. inverter manufacturer and a U.S. distributor, the manufacturer remotely disabled its inverters in the U.S. and several other countries.¹⁵ A DOE supply chain assessment noted that “[a]lthough inverters can be designed and assembled in the United States, the application-specific integrated circuits and semiconductor power-handling components are almost entirely produced [outside the U.S.]. It

⁸ https://inldigitallibrary.inl.gov/sites/STI/STI/Sort_147618.pdf

⁹ https://inldigitallibrary.inl.gov/sites/STI/STI/Sort_147618.pdf

¹⁰ https://www.uscc.gov/sites/default/files/2025-11/2025_Annual_Report_to_Congress.pdf

¹¹ <https://www.forescout.com/research-labs/sun-down-a-dark-side-to-solar-energy-grids/>

¹² <https://www.techworm.net/2025/03/46-critical-flaws-in-solar-inverters.html>

¹³ https://www.uscc.gov/sites/default/files/2025-11/2025_Annual_Report_to_Congress.pdf

¹⁴ <https://www.governing.com/infrastructure/texas-power-company-warns-of-catastrophic-failure-if-storage-issues-go-unresolved>

¹⁵ <https://content.striderintel.com/wp-content/uploads/2025/11/Strider-Report-In-Broad-Daylight-2025.pdf>

will be challenging to significantly reduce the risk of foreign interference in inverters unless the embedded electronic components are also produced in the United States.”¹⁶

Given these considerations, we determine that power inverters produced in a foreign country, regardless of the nationality of the producer, pose an unacceptable risk to the national security of the United States and to the safety and security of U.S. persons and should be included on the FCC’s Covered List, unless the Department of War or Department of Homeland Security makes a specific determination to the FCC that a given power inverter or class of power inverters do not pose such risks..

Definitions

FCC: For the purpose of this determination, the term “FCC” means the Federal Communications Commission.

Covered List: For the purpose of this determination, the term “Covered List” shall mean the list of covered communications equipment or services published on the FCC’s website under 47 U.S.C. 1601(a).

Power Inverter: For the purpose of this determination, the term “power inverter” shall mean a device:

- (a) A bi-directional power device or system that converts direct current electricity to alternating current electricity, or converts alternating current electricity to direct current electricity, to include microinverters, string inverters, central inverters, and hybrid (battery-based) inverters; and
- (b) Contains components that enable remote communication, control, sensing, data-collection, or monitoring through Wi-Fi, cellular, Bluetooth, or other similar connections.

Foreign-Produced: For the purpose of this determination, the term “foreign-produced” refers to any article that does not qualify as a “domestic end product,” as that term is defined in 48 CFR § 25.101(a).

¹⁶ <https://www.energy.gov/sites/default/files/2022-02/Solar%20Energy%20Supply%20Chain%20Report%20-%20Final.pdf>