



PUBLIC NOTICE

Federal Communications Commission
45 L Street NE
Washington, DC 20554

News Media Information 202-418-0500
Internet: www.fcc.gov

DA 26-786

Released: July 28, 2026

FCC'S PUBLIC SAFETY AND HOMELAND SECURITY BUREAU ANNOUNCES ADDITION OF FOREIGN-PRODUCED POWER INVERTERS AND ADVANCED ROBOTIC DEVICES TO FCC COVERED LIST

WC Docket No. 18-89, ET Docket No. 21-232, EA Docket No. 21-233

The Federal Communications Commission's (FCC or Commission) Public Safety and Homeland Security Bureau (PSHSB) maintains a list of equipment and services (Covered List) that have been determined to "pose an unacceptable risk to the national security of the United States or the security and safety of United States persons."¹ Pursuant to section 2 of the Secure and Trusted Communications Networks Act of 2019 (Secure Networks Act)² and sections 1.50002(a) and 1.50003 of the Commission's rules,³ PSHSB announces the addition of foreign-produced power inverters and advanced robotic devices to the Covered List.

National Security Determinations. The White House convened an Executive Branch interagency body with appropriate national security expertise, including appropriate national security agencies identified in the Secure Networks Act.⁴ On July 27, 2026, the Executive Branch interagency body sent the FCC two National Security Determinations.

Power inverters. The first [National Security Determination](#) addresses the unacceptable risks posed by power inverters produced in foreign countries.⁵ Among other points, the National Security Determination states:

"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 . . . 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

¹ Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 133 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1601-1609) (Secure Networks Act); 47 CFR §§ 1.50002, 1.50003. For the current version of the Covered List, see Federal Communications Commission, *List of Equipment and Services Covered By Section 2 of The Secure Networks Act*, <https://www.fcc.gov/supplychain/coveredlist> (last updated Mar. 18, 2026).

² 47 U.S.C. § 1601.

³ 47 CFR §§ 1.50002(a), 1.50003; see also *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Second Report and Order, 35 FCC Rcd 14284 (2020) (*Supply Chain Second Report and Order*).

⁴ See 47 U.S.C. § 1601(c)(1).

⁵ The Power Inverters National Security Determination is attached as Appendix B to this Public Notice.

or use them to collect and exfiltrate data, facilitate remote access and surveillance by foreign government actors, or be otherwise exploited through a cyberattack.”⁶

As a result of the threats described in the National Security Determination, the Executive Branch interagency body determined that power inverters produced in a foreign country pose the following unacceptable risks to the United States: (1) “facilitating a supply chain vulnerability that could disrupt U.S. economic security, including sectors critical to national security”; and (2) “creat[ing] a cybersecurity risk that threatens the security of critical infrastructure and the safety of U.S. persons.”⁷

Based on these findings, the Executive Branch interagency body, including appropriate national security agencies, determined that the following equipment and services should be added to the FCC’s Covered List because they pose an unacceptable risk to the national security of the United States and to the safety and security of U.S. persons: “Power inverters produced in a foreign country, regardless of the nationality of the producer, 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.”⁸

Advanced robotic devices. The second [National Security Determination](#) addresses the unacceptable risks posed by advanced robotic devices produced in foreign countries.⁹ Among other points, the National Security Determination states:

“The networked capabilities of advanced robotic systems create extensive vulnerabilities and vectors for attacks that can manipulate the data and physical operation of the advanced robotic system. Relying on foreign-produced advanced robotic devices presents unacceptable supply chain and cybersecurity vulnerabilities . . . Advanced robotic devices collect data that could be leveraged by malign actors to surveil Americans, enhance the capabilities of foreign intelligence services, or to remotely commandeer the robots.”¹⁰

As a result of the threats described in the National Security Determination, the Executive Branch interagency body determined that advanced robotic devices produced in foreign countries presented the following unacceptable risks: (1) “posing a supply chain vulnerability that could disrupt U.S. economic and national security”; and (2) “creating a cybersecurity risk that threatens the security of critical infrastructure and thus the safety and security of U.S. persons.”¹¹

Based on these findings, the Executive Branch interagency body, including several appropriate national security agencies, determined that the following equipment should be added to the FCC’s Covered List because they pose an unacceptable risk to the national security of the United States and to the safety and security of U.S. persons: “All foreign-produced advanced robotic devices, unless the

⁶ Power Inverters National Security Determination at 2-3.

⁷ *Id.* at 2.

⁸ *Id.* at 2.

⁹ The Advanced Robotic Devices National Security Determination is attached as Appendix C to this Public Notice.

¹⁰ Advanced Robotic Devices National Security Determination at 2-3.

¹¹ *Id.* at 2.

Department of War (DOW) transmits to the FCC a specific determination that a given foreign-produced advanced robotic device, or a class of such devices, does not pose such risks.”¹²

The Covered List. We find that each National Security Determination constitutes a specific determination of an unacceptable risk to the national security of the United States or the security or safety of United States persons pursuant to section 2 of the Secure Networks Act.¹³ Therefore, we conclude that the Commission is required to place the identified equipment on the Covered List.¹⁴ We update the Covered List to include:

“Foreign-produced power inverters, except power inverters which have been granted a Conditional Approval by DoW or DHS”; and

“Foreign-produced advanced robotic devices, except advanced robotic devices which have been granted a Conditional Approval by DoW.”

We accept the National Security Determinations’ definitions of “foreign-produced,” “power inverters,” and “advanced robotic devices,” as provided in the Appendices below.

Conditional Approvals. The Executive Branch interagency body has established a process in which entities producing power inverters or advanced robotic devices in a foreign country can request an evaluation as to whether their devices do not pose unacceptable risks to national security and receive Conditional Approvals that would exempt the devices from the Covered List. DoW or DHS may evaluate such submissions for power inverters. DoW may evaluate such submissions for advanced robotic devices. Entities seeking Conditional Approvals for power inverters must provide the information requested in the [Power Inverters Guidance Document](#). Likewise, entities seeking Conditional Approvals for advanced robotic devices must provide the information requested in the [Advanced Robotic Devices Guidance Document](#).

If we receive a further specific determination from DoW or DHS that a given power inverter or advanced robotic device, or class of such devices, does not pose unacceptable risks, we will further update the Covered List.

PSHSB takes this action under its authority and obligation to publish and maintain the Covered List. Sections 1.50002(a) and 1.50003 of the Commission’s rules require PSHSB to publish the Covered List on the Commission’s website, to maintain and update the Covered List, and to monitor the status of determinations.¹⁵

Equipment Authorization Impacts of the Covered List. Under the Commission’s existing rules in section 2.903(a), once added to the Covered List, “covered” equipment is prohibited from receiving equipment authorizations.¹⁶ Moreover, pursuant to section 2.911 of the Commission’s rules, all applications seeking equipment authorization from the Commission must certify that the equipment is not prohibited from receiving an equipment authorization by virtue of being “covered equipment.”¹⁷ By so

¹² Advanced Robotic Devices National Security Determination at 4.

¹³ 47 U.S.C. § 1601(c).

¹⁴ 47 U.S.C. § 1601(b)-(d).

¹⁵ 47 CFR §§ 1.50002(a), 1.50003. *See Supply Chain Second Report and Order*, 35 FCC Rcd at 14317, 14319, 14325, paras. 72, 77, 92.

¹⁶ 47 CFR § 2.903(a).

¹⁷ 47 CFR § 2.911(d)(5)(i).

certifying, the applicant would be certifying that the equipment does not qualify as equipment listed in this Public Notice as “covered.” We clarify that these updates will not implicate various rules and programs applicable to entities “identified” on the Covered List, because this newly-covered equipment is identified by place of production, not by entity.¹⁸

The updated Covered List is attached as Appendix A to this Public Notice and is published on the Bureau’s website at <https://www.fcc.gov/supplychain/coveredlist>.¹⁹ The Power Inverters National Security Determination is attached as Appendix B. The Advanced Robotic Devices National Security Determination is attached as Appendix C.

We note the continued availability of FCC staff guidance pursuant to sections 0.191 and 0.31(i) of the Commission’s rules. Commission staff will provide guidance to TCBs, test labs, and equipment authorization applicants on the impact of these updates.

For further information, please contact Chris Smeenk, Attorney Advisor, Operations and Emergency Management Division, Public Safety and Homeland Security Bureau at 202-418-1630 or Chris.Smeenk@fcc.gov.

¹⁸ See 47 CFR §§ 2.903, 2.906, 2.907, 2.911, 2.929, 2.932, 2.938, 2.1033, 2.1043.

¹⁹ The FCC website also contains a list of certain affiliates and subsidiaries of entities identified on the Covered List. The list of affiliates and subsidiaries does not constitute a comprehensive list of all entities that the Commission may find, upon further examination, to qualify as relevant subsidiaries or affiliates of entities on the Covered List. Those entities, whether or not they currently provide covered communications equipment or services, are subject to the Commission’s prohibitions, such as the prohibition against obtaining authorizations for covered equipment. See *Reminder: Communications Equipment And Services On The Covered List Pose An Unacceptable Risk To National Security*, National Security Advisory No. 2025-01, DA 25-927, note 3 (PSHSB Oct. 14, 2025).

APPENDIX A

COVERED LIST (Updated July 28, 2026)*†±

Covered Equipment or Services*	Date of Inclusion on Covered List
Telecommunications equipment produced or provided by Huawei Technologies Company , including telecommunications or video surveillance services produced or provided by such entity or using such equipment.	March 12, 2021
Telecommunications equipment produced or provided by ZTE Corporation , including telecommunications or video surveillance services provided or provided by such entity or using such equipment.	March 12, 2021
Video surveillance and telecommunications equipment produced or provided by Hytera Communications Corporation , to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services produced or provided by such entity or using such equipment.	March 12, 2021
Video surveillance and telecommunications equipment produced or provided by Hangzhou Hikvision Digital Technology Company , to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services produced or provided by such entity or using such equipment.	March 12, 2021
Video surveillance and telecommunications equipment produced or provided by Dahua Technology Company , to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services produced or provided by such entity or using such equipment.	March 12, 2021
Information security products, solutions, and services supplied, directly or indirectly, by AO Kaspersky Lab or any of its predecessors, successors, parents, subsidiaries, or affiliates.	March 25, 2022
International telecommunications services provided by China Mobile International USA Inc. subject to section 214 of the Communications Act of 1934.	March 25, 2022
Telecommunications services provided by China Telecom (Americas) Corp. subject to section 214 of the Communications Act of 1934.	March 25, 2022
International telecommunications services provided by Pacific Networks Corp. and its wholly-owned subsidiary ComNet (USA) LLC subject to section 214 of the Communications Act of 1934.	September 20, 2022
International telecommunications services provided by China Unicom (Americas) Operations Limited subject to section 214 of the Communications Act of 1934.	September 20, 2022
Cybersecurity and anti-virus software produced or provided by Kaspersky Lab, Inc. or any of its successors and assignees.	July 23, 2024
Uncrewed aircraft systems (UAS) and UAS critical components produced in a foreign country ^{††} —except: (a) UAS and UAS critical components included on the Defense Contract Management Agency's (DCMA's) Blue UAS Cleared List, until January 1, 2028, [#] (b) UAS and UAS critical components that qualify as “domestic end products” under the Buy American Standard, 48 CFR 25.101(a) , until January 1, 2028; (c) devices which have been granted a Conditional Approval by DoW or DHS ; and	December 22, 2025 Updated: January 7, 2026 Updated: March 18, 2026

(d) foreign-produced “Toy Drones,” as defined in the National Security Determination , and “Toy Drones that contain foreign-produced components.”	Updated: June 15, 2026
All communications and video surveillance equipment and services listed in Section 1709(a)(1) of the FY25 National Defense Authorization Act (Pub. L. 118-159).	Updated: July 21, 2026
Routers [^] produced in a foreign country, except routers which have been granted a Conditional Approval by DoW or DHS .	March 23, 2026
International telecommunications services provided by Digitalssystem Technology Inc. , subject to section 214 of the Communications Act of 1934.	July 7, 2026
Foreign-produced power inverters, [£] except power inverters which have been granted a Conditional Approval by DoW or DHS .	July 28, 2026
Foreign-produced advanced robotic devices, [‡] except advanced robotic devices which have been granted a Conditional Approval by DoW .	July 28, 2026

*The inclusion of producers or providers of equipment or services named on this list should be read to include the subsidiaries and affiliates of such entities.

†Where equipment or services on the list are identified by category, such category should be construed to include only equipment or services capable of the functions outlined in sections 2(b)(2)(A), (B), or (C) of the Secure and Trusted Communications Networks Act of 2019, 47 U.S.C. § 1601(b)(2)(A)-(C).

±The scope of the Covered List is affected by the [Conditional Approvals](#) that we have received.

††For purposes of inclusion of UAS and UAS critical components, we incorporate the definitions included in the associated [National Security Determination](#).

#The “Blue UAS list” referred to in the [National Security Determination](#) is the combination of the “Blue UAS Cleared List” at <https://bluelist.appsplatformportals.us/Cleared-List/> and the list of compliant UAS components and software at <https://bluelist.appsplatformportals.us/Framework/>. We use the term “Blue UAS Cleared List” to refer to both lists.

^For purposes of inclusion of routers, we incorporate the definitions included in the associated [National Security Determination](#).

£For purposes of inclusion of power inverters, we incorporate the definitions included in the associated [National Security Determination](#).

‡For purposes of inclusion of advanced robotic devices, we incorporate the definitions included in the associated [National Security Determination](#).

APPENDIX B

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://indigitallibrary.inl.gov/sites/STI/STI/Sort_147618.pdf

⁹ https://indigitallibrary.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>

APPENDIX C

National Security Determination on the Threat Posed by Foreign-Produced Advanced Robotic Devices*July 27, 2026***Summary of Determination:**

The Trump Administration's AI Action Plan identifies robotics as a next-generation technology essential to our defense and national security.¹ Robotics technology is rapidly advancing, driven by enhancements in AI, sensing, and actuation technologies. Advanced robotic devices will be critical to creating efficiencies in our economy, dominating on the battlefield, and securing our homeland. To ensure the United States is able to take advantage of this generational technology, the United States must have an independent and resilient robotics supply chain and industrial base. As the 2025 National Security Strategy states, "The United States will reindustrialize its economy, 're-shore' industrial production, and encourage and attract investment in our economy and our workforce, with a focus on the critical and emerging technology sectors that will define the future."²

As the technology matures, advanced robotic devices have growing use cases in monitoring and securing critical infrastructure.³ Robots are often equipped with high-fidelity sensors, including Light Detection and Ranging (LiDAR), tactile, acoustic, and thermal sensors that collect and maintain sensitive data on their surroundings. Advanced robotic devices are inherently networked systems which creates broad attack surfaces and leaves them vulnerable to data exfiltration, remote disruption of the physical robot, and dependencies on unsecure over the air updates.⁴ The data collected by advanced robotic devices, especially those securing sensitive locations and critical infrastructure must be protected and maintained in the United States.

In addition to securing critical infrastructure, advanced robotic devices also have applications in industrial manufacturing, from material handling to order fulfillment.⁵ Integrating these technologies into American manufacturing will lower production costs, increase output, and support America's reindustrialization. In order for the American economy to rely on these technologies, we must have a secure domestic advanced robotics supply chain and industrial base.

Advanced robotic devices such as Unmanned Ground Vehicles (UGVs) and quadrupeds will be essential to the modern battlefield. UGVs will enable the U.S. military to augment American

¹ The White House. "Winning the Race: America's AI Action Plan." July 2025. <https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf>

² The White House. "National Security Strategy of the United States of America." November 2025. <https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf>

³ Lloyd Lee. Business Insider. "Robot dogs are protecting data centers. Operators are seeing payoffs." March 2024. <https://www.businessinsider.com/robot-dogs-quadruped-data-center-security-boston-dynamics-ghost-robotics-2026-3>; Kristina Webb. Palm Beach Daily News. "Secret Service uses robot dogs to guard Trump's Mar-a-Lago in Florida." November 2024. <https://www.palmbeachdailynews.com/story/news/local/2024/11/20/robot-dogs-added-to-security-detail-at-trumps-mar-a-lago-in-florida/76429766007/>

⁴ AUVSI Partnership for Robotics Competitiveness. AUVSI. "Securing U.S. Leadership in Robotics and Physical Artificial Intelligence." February 2026.

⁵ Boston Dynamics. "Boston Dynamics Unveils New Atlas Robot to Revolutionize Industry." January 2026. <https://bostondynamics.com/blog/boston-dynamics-unveils-new-atlas-robot-to-revolutionize-industry/>

warfighters on the frontlines in a way that will save American lives while still inflicting damage on our adversaries. The U.S. military is already pursuing advanced robotics for autonomous breaching, resupply missions, force protection, and offensive strike.⁶ The use of UGVs in current conflicts shows how attritable unmanned assets can inflict casualties while offsetting the effects of exquisite conventional capabilities.

As our dependence grows on advanced robotic devices for critical infrastructure protection, manufacturing, and U.S. military dominance, it is vital that we have a secure domestic supply chain and industrial base for advanced robots. The networked capabilities of advanced robotic systems create extensive vulnerabilities and vectors for attacks that can manipulate the data and physical operation of the advanced robotic system. Relying on foreign-produced advanced robotic devices presents unacceptable supply chain and cybersecurity vulnerabilities.

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), comprising agencies that included appropriate national security agencies, *id.* § 1601(c)(4), which determined jointly and severally that: All foreign-produced advanced robotic devices 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 (DOW) transmits to the FCC a specific determination that a given foreign-produced advanced robotic device, or a class of such devices, does not pose such risks. The interagency group and the agencies comprising it determined that foreign-produced advanced robotic devices presented the specific unacceptable risks of (a) posing a supply chain vulnerability that could disrupt U.S. economic and national security, and (b) creating a cybersecurity risk that threatens the security of critical infrastructure and thus the safety and security of U.S. persons.

To facilitate this transition period, entities that produce advanced robotic devices 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 for their products while they work to onshore manufacturing and address the U.S. government's national security concerns described above.

Supporting Evidence:

Advanced robotic devices, including four-legged quadrupeds, bipeds, and wheeled and tracked vehicles, are gaining popularity in a diverse range of use-cases, from providing physical security at sensitive locations, enabling industrial inspections in environments dangerous to humans, and providing military advantages on the battlefield. Recent improvements in advanced robotics and the critical components within robots are already enabling productivity gains in key sectors like manufacturing while helping employers overcome critical labor gaps.⁷ The global supply chain

⁶ Kyle Richardson. U.S. Army. "Autonomous Breaching System will surpass legacy systems to enhance breaching operations." January 2026.
https://www.army.mil/article/290196/autonomous_breaching_system_will_surpass_legacy_systems_to_enhance_breaching_operations

⁷ Ethan Karp. Forbes. "Humanoid Robots in Manufacturing: Timelines, Cost, and Opportunity." October 2025.
<https://www.forbes.com/sites/ethankarp/2025/10/29/humanoid-robots-in-manufacturing-timelines-cost-and-opportunity/>

for advanced robotic devices and their critical components, including actuators, end effectors, batteries, and sensors, are increasingly consolidated in a handful of countries, some of which have repeatedly shown willingness to disrupt American supply chains in times of geopolitical tensions.⁸ If the United States continues to rely on foreign sources of advanced robotic devices and critical components, it will subject the parts of the U.S. economy and national security enterprise that are reliant on these robots to the whims of foreign entities that could disrupt or degrade the supply chains at a time of their choosing. This reliance is an unacceptable supply chain vulnerability that presents an immediate national security threat.

In addition to the supply chain vulnerability, foreign-produced advanced robotics devices present an unacceptable cybersecurity and safety risk. Advanced robotic devices collect data that could be leveraged by malign actors to surveil Americans, enhance the capabilities of foreign intelligence services, or to remotely commandeer the robots. In early 2026 a security vulnerability was discovered in a category of foreign-produced advanced robotic devices that enabled actors to remotely access thousands of robots that were in homes around the world.⁹ This vulnerability offered ready access to live camera feeds, microphone audio, and detailed maps of consumers' homes. In another recent example, a cybersecurity vulnerability in certain foreign-produced humanoid robots allowed a remote actor to take over the operations of the humanoid robot and scan for other humanoid robots in the area, providing malign actors the ability to create a humanoid botnet that could spread without user intervention.¹⁰ Additionally, in April 2025, security researchers identified a potentially pre-installed backdoor on foreign-produced robotic quadrupeds that gave access to the camera feed and allowed them to take full control of the robot quadruped.¹¹ As advanced robotic devices increase in relevancy across critical infrastructure security, manufacturing, and the military, it is critical that they are secure and reliable systems which cannot be remotely accessed or manipulated by malign actors.

Many advanced robotic devices also have high fidelity sensors, including LiDAR, electro-optical/infrared, acoustic, and thermal, allowing the advanced robotic device to create datasets that have value for foreign intelligence services, including high-fidelity maps of the environment in which the robot operates.¹² When advanced robotic devices and their critical components are sourced from foreign countries, U.S. stakeholders have limited visibility into the development practices and software provenance of device. This magnifies the risk that vulnerabilities remain unaddressed, updates are withheld, or functionality is altered in ways that degrade the device. Some legal regimes in foreign countries prohibit entities from disclosing cyber security vulnerabilities to customers, increasing the risk that foreign governments will use vulnerabilities

⁸ Raffaele Huang. The Wall Street Journal. "Under the Skin of America's Humanoid Robots: Chinese Technology." April 2026. <https://www.wsj.com/tech/under-the-skin-of-americas-humanoid-robots-chinese-technology-27dd4fdf>

⁹ The Guardian. "The accidental hacker: how one man gained control of 7,000 robots." February 2026. <https://www.theguardian.com/lifeandstyle/2026/feb/24/accidental-hacker-how-one-man-gained-control-robots->

¹⁰ Evan Ackerman. IEEE Spectrum. "Exploit Allows for Takeover of Fleets of Unitree Robots." September 2025. <https://spectrum.ieee.org/unitree-robot-exploit>

¹¹ Sam Sabin. Axios. "Chinese robotics manufacturer left backdoor in product." April 2025. https://www.axios.com/2025/04/01/threat-spotlight-backdoor-in-chinese-robots-future-of-cybersecurity?utm_source=chatgpt.com

¹² Craig Singleton and Mark Montgomery. Foundation for Defense of Democracies. "Laser Focus: Countering China's LiDAR Threat to U.S. Critical Infrastructure and Military Systems." December 2024. <https://www.fdd.org/analysis/2024/12/02/laser-focus-countering-chinas-lidar-threat-to-u-s-critical-infrastructure-and-military-systems/>

in advanced robotics or their critical components to manipulate or exfiltrate data from the device.¹³

Given this evidence, the U.S. government has a clear and compelling national security concern that foreign-produced advanced robotic devices could be weaponized to directly harm U.S. national security and U.S. persons. As a result, a White House convened executive branch interagency body determined that all foreign-produced advanced robotic devices 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 DOW transmits to the FCC a specific determination that a given foreign-produced advanced robotic device, or a class of such devices, does not pose such risks.

Definitions:

Advanced Robotic Devices: For the purpose of this determination, the term “advanced robotic devices” means:

- (A) A mechanical mobile device, including autonomous mobile robots, humanoid robots, and quadrupeds, that –
 - i. Is capable of locomotion, obstacle avoidance, navigation, or movement on the ground;
 - ii. Operates at a distance from a human operator or supervisor based on commands or in response to sensor data or any combination thereof; and
 - iii. The combined weight of the device and, if applicable, ground station or docking station is over 4.4lbs; and
 - iv. Contains a component falling within each of the below subparagraphs:
 - i. a sensor capable of perceiving its environment;
 - ii. a component that is capable of providing network connectivity (wired or wireless, including Bluetooth/WiFi, cellular, or satellite) with connection speeds of at least 200 kbps in either direction; and
 - iii. software running either locally or remotely, including firmware and AI or machine-learning model weights, that controls the robot's autonomous navigation or movement perception, data collection, or remote command-and-control; and
- (B) Does not include:
 - i. A “connected vehicle,” as that term is defined in 15 CFR § 791.301, but including a connected vehicle of any gross weight;
 - ii. A vehicle operated only on a rail line;
 - iii. An “uncrewed aircraft” or “uncrewed aircraft system,” as defined in 47 CFR § 78.5;
 - iv. An unmanned underwater vehicle that is able to operate without a human occupant;
 - v. Items that are classified as devices under section 513 of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. §360c), including surgical instruments,

¹³ Devin Thorne and Samantha Hoffman. “China’s vulnerability disclosure regulations put state security first.” The Australian Strategic Policy Institute. August 2021. <https://www.aspistrategist.org.au/chinas-vulnerability-disclosure-regulations-put-state-security-first/>

- medical and surgical robotic systems, external limb prostheses and their components, and ambulatory and mobility assistive devices (such as canes, crutches, walkers, and wheelchairs), whether or not powered, and whether the item was cleared under section 510(k), approved under section 515, classified under section 513(f)(2), or exempt from premarket notification; and
- vi. A fixed, stationary, non-mobile robot, including articulating, parallel/delta, Cartesian/gantry, or Selective Compliance Assembly, or Articulated, Robot Arm (SCARA) robots intended for industrial or medical use.

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

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