

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 fulfilment.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).