

**Congress of the United States**  
**Washington, DC 20515**

March 2, 2026

The Honorable Howard W. Lutnick  
Secretary  
U.S. Department of Commerce  
1401 Constitution Avenue NW  
Washington, DC 20230

The Honorable Brendan Carr  
Chairman  
Federal Communications Commission  
45 L Street NE  
Washington, DC 20554

Dear Secretary Lutnick and Chairman Carr:

We write to request a formal investigation into Anker Innovations, a People's Republic of China's (PRC) company that poses unacceptable risks to U.S. national security and consumer safety. Anker makes several product brands including Eufy internet-connected smart home products and SOLIX battery technologies that have equipment authorizations issued by the Federal Communications Commission (Commission).

As you are aware, the Secure and Trusted Communications Networks Act directs the Commission to periodically update the Covered List of communications equipment and services that are deemed to pose an unacceptable risk to national security or the security and safety of United States persons, which can be based on a determination made by the Department of Commerce or other sources.

Anker, through its Eufy brand, has a documented history of significant security vulnerabilities related to its security camera business and has been accused of misleading the public about these issues. In 2025, the State of New York secured a \$450,000 settlement from companies distributing Eufy home security products after finding that “video streams from the cameras were not always securely encrypted and could be accessible to anyone with the relevant link without authentication.” Furthermore, “the OAG’s investigation revealed that, in certain situations, video sent over the internet from eufy home security products was not protected by end-to-end encryption, and that at least a portion of the connection did not use any type of encryption at all.” Public reports confirm that Anker eventually admitted its statements on Eufy security camera encryption were inaccurate and that unencrypted video streams were accessible.

Anker’s Eufy brand offers a variety of network-connected devices: indoor and outdoor cameras, surveillance systems, video doorbells, “smart” projectors, app-enabled chargers, smart speakers, 3D printers with Wi-Fi modules, and what it claims to be the “World’s First NVR Security System with Local AI Agent.” Eufy also announced a new Face Management function for the S380 HomeBase camera system which will enable the camera to capture faces and generate a local collection. It will notify the owner and automatically perform some interactions after seeing a person appear several times. These devices can transmit audio, video, and metadata over the internet, providing potential vectors for both remote surveillance network mapping, and traffic analysis.

As a PRC company, Anker is subject to the People's Republic of China National Intelligence Law of 2017, Article 7, which compels "all organizations and citizens" to support, assist, and cooperate with state intelligence efforts upon request. This statutory regime applies to Anker and all its subsidiaries, creating a legally binding pathway for the Chinese government—including the People's Liberation Army (PLA)—to compel cooperation, obtain data, or alter product functionality for intelligence purposes.

In addition, Anker offers many of these systems on U.S. military exchange websites, and for direct sales, Anker also provides up to a 20% discount on its Eufy products to current and former U.S. military, their spouses and dependents. While these are retail sales, rather than direct Department of War procurement, the FCC has previously noted that the presence of high-risk network-connected devices in sensitive physical locations can constitute a security risk.

Anker also potentially exploits U.S. trade and market mechanisms to gain an unfair and dominant market position, posing a significant risk to American businesses and national security. Anker is a major Chinese brand that benefits from substantial Chinese Communist Party (CCP) backing that fundamentally distorts fair market competition, undercutting American competitors. Public financial disclosures reveal that Anker received at least \$12 million in confirmed PRC government subsidies in 2023, with acknowledgments that the total extent of subsidies may be understated. This state-sponsored support almost certainly enables Anker to engage in aggressive, anti-competitive pricing that non-subsidized American companies cannot sustain. This advantage has fueled remarkable growth for Anker, whose revenue nearly tripled between 2020 and 2024, reflecting a compound annual growth rate (CAGR) of approximately 27%.

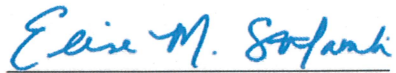
At worst, Anker could introduce foreign surveillance and destructive capabilities into American households. At best, it is leveraging anti-competitive practices to gain a controlling position in a strategic U.S. supply chain. Therefore, we believe there is an urgent and compelling need for the Commerce Department and Federal Communications Commission to launch a formal investigation into Anker Innovations and respond to the following questions:

1. What is Anker Innovation's ownership structure, including the role of its Chinese parent company?
2. Do Anker's devices or components transmit data to servers located in China or to networks controlled by Anker's Chinese parent?
3. What is the function of the microphones in Anker devices and what do they record? Is all this properly disclosed to consumers?
4. Given China's National Security Law, which mandates data cooperation with the CCP, what steps can the FCC take to prevent U.S. consumer data collected by Anker devices from being accessed by foreign governments?
5. Does the FCC's equipment authorization process account for the possibility that a device or its components could surveil Americans and transmit data to a foreign adversary nation?
6. What additional measures is the FCC considering to ensure that foreign-manufactured devices — particularly those linked to Chinese entities — do not compromise U.S. privacy or security?

Taking action is crucial not only to shield American brands and innovators from unfair competition by China, but also to safeguard U.S. citizens from the risk of their personal data being exploited and to reduce exposure to the inherent dangers of cheaply made, potentially compromised electronic products.

We look forward to your prompt response and welcome the opportunity to collaborate with your agency on this critical matter of economic security and public safety.

Sincerely,



Elise M. Stefanik  
Elise M. Stefanik  
Chairwoman  
House Republican Leadership



Rick Scott  
Rick Scott  
United States Senator