PUBLIC COMMENT: FOUNDATION FOR DEFENSE OF DEMOCRACIES

Federal Communications Commission

Seeking Comment on Prohibiting Importation and Marketing of Previously Authorized Covered Communications Equipment Added to the Covered List in 2024 or Earlier

[PSHSB & OET: PS Docket No. 26-72; DA 26-294; FR ID 339368]

AUTHORS

Jack Burnham
Senior Research Analyst, FDD's China Program

RADM (Ret.) Mark Montgomery
Senior Director and Senior Fellow, FDD's Center on Cyber and Technology Innovation

Washington, DC
April 13, 2026

FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

www.fdd.org

Introduction

The FCC has long recognized the national security threat posed by certain Chinese telecommunications firms. Beginning in March 2021, the Commission added a series of Chinese national champions — Huawei, ZTE Corporation, and Hangzhou Hikvision Digital Technology Company (Hikvision) — to its Covered List due to their reported ties to the People's Liberation Army (PLA) and their role in undermining the security of American networks.

While the FCC has worked to remove these firms from U.S. supply chains, their legacy equipment remains eligible for use in the United States due to their prior authorization. That allows these threats to quietly proliferate across the American market. As such, the Commission should broaden the scope of its prohibitions under the Covered List to encompass a fuller range of products produced prior to 2024.

This move will close a regulatory loophole that allows Chinese firms to compromise U.S. networks. It will also align with the FCC's previous actions — in November 2022, the Commission strengthened its prohibitions on the importation and sale of covered equipment under its equipment authorization program.[1]

Chinese Firms on the Covered List Maintain Access to the American Market via Regulatory Loopholes

While Huawei, ZTE Corporation, and Hikvision were added to the Covered List prior to 2024, authorized products produced by these firms may still be sold in the United States despite the firms continuing to engage in troubling patterns of behavior, including maintaining ties to both Beijing and the Chinese military. Banning the sale of new products does not mitigate the potential backdoors installed in older equipment. Continuing to permit this equipment to be sold allows the problem to metastasize within American telecommunications networks.

Huawei remains a Chinese national champion, having branched out from providing telecommunications equipment to forming a core aspect of China's artificial intelligence (AI) ecosystem as a key provider of domestic computing power. The problem is no longer simply Huawei employees providing technical support to the Chinese military.[2] The firm is now a key supplier for China's broader defense industrial base.[3] Huawei provides advanced AI chips to Alibaba and Zhipu AI. The White House reportedly accused the former in November 2025 of providing computing to the Chinese military, while the Department of Commerce added the

[1] Jiwon Ma, "Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program," *Foundation for Defense of Democracies*, July 7, 2025. (https://www.fdd.org/analysis/2025/07/07/protecting-against-national-security-threats-to-the-communications-supply-chain-through-the-equipment-authorization-program)

[2] "Huawei Personnel Worked With China Military on Research Projects," *Bloomberg News*, June 26, 2019. (https://www.bloomberg.com/news/articles/2019-06-27/huawei-personnel-worked-with-china-military-on-research-projects)

[3] Jill Gallagher, "U.S. Restrictions on Huawei Technologies: National Security, Foreign Policy, and Economic Interests," *Congressional Research Service*, January 5, 2022. (https://www.congress.gov/crs-product/R47012)

latter to its Entity List in January 2025 for contributing to Chinese military modernization.[4] U.S. officials have also long accused Huawei of utilizing backdoors pre-installed in its products, including those positioned near U.S. military installations — an FBI investigation in 2022 found that found Huawei could disrupt U.S. nuclear communications essential for command and control.[5]

Placed on the Covered List in March 2021, ZTE Corporation also maintains a dense network of ties to China's military industrial base. Along with reportedly being considered a national champion due to its financial ties to Beijing, the firm also maintained an ownership structure dominated by the China Aerospace Science and Technology Corporation and the China Aerospace Science and Industry Corporation, both of which are involved in designing precision weapons and military satellite communications.[6]

Under an agreement brokered by Washington and Beijing, ZTE agreed to $1.19 billion in fines to Commerce for violating U.S. sanctions on Iran and North Korea, at the time the largest-ever criminal fine in a sanctions case, and was placed on the Entity List.[7] U.S. authorities also expressed concerns that ZTE's products may provide backdoors for Beijing to conduct espionage. The company's own revelation in 2012 that some of its handsets presented embedded vulnerabilities — vulnerabilities that independent security experts termed "highly unusual" — prompted many of these concerns.[8]

Hikvision also remains a threat to U.S. national security. Prior to being listed in 2021, the PLA allegedly designated the firm as a "top tier supplier" in 2014 for its contributions of drones,

---

[4] "Huawei's new AI chip finds favour with ByteDance, Alibaba which plan to place orders, sources say," *Reuters*, March 27, 2026. (https://www.reuters.com/world/china/huaweis-new-ai-chip-find-favour-with-bytedance-alibaba-which-plan-place-orders-2026-03-27); Demetri Sevastopulo, "White House memo claims Alibaba is helping Chinese military target US," *Financial Times* (UK), November 14, 2025. (https://www.ft.com/content/30fb83a0-8cb9-4805-b5d2-19b5ef510043?syn-25a6b1a6=1); Addition of Entities to and Revision of Entry on the Entity List, Department of Commerce, Bureau of Industry and Security, 90 Federal Register 4617, January 16, 2025. (https://www.govinfo.gov/app/details/FR-2025-01-16/2025-00704)

[5] Jiwon Ma, "Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program," *Foundation for Defense of Democracies*, July 7, 2025. (https://www.fdd.org/analysis/2025/07/07/protecting-against-national-security-threats-to-the-communications-supply-chain-through-the-equipment-authorization-program); Katie Bo Lillis, "FBI investigation determined Chinese-made Huawei equipment could disrupt US nuclear arsenal communications," *CNN*, July 25, 2022. (https://www.cnn.com/2022/07/23/politics/fbi-investigation-huawei-china-defense-department-communications-nuclear)

[6] Christopher Balding, "ZTE's Ties to China's Military-Industrial Complex Run Deep," *Foreign Policy*, July 19, 2018. (https://foreignpolicy.com/2018/07/19/ztes-ties-to-chinas-military-industrial-complex-run-deep); Justin Rohrlich, "The ZTE Conundrum," *The Wire China*, October 11, 2020. (https://www.thewirechina.com/2020/10/11/the-zte-conundrum)

[7] Raymond Zhong, "China's ZTE, Saved by U.S., Has a Checkered Past and Shaky Future," *The New York Times*, June 8, 2018. (https://www.nytimes.com/2018/06/08/technology/zte-china-corruption.html); Paul Mozur and Cecilia Kang, "U.S. Fines ZTE of China $1.19 Billion for Breaching Sanctions," *The New York Times*, March 7, 2017. (https://www.nytimes.com/2017/03/07/technology/zte-china-fine.html)

[8] Jeremy Wagstaff and Lee Chyen Yee, "ZTE confirms security hole in U.S. phone," *Reuters*, May 18, 2012. (https://www.reuters.com/article/technology/zte-confirms-security-hole-in-us-phone-idUSBRE84H08J)

drone-jamming technologies, and other related equipment.[9] In a sign of the depth of Hikvision's ties to the country's defense industrial base, the firm itself advertised a joint study between its engineers and military commanders conducted in 2021 on how Hikvision's cameras could assist in the development and deployment of tanks, missiles, and other platforms.[10] Beijing also deployed Hikvision's technology to aid its repression of the country's Uyghur ethnic minority. The firm itself validated this finding, revealing in an internal review conducted in April 2023 that police agencies across Xinjiang had deployed Hikvision cameras to facilitate mass detention and public surveillance across the province.[11]

Recommendations

The equipment that received FCC authorization prior to its manufacturer being placed on the Covered List is often functionally equivalent to these firms' more recently banned products. Banning only newer equipment still leaves in place older components that continue to receive firmware updates from their manufacturers and communicate and transmit data to covered entities. The FCC should therefore expand the scope of its prohibitions to encompass all authorized products produced by covered entities.

- **The FCC should prohibit the continued importation and marketing of certain previously authorized equipment that has been deemed to pose a national security risk.** The equipment placed on the Covered List poses a direct threat to U.S. national security — the federal government has spent decades identifying the risks posed by Chinese national champions, targeting Chinese telecommunications manufacturers via sanctions and publicly warning of their ties to Beijing and the Chinese military. Since their inclusion on the Covered List, most of these firms have become even more integrated with the Chinese military while exporting their technologies to other authoritarian regimes. Allowing them to sell and market previously authorized equipment to the American market will perpetuate vulnerabilities in U.S. telecommunications infrastructure.

- **The FCC should prohibit the importation and sale of communications equipment added to the Covered List in 2024 or earlier.** The equipment produced by covered firms prior to 2024 is often functionally identical to more recent products that the FCC has already deemed to pose a national security risk. This is particularly the case if these products are being sold from stockpiled inventory already present within the United States. These similarities should prompt the FCC to ban their sale within the United States.

[9] Dan Strumpf, "Chinese Surveillance-Gear Maker Hikvision Has Ties to Country's Military, Report Says," *The Wall Street Journal*, May 25, 2021. (https://www.wsj.com/world/china/chinese-surveillance-gear-maker-hikvision-has-ties-to-countrys-military-report-says-11621941983)
[10] Ibid.
[11] Bethany Allen-Ebrahimian and Ina Fried, "Hikvision internal review found contracts targeted Uyghurs," *Axios*, April 17, 2023. (https://www.axios.com/2023/04/17/hikvision-internal-review-xinjiang-contracts-uyghurs)

Conclusion

The FCC must act to prevent adversaries from exploiting regulatory loopholes to maintain access to U.S. critical infrastructure. The cost of inaction — measured in both dollars and national security risk — grows every day.

Thank you for considering our comments, and we look forward to seeing how our input is incorporated into the Commission's ongoing policy work.