Congress of the United States

Washington, DC 20515

November 13, 2025

The Honorable Howard Lutnick
Secretary of Commerce
U.S. Department of Commerce
1401 Constitution Ave., NW
Washington, D.C. 20230

Dear Secretary Lutnick,

We write to respectfully request that the Department of Commerce (Commerce) investigate TP-Link Technologies Co., Ltd. and its affiliates (TP-Link) under Commerce's information and communication technology services (ICTS) authorities, pursuant to Executive Order 13873.[1] TP-Link is a People's Republic of China-based (PRC) technology company that designs and manufactures networking equipment, including internet-connected security cameras, baby monitors, and other smart connectivity devices.[2] Open-source information indicates that TP-Link represents a serious and present danger to U.S. ICTS security.[3]

For years, the PRC and Chinese Communist Party (CCP) have pursued a deliberate, two-pronged strategy to undermine U.S. cybersecurity. First, the CCP exerts direct and indirect control over Chinese technology firms, providing them with state-backed subsidies to undercut American competitors.[4] Through this influence, CCP-affiliated companies gain access to vast amounts of

[1] The U.S. government has recognized for years that information and communication technology from foreign adversaries presents a threat to U.S. national security and the privacy of its citizens. Executive Order 13873 (2019) specifically found "that foreign adversaries are increasingly creating and exploiting vulnerabilities in information and communications technology" to commit "malicious cyber-enabled actions, including economic and industrial espionage against the United States and its people." Executive Order 13873, 84 FR 22689, May 15, 2019, https://www.federalregister.gov/Commerceuments/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain.

[2] While TP-Link recently split into a PRC company and an ostensibly American one, "a Bloomberg News investigation found that the resulting American venture still has substantial operations in mainland China." According to Bloomberg, "Chinese corporate records and government announcements show that 'much of the research, development and manufacturing operations' of the new U.S. company remain in China, despite the restructuring." The American TP-Link "continues to employ 11,000 people" in China, and the "crown jewel" of its remaining operations in China is "Shenzhen Lianzhou International Technology Co. Ltd.—the massive research, development and manufacturing arm that has attracted Chinese government support and that continues to power TP-Link despite the reorganization." Kate O'Keeffe, "Wi-Fi Giant TP-Link's U.S. Future Hinges on Its Claimed Split from China." *Bloomberg*, April 11, 2025, https://www.bloomberg.com/news/articles/2025-04-11/wi-fi-giant-tp-link-s-us-future-hinges-on-its-claimed-split-from-china.

[3] Moolenaar, John, and Raja Krishnamoorthi. *Letter to Commerce: Call for Investigation into Chinese Wi-Fi Routers in U.S. Vulnerable to CCP Hacking & Data Harvesting.* House Select Committee on the Chinese Communist Party, 15 Aug. 2024, https://selectcommitteeontheccp.house.gov/media/letters/letter-commerce-call-investigation-chinese-wi-fi-routers-us-vulnerable-ccp-hacking.

[4] Could use this source or ask FAI if they have one, https://itif.org/publications/2025/09/08/more-than-99-percent-

data collected from U.S. consumers.[5] This vulnerability is compounded by China's national data laws, which compel companies to share information with the government upon request.[6]

This access extends far beyond cloud storage. Using advanced software and generative AI tools, the CCP can analyze and exploit video and data from these systems to monitor individual and group behavior, geolocate known persons, and uncover private or sensitive activities without users' consent or awareness.

In March 2024, the Federal Communications Commission (FCC) sent letters to major retailers urging caution in selling video doorbells from another PRC manufacturer (the Eken Group).[7] The FCC letter highlighted how without adequate cybersecurity protocols, these devices may "provide bad actors with an entry point into our networks, daily routines, and even our homes."[8] Further, on December 16, 2024, the Federal Bureau of Investigation (FBI) issued a Private Industry Notification warning of remote access trojan (RAT) attacks against "Chinese-branded web cameras and DVRs."[9] Similarly, in February 2025, DHS issued a bulletin warning that internet-connected cameras "especially those manufactured in the PRC" could be exploited for espionage targeting the nation's critical infrastructure installations.[10] The DHS noted that these surveillance cameras often lack data encryption and secure configuration settings, leaving them vulnerable to cyber threats.[11]

Reports indicate TP-Link is rapidly expanding its share of the U.S. market for internet-connected security cameras. TP-Link has achieved "miraculous growth" by "selling at price points below profitability" to drive out American competition[12] using its PRC government subsidies, such as those given to its Shenzhen Lianzhou International Technology Co. Ltd. operations.[13] TP-Link also sells routers and internet-connected security cameras under the brands of TP-Link, Tapo[14], and Kasa.[15] These products' market penetration in the United States is extremely concerning.

---

listed-firms-in-china-receive-direct-subsidies-chinese-government/

[5] Center for Internet Security, Inc. Cyber Threat Intelligence Team. "The Chinese Communist Party (CCP): A Quest for Data Control." *CIS*, 14 Aug. 2024, www.cisecurity.org/insights/blog/the-chinese-communist-party-ccp-a-quest-for-data-control.

[6] *Id*.

[7] For example, *see* Letter from Geoffrey Starks, Commissioner, Federal Communications Commission, to Walmart Inc., March 8, 2024, https://Commerces.fcc.gov/public/attachments/-401038A6.pdf.

[8] *Id.*

[9] Cyber Division, Federal Bureau of Investigation, "Privacy Industry Notification; HiatusRAT Actors Targeting Web Cameras and DVRs", *Internet Crime Complaint Center***,** Dec. 16, 2024, https://www.ic3.gov/CSA/2024/241216.pdf.

[10] Office of Intelligence and Analysis, Department of Homeland Security, "People's Republic of China: Exploitation of Internet-Connected Cameras Threatens US Critical Infrastructure", Feb. 3, 2025, https://wwema.org/wp-content/uploads/2025/02/Cybersecurity-DHS-IA-IF-2025-Peoples-Republic-of-China-Exploitation-of-Internet-Connected-Cameras.pdf.

[11] *Id.*

[12] *Id.*

[13] The Select Committee on the Chinese Communist Party recently asserted that an additional CCP-influenced company, Anker, that sells the internet-connected security camera brand Eufy, "operates with substantial government backing that distorts fair competition." ("Rep. John Moolenaar, 'Moolenaar Asks Commerce to Investigate CCP-Backed Anker Innovations and Protect American Consumers,' Select Committee on the CCP.

[14] "Tapo | Smart Devices for Smart Living." *Tapo*, TP-Link Systems Inc., 2025, https://www.tapo.com/us/.

[15] "About Us." *Kasa Smart*, TP-Link Systems Inc., 2025, https://www.kasasmart.com/about.

Rob Joyce, former director of cybersecurity for the National Security Agency, has summarized the PRC's approach, "The PRC [is] undercutting our market to deliver their Chinese-controlled technologies into our homes, raising significant national security concerns."[16] These concerns are especially elevated for CCP-influenced internet-connected security camera companies using cloud-based platforms to store their customers' videos. This access also extends far beyond cloud storage. Using advanced software and generative artificial intelligence (AI) tools, the CCP can analyze and exploit video and data from these systems to monitor individual and group behavior, geolocate known persons, and uncover private or sensitive activities without users' consent or awareness.[17]

Right now, nothing stops CCP-tied companies from spying on Americans through internet-connected cameras in our homes. The Chinese Communist Party can capture and exploit these videos to track, blackmail, or extort U.S. citizens—including top government and military officials.

In contrast to U.S. security interests, TP-Link products are currently sold through the Army and Air Force Exchange and the Navy Exchange,[18] placing these devices in proximity to U.S. military installations and personnel on American soil and abroad.

Additionally, "PRC state-sponsored cyber actors have extensively targeted vulnerabilities associated with PRC-made cameras since at least 2020," including an attack on a U.S. oil-and-gas company's PRC-made cameras in March 2024 and an attack in September 2024 that used internet-connected cameras as part of a botnet.[19] In early 2025, an estimated "12,000 PRC-manufactured internet-connected cameras were in use at hundreds of US-based critical infrastructure entities."[20]

On May 14, 2025, 17 members of Congress sent Commerce a letter urging it to "take swift action to prohibit further sales of TP-Link networking products in the United States."[21] Members noted TP-Link's deep ties to the CCP and its role in embedding foreign surveillance capabilities into American networks, rendering its products a clear and present danger.

---

[16] Testimony by Rob Joyce Before the House Select Committee on the Chinese Communist Party, March 5, 2025, Opening Statement. https://Commerces.house.gov/meetings/ZS/ZS00/20250305/117983/HHRG-119-ZS00-Wstate-JoyceR-20250305.pdf.

[17] Harrell, Peter. *Managing the Risks of China's Access to U.S. Data and Control of Software and Connected Technology*. Carnegie Endowment for International Peace, 30 Jan. 2025, https://carnegieendowment.org/research/2025/01/managing-the-risks-of-chinas-access-to-us-data-and-control-of-software-and-connected-technology?lang=en.

[18] Mira Ricardel, "Tariffs or Not, China's Infiltration of U.S. Systems Needs New Attention," *Defense News*, May 22, 2025, https://www.defensenews.com/opinion/2025/05/22/tariffs-or-not-chinas-infiltration-of-us-systems-needs-new-attention/.

[19] *Id.*

[20] *Id.*

[21] Letter from Senator Tom Cotton to Secretary Howard Lutnick, Department of Commerce, May 14, 2025, https://www.cotton.senate.gov/imo/media/Commerce/tplinkfinal.pdf.

Accordingly, we respectfully request that Commerce evaluate the national security risks posed by internet-connected security cameras sold by TP-Link and determine whether the use of ICTS authorities is warranted to mitigate these risks. Specifically, we ask that Commerce respond no later than November 30, 2025, providing:

1. An assessment of the national security risks associated with TP-Link's internet-connected security cameras; and

2. An evaluation of whether ICTS authorities are sufficient and appropriate to address these risks.

If Commerce determines TP-Link products present a national security threat, we urge the Department to exercise its ICTS authorities to mitigate the danger promptly.

In addition, we request that Commerce consider other immediate steps to address this issue, including:

1. Recommending that the FCC add TP-Link and other Chinese Communist Party (CCP)-influenced companies to its Covered List;

2. Conducting and reporting to Congress a study on the national security risks posed by internet-connected security cameras designed, developed, manufactured, or supplied by TP-Link and other CCP-influenced entities; and

3. Recommending that the FBI and the Department of Homeland Security (DHS) issue additional public service bulletins to inform retailers, distributors, and consumers of the risks associated with these devices.

Thank you for your attention to this important matter. If you have any questions, please do not hesitate to reach out to any of our offices if we can be of assistance.

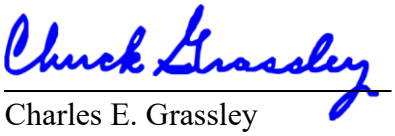
Sincerely,

Joni K. Ernst
United States Senator

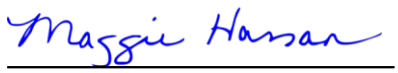
Ashley Hinson
Member of Congress

Raja Krishnamoorthi
Member of Congress

John Barrasso, M.D.
United States Senator



Charles E. Grassley
United States Senator



Margaret Wood Hassan
United States Senator

Rick Scott
United States Senator

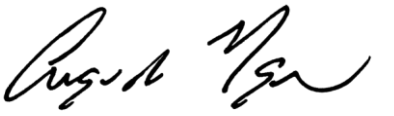
Pete Ricketts
United States Senator

Donald G. Davis
Member of Congress

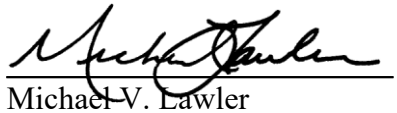
Randy Feenstra
Member of Congress

Michael T. McCaul
Member of Congress

Elise M. Stefanik
Member of Congress

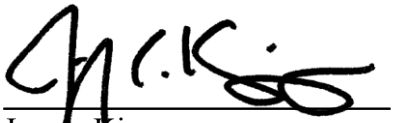


August Pfluger
Member of Congress

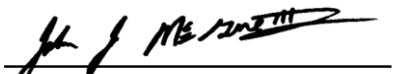


Michael V. Lawler
Member of Congress

Juan Ciscomani
Member of Congress



Jen A. Riggans
Member of Congress



John J. McGuire III
Member of Congress

Mike Carey
Member of Congress

Pat Harrigan
Member of Congress

Ronny L. Jackson
Member of Congress

Keith Self
Member of Congress

Rich McCormick, MD, MBA
Member of Congress

Ben Cline
Member of Congress