Congress of the United States
House of Representatives
SELECT COMMITTEE ON THE CHINESE COMMUNIST PARTY

August 13, 2024

The Honorable Gina Raimondo
Secretary
Department of Commerce
1401 Constitution Avenue NW
Washington, D.C. 20230

Dear Secretary Raimondo:

We write to respectfully request that you investigate TP-Link Technologies Co., Ltd. (TP-Link) and its affiliates under the Department of Commerce's (Commerce) information and communication technology services (ICTS) authorities, pursuant to Executive Order 13873.[1] TP-Link is a technology company based in the People's Republic of China (PRC) that manufactures Wi-Fi routers, Wi-Fi devices, and mesh Wi-Fi network devices, along with hardware and software components and other products. TP-Link's products account for a substantial part of the U.S. market for Wi-Fi routers and related devices. Open-source information indicates that the company may represent a serious threat to U.S. ICTS security. We therefore request that Commerce investigate TP-Link under its ICTS authorities to determine whether the company poses a national security risk. If it finds that is the case, we request that Commerce use its ICTS authorities to properly mitigate the risk.

Ninety-five percent of U.S. adults reported that they used the internet in 2023, with small office/home office (SOHO) routers serving as a principal means for U.S. residents to access the internet.[2] According to industry reports and press releases, as of 2022, TP-Link is the world's largest provider of Wi-Fi products, selling over 160 million products annually to more than 170 countries, and is a leading SOHO router provider in the United States.[3] TP-Link products are also found on U.S. military bases, with the

[1] Exec. Order No. 13873, Securing the Information and Communications Technology and Services Supply Chain (May 15, 2019), https://www.govinfo.gov/content/pkg/FR-2019-05-17/pdf/2019-10538.pdf.
[2] *Internet, Broadband Fact Sheet*, PEW RESEARCH CENTER (Jan. 31, 2024), https://www.pewresearch.org/internet/fact-sheet/internet-broadband/.
[3] *TP-Link: The World's No. 1 WiFi Product Provider for 12 Years Running*, TP-LINK, https://tp-link.com/us/press/news/20553/ (last visited July 31, 2024); *TP-LinkSales Revenue Tops $2.1 billion in 2016*, TP-LINK (Oct. 30, 2017), https://www.tp-link.com/fi/press/news/17669/ (last visited July 31, 2024).

Army & Air Force Exchange and the Navy Exchange selling these devices to members of the military and their families.[4]

An increasing number of outside researchers and analysts have identified specific concerns about the risks posed by TP-Link. A former Commissioner of the Federal Communications Commission (FCC) recently noted that while "U.S. cybersecurity authorities and analysts have documented vulnerabilities from home equipment vendors across the board [] TP-Link products have had more than their fair share of citations."[5] In addition, pursuant to the PRC's increasingly draconian data protectionist and national security-focused legal regime, companies like TP-Link are required to provide data to the PRC government and otherwise comply with the demands of its national security apparatus.

TP-Link's unusual degree of vulnerabilities and required compliance with PRC law are in and of themselves disconcerting. When combined with the PRC government's common use of SOHO routers like TP-Link to perpetrate extensive cyberattacks in the United States, it becomes significantly alarming. As Federal Bureau of Investigation (FBI) Director Christopher Wray stated, PRC-sponsored hacking has "reached something closer to a fever pitch" with the PRC "…poised to attack whenever Beijing decides the time is right."[6] In a hearing before the Select Committee, Director Wray called Volt Typhoon and other PRC Advanced Persistent Threat (APT) groups "the defining threat of our generation,"[7] with the Cybersecurity Infrastructure and Security Agency (CISA) and

---

[4] As of August 2024, the Army & Air Force Exchange Service currently lists 31 TP-Link devices through its online store, while the Navy Exchange lists 17 TP-Link devices on its site. *See Results for: TP-Link*, ARMY & AIR FORCE EXCHANGE SERVICE, https://www.shopmyexchange.com/browse?query=tp-link (last visited August 13, 2024); *Results for: TP-Link*, NAVY EXCHANGE, https://www.mynavyexchange.com/browse/_/N-1393213266?Dy=1&Nr=AND%28sku.inStockFilter%3A1%2Csku.imagesAvailable%3A1%29&collection=%2Fcontent%2FShared%2FAuto-Suggest+Panels (last visited August 13, 2024). Additionally, in 2021, the Department of Defense awarded a government contractor a $174,195 contract for which the only description is "TP-Link." *See* Delivery Order (DO) PIID HC108421F0065, USASPENDING.GOV, (Jan. 15, 2021), https://www.usaspending.gov/award/CONT_AWD_HC108421F0065_9700_GS02F0008V_4730. We likewise found references to TP-Link in multiple other contracting vehicles over recent years. *See, e.g.*, Delivery Order (DO) PIID HC108421FA100, USASPENDING.GOV, (Apr. 26, 2021), https://www.usaspending.gov/award/CONT_AWD_HC108421FA100_9700_NNG15SC71B_8000; Delivery Order (DO) PIID HC108421FA564, USASPENDING.GOV, (Sept. 13, 2021), https://www.usaspending.gov/award/CONT_AWD_HC108421FA564_9700_NNG15SC71B_8000.

[5] Michael O'Rielly, *Chinese Wireless Routers: The Next Entry Point for State-Sponsored Hackers?*, HUDSON INSTITUTE (Mar. 6, 2024), https://www.hudson.org/information-technology/chinese-wireless-routers-next-entry-point-state-sponsored-hackers-michael-orielly.

[6] Christopher Wray, Director, Federal Bureau of Investigation, Remarks at the Munich Security Conference (Feb. 15, 2024), https://www.fbi.gov/news/speeches/director-wray-s-remarks-at-the-munich-security-conference.

[7] *See* Carly Page, *US Disrupts China-Backed Hacking Operation Amid Warning of Threat to American Infrastructure*, TECHCRUNCH (Jan. 31, 2024), https://techcrunch.com/2024/01/31/fbi-cisa-volt-typhoon-cyberattack-american-infastructure/; Helen Davidson, *Explainer: What is Volt Typhoon and Why Is It the 'Defining Threat of Our Generation'?*, THE GUARDIAN (Feb. 13, 2024), https://www.theguardian.com/technology/2024/feb/13/volt-typhoon-what-is-it-how-does-it-work-chinese-cyber-operation-china-hackers-explainer; *see also The CCP Cyber Threat to the American Homeland and National Security: Hearing Before the Select Committee on the Chinese Communist Party* (Jan. 31, 2024),

FBI recently urging manufacturers to implement security designs to guard against breaches in light of the threats posed by groups like Volt Typhoon.[8]

Volt Typhoon and other PRC APT groups are able to threaten U.S. critical infrastructure in large part because of their ability to compromise SOHO routers like those manufactured by TP-Link. Expert analysis last year has shown that these PRC APT groups consistently exploit known vulnerabilities in TP-Link routers in malicious campaigns, including those that had the PRC "target[] government officials in European countries."[9] In that cyber campaign, the malicious "modified firmware images have been found only on TP-Link routers thus far."[10] Just months ago, the Department of Justice (DOJ) conducted a court-authorized operation to remove Volt Typhoon malware from hundreds of routers nationwide.[11] As Director Wray put it, Volt Typhoon's "pre-positioning constitutes a potential real-world threat to our physical safety that the FBI is not going to tolerate."[12]

Given the PRC's data and national security laws, the proliferation of PRC-made SOHO routers in the United States, and the demonstrated willingness of the PRC government to sponsor hacking campaigns using PRC-affiliated SOHO routers like those made by TP-Link, we request that Commerce verify the threat posed by PRC-affiliated SOHO routers—particularly those offered by the world's largest manufacturer, TP-Link—and consider using its ICTS authorities to properly mitigate this glaring national security issue. Specifically, we request that you respond no later than August 30, 2024, describing (1) your assessment of the national security risks posed by TP-Link SOHO routers, and (2) your assessment of whether ICTS authorities are appropriate to allay any risks.

---

https://selectcommitteeontheccp.house.gov/committee-activity/hearings/hearing-notice-ccp-cyber-threat-american-homeland-and-national-security.

[8] *CISA and FBI Release Secure by Design Alert Urging Manufacturers to Eliminate Defects in SOHO Routers*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (Jan. 31, 2024), https://www.cisa.gov/news-events/alerts/2024/01/31/cisa-and-fbi-release-secure-design-alert-urging-manufacturers-eliminate-defects-soho-routers.

[9] Dennis Fisher, Camaro Dragon Group Targets Routers with Malicious Firmware, DECIPHER, https://duo.com/decipher/camaro-dragon-group-targets-routers-with-malicious-firmware (May 16, 2023); *see also* CYFIRMA, Comprehensive Analysis of CVE-2024-21833 Vulnerability in TP-Link Routers: Threat Landscape, Exploitation Risks, and Mitigation Strategies, https://www.cyfirma.com/research/comprehensive-analysis-of-cve-2024-21833-vulnerability-in-tp-link-routers-threat-landscape-exploitation-risks-and-mitigation-strategies/ (Jan. 31, 2024).

[10] Dennis Fisher, Camaro Dragon Group Targets Routers with Malicious Firmware, DECIPHER, https://duo.com/decipher/camaro-dragon-group-targets-routers-with-malicious-firmware (May 16, 2023) ("Interestingly, it's unclear how the Camaro Dragon attackers are gaining access to the target devices.").

[11] Press Release, Department of Justice, U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure (Jan. 31, 2024), https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical.

[12] *Id.*

We thank you for your prompt response and attention to this important matter. Thank you for your work on behalf of the American people.

Sincerely,

John Moolenaar
Chairman

Raja Krishnamoorthi
Ranking Member

cc: The Honorable Alejandro Mayorkas, Secretary, U.S. Department of Homeland Security
The Honorable Avril Haines, Director of National Intelligence
The Honorable Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency
Robert J. Bianchi, Chief Executive Officer, Navy Exchange Service Command
Tom Schull, Director & Chief Executive Officer, Army & Air Force Exchange Service