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

May 16, 2025

The Honorable Marco Rubio
Secretary
U.S. Department of State
2201 C Street NW
Washington, DC 20520

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

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

Dear Secretary Rubio, Secretary Lutnick, and Chairman Carr:

We write to highlight the threat of HarmonyOS and the imperative of multilateral collaboration and diplomacy to prevent HarmonyOS's proliferation. HarmonyOS is an operating system developed by Huawei as an alternative to the current leading mobile operating systems developed by Google (Android) and Apple (iOS), as well as desktop operating systems such as those developed by Microsoft (Windows).[1] HarmonyOS is also intended for use in products other than smartphones, tablets, and computers, including connected vehicles and smart devices.[2] Given the serious national security and geopolitical implications associated with foreign adversary operating systems, it is critical that HarmonyOS be thoroughly scrutinized and that we work with our allies and partners to prevent it from becoming embedded in devices across the world.

Devices operating with HarmonyOS could provide a direct channel for data collection, potential cyber exploitation, and digital authoritarianism by the People's Republic of China (PRC). Under PRC law, Huawei must "support, assist, and cooperate with national intelligence efforts."[3]

---

[1] Zhang Erchi, Qin Min, and Denise Jia, Huawei's HarmonyOS Next is set to rival iOS and Android in China, CAIXIN (Apr. 6, 2024), https://asia.nikkei.com/Spotlight/Caixin/Huawei-s-HarmonyOS-Next-is-set-to-rival-iOS-and-Android-in-China.

[2] Zhang Yushuo, BMW, Huawei Ally on HarmonyOS-Based In-Car System for German Carmaker's China-Made Cars, YICAI (Mar. 18, 2025), https://www.yicaiglobal.com/news/bmw-huawei-to-co-develop-smart-in-vehicle-ecosystem-for-german-automakers-china-made-cars.

[3] National Intelligence Law of the People's Republic of China (promulgated by the STANDING COMM. NAT'L PEOPLE'S CONG., June 27, 2017, effective June 28, 2017, as amended Apr. 27, 2018) (P.R.C.), https://flk.npc.gov.cn/detail2.html?MmM5MDlmZGQ2NzhiZjE3OTAxNjc4YmY4NDk4ZDA5ZjE%3D.

This means there are reasonable concerns that, even though HarmonyOS is open source, the operating system, or future updates or patches to the system, could contain backdoors and vulnerabilities designed to facilitate espionage.[4] Moreover, Huawei's control of AppGallery —the equivalent of the iPhone Appstore—could provide the Chinese Communist Party with a veto power over a user's download decisions and the ability to access sensitive code of various apps in order to perform "security vetting." These are far from the only concerns with HarmonyOS, but are illustrative of how HarmonyOS's proliferation would both threaten our security and serve as a potential tool for the CCP to expand its digital authoritarianism.

In addition, unlike operating systems subject to U.S. regulatory jurisdiction, HarmonyOS is controlled by a sanctioned and red-flagged entity. Huawei is on the Commerce Department's Entity List, the FCC's Covered List, and the U.S. Department of Defense's list of Chinese Military Companies.[5] Simply put, in the universe of bad actors, Huawei is as bad as it gets.

The U.S. Government should fully examine HarmonyOS's architecture and codebase. We should also ensure our allies and partners around the world are aware of Huawei's, and thus the Chinese Communist Party's, control over HarmonyOS, including its updates and patches. Rather than being forced to attempt to remove HarmonyOS from sensitive devices around the world after these risks become widely appreciated, we should use diplomacy and intelligence sharing to encourage the global community to continue to utilize trusted operating systems.

Thank you for your attention to this critical matter of national security.

Sincerely,

John Moolenaar
Chairman

Raja Krishnamoorthi
Ranking Member

[4] Eduard Kovacs, Nearly 300 Vulnerabilities Patched in Huawei's HarmonyOS in 2022, SECURITY WEEK (Jan. 3, 2023), https://www.securityweek.com/nearly-300-vulnerabilities-patched-huaweis-harmonyos-2022/; Samm Sacks, Tech Take: Trusted Tech and the Challenge of Mobile Operating Systems: Harmony OS, KRACH INST. FOR TECH. DIPLOMACY (Apr. 22, 2025), https://techdiplomacy.org/news/tech-take-trusted-tech-and-the-challenge-of-mobile-operating-systems-harmony-os/.

[5] *Public Safety and Homeland Security Bureau, Federal Communications Commission, List of Equipment and Services Covered by Section 2 of the Secure Networks Act* (Mar. 12, 2021), https://docs.fcc.gov/public/attachments/DOC-370755A1.pdf; *U.S. Department of Defense, Entities Identified as Chinese Military Companies Operating in the United States* (June 3, 2021), https://media.defense.gov/2021/Jun/03/2002734519/-1/-1/0/ENTITIES-IDENTIFIED-AS-CHINESE-MILITARY-COMPANIES-OPERATING-IN-THE-US.PDF; *Bureau of Industry and Security, U.S. Department of Commerce, Huawei and Affiliates Entity List Rule – Effective Date* (May 21, 2019), https://www.bis.doc.gov/index.php/documents/regulations-docs/2395-effective-date-of-huawei-and-affiliates-entity-list-rule/file.