

JOHN MOOLENAAR, MICHIGAN  
CHAIRMAN  
ROB WITTMAN, VIRGINIA  
ANDY BARR, KENTUCKY  
DAN NEWHOUSE, WASHINGTON  
DARIN LAHOOD, ILLINOIS  
NEAL DUNN, FLORIDA  
DUSTY JOHNSON, SOUTH DAKOTA  
ASHLEY HINSON, IOWA  
CARLOS GIMENEZ, FLORIDA  
GUS BILIRAKIS, FLORIDA  
YOUNG KIM, CALIFORNIA  
NATHANIEL MORAN, TEXAS  
ZACH NUNN, IOWA



**Congress of the United States**  
**House of Representatives**

**SELECT COMMITTEE ON THE CHINESE COMMUNIST PARTY**

RAJA KRISHNAMOORTHY, ILLINOIS  
RANKING MEMBER  
KATHY CASTOR, FLORIDA  
ANDRÉ CARSON, INDIANA  
SETH MOULTON, MASSACHUSETTS  
RO KHANNA, CALIFORNIA  
MIKIE SHERRILL, NEW JERSEY  
HALEY STEVENS, MICHIGAN  
RITCHIE TORRES, NEW YORK  
SHONTEL BROWN, OHIO  
GREG STANTON, ARIZONA  
JILL TOKUDA, HAWAII

June 4, 2025

Mike Milinkovich  
Executive Director  
Eclipse Foundation  
Rond Point Schuman 11  
Brussels, Belgium

Dear Mr. Milinkovich:

We write to express our concern regarding HarmonyOS, OpenHarmony, and the Eclipse Foundation's collaboration with the OpenAtom Foundation in their development and global promotion, particularly in the United States and allied nations. As we noted in a recent letter to federal agencies on the threat of HarmonyOS, it is an operating system developed by Huawei as a Chinese Communist Party (CCP)-controlled 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).<sup>1</sup> HarmonyOS is also intended for use in products other than smartphones, tablets, and computers, including connected vehicles and smart devices.<sup>2</sup> While the HarmonyOS operating system is proprietary and principally used in Huawei devices, OpenHarmony is intended for use on third party devices and as base operating system framework for developers, enterprises, and hardware vendors. According to your website, as depicted below, a goal of your collaboration with Huawei is to “extend[] OpenHarmony code base with add-ons for the European and Global markets.”<sup>3</sup> Huawei, the original developer of HarmonyOS, has been identified by the U.S. Government as a profound national security threat

---

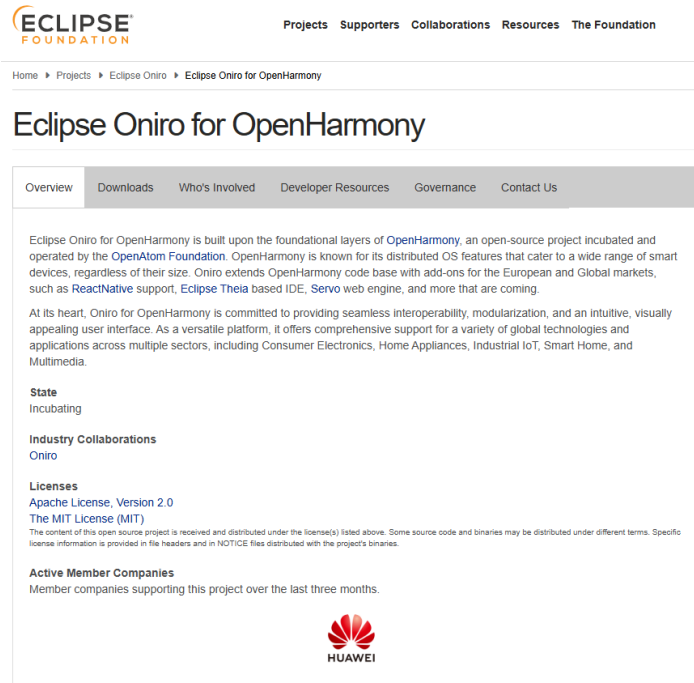
<sup>1</sup> *Huawei's HarmonyOS Next Is Set to Rival iOS and Android in China* - Nikkei Asia, <https://asia.nikkei.com/Spotlight/Caixin/Huawei-s-HarmonyOS-Next-is-set-to-rival-iOS-and-Android-in-China> (last visited May 22, 2025).

<sup>2</sup> *BMW, Huawei Ally on HarmonyOS-Based In-Car System for German Carmaker's China-Made Cars*, <https://www.yicai.com/news/bmw-huawei-to-co-develop-smart-in-vehicle-ecosystem-for-german-automakers-china-made-cars> (last visited May 22, 2025).

<sup>3</sup> Maria Teresa Delgado, *Eclipse Oniro for OpenHarmony* | *Projects.Eclipse.Org*, (Feb. 2, 2023), <https://projects.eclipse.org/projects/oniro.oniro4openharmony>.

due to its ties to the CCP.<sup>4</sup> Huawei is on the Commerce Department's Entity List,<sup>5</sup> the FCC's Covered List,<sup>6</sup> and the U.S. Department of Defense's list of Chinese Military Companies.<sup>7</sup>

The OpenHarmony project, while presented as open-source, receives much of its foundational code from Huawei. Huawei initially donated the L0-L2 branch source code of HarmonyOS to the OpenAtom Foundation.<sup>8</sup> This substantial, if not overwhelming, reliance on Huawei's original code is deeply problematic. Despite the transfer of the project to the OpenAtom Foundation, the deep roots in Huawei's development inevitably carry the risks associated with Huawei as an entity. This includes the potential for inherent design choices, architectural elements, or even subtle coding practices that could be influenced by Huawei's obligations to the CCP, as detailed below. Even if the project is open-source, the sheer volume of Huawei's initial contribution makes independent verification that CCP backdoors are not embedded in the protocol a monumental, if not impossible, task.



Given this context, there are reasonable concerns that HarmonyOS, even in its open-source form, or future updates and patches to the system, could contain backdoors or vulnerabilities designed to facilitate espionage or data exfiltration. The sheer volume of reported vulnerabilities in HarmonyOS further underscores the potential for exploitation.<sup>9</sup> The integration

<sup>4</sup> *Is China's Huawei a Threat to U.S. National Security?* | Council on Foreign Relations, <https://www.cfr.org/background/chinas-huawei-threat-us-national-security>.

<sup>5</sup> *Addition of Huawei Non-U.S. Affiliates to the Entity List, the Removal of Temporary General License, and Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule)*, FEDERAL REGISTER (Aug. 20, 2020), <https://www.federalregister.gov/documents/2020/08/20/2020-18213/addition-of-huawei-non-us-affiliates-to-the-entity-list-the-removal-of-temporary-general-license-and>.

<sup>6</sup> Federal Comm'n's Comm'n, Public Safety and Homeland Security Bureau, DA 20-690, Order (June 30, 2020), <https://docs.fcc.gov/public/attachments/da-20-690a1.pdf>.

<sup>7</sup> ENTITIES IDENTIFIED AS CHINESE MILITARY COMPANIES OPERATING IN THE UNITED STATES IN ACCORDANCE WITH SECTION 1260H OF THE WILLIAM M. (MAC) THORNBERRY NDAA FOR FY21 (2025), <https://media.defense.gov/2025/Jan/07/2003625471/-1/-1/1/ENTITIES-IDENTIFIED-AS-CHINESE-MILITARY-COMPANIES-OPERATING-IN-THE-UNITED-STATES.PDF>.

<sup>8</sup> *Huawei Makes HarmonyOS Open Source to Boost It as Android Alternative* - Caixin Global, <https://www.caixinglobal.com/2021-06-07/huawei-makes-harmonyos-open-source-to-boost-it-as-android-alternative-101724168.html> (last visited May 22, 2025).

<sup>9</sup> *Huawei HarmonyOS Security Vulnerabilities, CVEs, Versions and CVE Reports*, [https://www.cvedetails.com/product/80962/Huawei-HarmonyOS.html?vendor\\_id=5979](https://www.cvedetails.com/product/80962/Huawei-HarmonyOS.html?vendor_id=5979) (last visited May 22, 2025).

of HarmonyOS or OpenHarmony into various devices, from smartphones and tablets to vehicles and smart infrastructure, could provide the CCP with a direct channel for data collection and cyber exploitation.

China's national security laws, including the National Intelligence Law, compel Huawei to "support, assist, and cooperate with national intelligence efforts." This means that any entity, including Huawei and, by extension, developers contributing to Huawei-affiliated projects, could be legally compelled to provide data or access to their systems to Chinese intelligence agencies.<sup>10</sup> This creates an undeniable risk that devices running such operating systems could be leveraged for surveillance and digital authoritarianism by the CCP, regardless of the best intentions of the open-source community. The People's Republic of China (PRC) Government's ability to demand access to source code, encryption keys, and user data under these laws presents an unacceptable risk to the security and privacy of users globally.<sup>11</sup>

To address these serious concerns, we respectfully request the following information from the Eclipse Foundation by no later than June 18, 2025:

1. Given that Huawei contributed most of the foundational code (L0-L2) to the OpenHarmony project, what independent technical and governance mechanisms are in place within the OpenAtom Foundation and the OpenHarmony project to ensure that Huawei's influence on the codebase's long-term development, security updates, and architectural direction is appropriately mitigated and transparent to the broader open-source community?
2. Has the Eclipse Foundation, or the OpenAtom Foundation, commissioned an independent, comprehensive third-party security audit of the full OpenHarmony codebase since Huawei's initial contribution, specifically targeting potential backdoors, hidden functionalities, or vulnerabilities that could be exploited by state actors? If so, please provide a summary of the findings and any corrective actions taken. If not, why not?
3. What explicit policies or procedures does the Eclipse Foundation have in place to prevent components, features, or updates within projects under its purview (such as OpenHarmony) from being designed or compelled to comply with the National Intelligence Law or other PRC national security laws that could mandate data access or surveillance capabilities for the CCP?
4. How does the Eclipse Foundation, in its role as a global open-source steward, communicate the national security and human rights risks associated with integrating software heavily derived from entities designated by the U.S. Government as security threats to its partners, developers, and users in the United States and other democratic nations?
5. Beyond the initial code donation, what ongoing due diligence does the Eclipse Foundation perform to assess the current level of Huawei's or other CCP-linked entities'

---

<sup>10</sup> *U.S. Businesses Must Navigate Significant Risk of Chinese Government Access to Their Data*, <https://www.wiley.law/newsletter-Mar-2021-PIF-US-Businesses-Must-Navigate-Significant-Risk-of-Chinese-Government-Access-to-Their-Data> (last visited May 22, 2025).

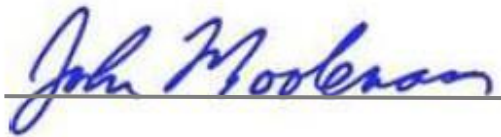
<sup>11</sup> *The Impact of China's National and Cyber Security Laws on Global Encryption - DataLocker Inc.*, (Oct. 3, 2024), <https://datalocker.com/blog/the-impact-of-chinas-national-and-cyber-security-laws-on-global-encryption/>.

influence over the OpenHarmony project's technical direction, intellectual property, and community governance within the OpenAtom Foundation?

6. Please describe the genesis of Eclipse Ontiro for OpenHarmony and all other collaborations between your foundation and Huawei or entities affiliated with Huawei.

We are actively working to encourage the global community to utilize trusted operating systems, which certainly does not include any operating system affiliated with Huawei. Organizations like the Eclipse Foundation have a critical role to play in upholding the integrity and security of the global digital ecosystem. We look forward to your prompt attention to this matter and a detailed explanation of the steps the Eclipse Foundation intends to take to mitigate these serious concerns.

Sincerely,

A handwritten signature in blue ink, reading "John Moolenaar", written over a horizontal line.

John Moolenaar  
Chairman

A handwritten signature in blue ink, reading "Raja Krishnamoorthi", written over a horizontal line.

Raja Krishnamoorthi  
Ranking Member