



SELECT COMMITTEE ON THE CCP

DEMOCRATS | RANKING MEMBER RO KHANNA

July 9, 2026

Ethan Klein
Chief Technology Officer
Executive Office of the President
1600 Pennsylvania Ave NW
Washington, DC 20500

Gregory Barbaccia
Federal Chief Information Officer
Office of Management and Budget
725 17th Street, NW
Washington, DC 20503

Dear Dr. Klein and Mr. Barbaccia:

I write with grave concern regarding the reported inclusion of an embedded software development kit (SDK) from restricted Chinese telecommunications firm Huawei in the recently released official White House Mobile App. Earlier this year, President Trump released “[t]he official White House mobile app” with the goal of “keep[ing Americans] connected to President Donald J. Trump and his administration like never before.”¹ However, due to the potential presence of a Huawei SDK, unsuspecting Americans may potentially be downloading an app that in fact exposes their personal data to collection by Chinese intelligence services like never before.

On a bipartisan basis, Congress and the Executive Branch have made clear that Huawei represents one of the most significant risks of enabling China’s intelligence collection against American citizens. Huawei was placed on the Department of Commerce Bureau of Industry and Security Entity List in 2019 and the Federal Communications Commission’s Covered List in 2021. President Trump himself has recognized these risks, noting that for “any country that uses [Huawei], we’re not going to do anything in terms of sharing intelligence.”² It is therefore a dangerous lapse in U.S. national security policy to potentially have or have had Huawei code embedded in the official White House app.

This is not a minor technical oversight. As a recent article asserted, “[t]he Huawei analytics kit collects device information, app usage data, and behavioral metrics. It maintains a persistent connection to Huawei servers. Every time someone opens the White House app, data flows back to infrastructure controlled by a company the U.S. government itself designates as a threat to

¹ Executive Office of the President. (2026). *The White House* (Version 47.0.12) [Mobile App]. Google Play Store. <https://play.google.com/store/apps/details?id=gov.whitehouse.app&ref=sambent.com>

² O’Brien, M. (2020, August 17). *Trump administration imposes new Huawei restrictions*. AP News. <https://apnews.com/article/smartphones-business-china-asia-pacific-us-news-7a01cf8cf13f7681df62094f27b1bcbe>

national security.”³ These concerns are intensified by the fact that over 700,000 Americans downloaded the app in just its first week of availability⁴ and the fact the app is apparently being pre-installed on federal devices across the Executive Branch.⁵

Alarming, the app also has been reported to embed six widgets from Elfsight, a Russia-founded company, each of which reportedly executes live JavaScript from Elfsight’s external servers in real time. This architecture raises concerns that a Russia-linked entity could potentially inject arbitrary malicious code into the White House application at any moment, with no review or approval from any U.S. government authority.⁶ This additional supply chain vulnerability appears to be yet another breach of trust from the Office of the President of the United States in terms of creating opportunities for foreign governments to potentially access to Americans’ personal data.

Finally, the app requires numerous permissions that seriously violate Americans’ privacy. The app relies on outside software that apparently sends U.S. personal data to third parties. This is reported to include a commercial vendor’s embedded “unique digital fingerprint that can track users across sessions.”⁷ As one former FBI official put it, “the U.S. government’s infrastructure is being attacked from all sides right now, and having an amateur WordPress developer running the White House’s public presence puts everybody who visits it at risk.”⁸

The official White House app is profoundly objectionable for many reasons, including its inclusion of an ICE reporting function and its promotion of political content via the President’s personal social media feed. But no American seeking to access a government service should be forced to subject their device to potential surveillance or manipulation by the Chinese or Russian intelligence services. The United States, under administrations of both parties, has assembled an international coalition to encourage countries to exclude Huawei technologies from their networks due to their serious security concerns. And yet, the same Administration now operates a consumer-facing mobile application bearing the presidential seal that may potentially actively interact with Huawei’s servers. This is unacceptable.

Accordingly, please answer the following questions by no later August 1, 2026.

1. The White House has stated “the app does not collect any user locations and has no Huawei software integrations.” How do you reconcile this statement with conflicting independent cybersecurity analysis?
2. Will you commit to remove any Huawei SDK and Elfsight widgets, and address all other cybersecurity and privacy issues associated with the official White House app? If the vulnerabilities have already been addressed, please provide specifics.
3. What, if any, due diligence or vulnerability assessments were performed prior to the app’s release to ensure its security?

³ Bent, S. (2026, March 28). *Fedware: 13 Government Apps That Spy Harder Than the Apps They Ban*. State of Surveillance. <https://www.sambent.com/the-white-house-app-has-huawei-spyware-and-an-ice-tip-line/>

⁴ Id.

⁵ Elliott, V. (2026, June 23). *Federal Workers Can’t Get the White House’s App Off Their Phones*. WIRED. <https://www.wired.com/story/story/government-workers-cant-get-the-white-houses-app-off-their-phones/>

⁶ Id.

⁷ Kennard, E., & Larreal, S. (2026b, April 3). *The White House App Is Riddled With Cybersecurity Vulnerabilities*. NOTUS. <https://www.notus.org/technology/trump-white-house-app-cybersecurity>

⁸ Id.

4. Why was the contract to develop this app awarded to 45Press, a small firm described by a former FBI official as “amateur”?⁹
5. Has the U.S. Government conducted any analysis to determine whether user data or information has been shared to any non-USG entity by virtue of a user’s download of or engagement with this app? If so, what data or information has been shared and with whom has it been shared?

Even more important than your timely response to these questions, however, is your immediate action to suspend this app from distribution until, at a minimum, the American people are assured that its cybersecurity and data privacy concerns are fully addressed. The White House should not be violating Americans’ data privacy, and it certainly should not expose them to potential intelligence collection by foreign governments.

Thank you for your attention to this matter.

Sincerely,



Ro Khanna
Ranking Member

⁹ Id.