U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency
Office of the Director
Washington, DC 20528

May 22, 2019

The Honorable Ron Wyden
United States Senate
Washington, DC 20510

Dear Senator Wyden:

Thank you for your February 7, 2019 letter.

The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) recognizes that mobile device users employ virtual private network (VPN) applications for multiple purposes, including encrypting communications and obscuring location information while using public Wi-Fi networks. While there are advantages to the use of VPN applications, they are not without risk. Regarding this risk, the National Institute of Standards and Technology (NIST) has published *Guidelines for Managing the Security of Mobile Devices in the Enterprise*.[i] The guidelines recognize, "Mobile devices are manufactured to easily find, acquire, install, and use third-party applications from mobile device application stores. This poses obvious security risks, especially for mobile device platforms and application stores that do not place security restrictions or other limitations on third-party application publishing."

As such, VPN applications, mobile device proxies, and other similar applications have the potential to be vulnerable to surveillance and other threats. According to open-source reporting, in November 2017, the Russian Government signed into law amendments that force domestic and foreign VPN providers to participate in Russia's blacklist enforcement system. This system allows the Russian Government to access and influence Russia-based VPN providers, such as Yandex.[ii] In December 2017, the Indian Government issued an advisory to employees that the Chinese Government leveraged popular mobile applications, including WeChat, Truecaller, Weibo, UC Browser, and UC News, to collect information on sensitive Indian security installations.[iii]

CISA has not observed indications that foreign-made VPN applications are widely used by U.S. Government employees on federally contracted mobile devices, however, CISA has limited visibility. Through our engagements with federal agencies and other stakeholders, CISA shares current threat information and guidance to mitigate risks, including the types identified in your letter. As one example, on February 22, 2018, CISA shared guidance issued by the Federal Trade Commission: https://www.us-cert.gov/ncas/current-activity/2018/02/22/FTC-Releases-Article-Choosing-VPN-Apps-Mobile-Phones.

Regarding the national security risk these applications may pose, CISA assesses a low to moderate impact to U.S. Government operations.[iv] Open-source reporting indicates nation-state actors have demonstrated intent and capability to leverage VPN services and vulnerable users for malicious purposes. The vulnerabilities are the ability of users to download untrusted VPN services and the lack of policy across organizations restricting their download. No overarching U.S. Government policy or

whitelist restricts users from downloading a foreign VPN application on government-operated mobile devices. Policy restrictions vary across departments and agencies. However, the number and identity of government-operated mobile devices that have downloaded foreign VPN applications is unknown. There may be no such devices.

Effective or partially effective security controls are available via policy changes and technical solutions. For example, CISA protects its enterprise data on its mobile devices by segregating via a software container, which also provides a sandbox and secure VPN tunnel. Whitelisting of approved applications is also an effective control.[v] However, the breadth of deployment of these technical solutions across government is unknown.

Even with the implementation of technical solutions, if a U.S. Government employee downloaded a foreign VPN application originating from an adversary nation, foreign exploitation of that data would be somewhat or highly likely. This exploitation could lead to loss of data integrity and confidentiality of communications transmitted over the application. Exposure of data would likely include contacts, user history, geolocation, photographs, and any other accesses granted by the user to the application.

CISA will continue to assess the situation and coordinate with interagency partners on the best methods to reduce risk. These efforts include establishing a common baseline of protection, guidance on risk mitigation, technical assistance, or training. If needed, CISA can issue compulsory directives that limit exposure to malicious mobile applications.

Thank you again for your letter. The co-signer of your letter will receive a separate, identical response. Should you wish to discuss this further, please do not hesitate to contact me.

Sincerely,

Christopher C. Krebs
Director

---

[i] NIST. (2013). Special Publication 800-124 Revision 1, Guidelines for Managing the Security of Mobile Devices in in the Enterprise. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf

[ii] The Moscow Times. (2017). "Russian Law Banning VPNs Comes Into Effect." https://themoscowtimes.com/news/russian-law-banning-anonymous-online-surfing-comes-into-effect-59434. Accessed April 11, 2018.

[iii] Financial Express. (2017). "Government reportedly lists 42 Chinese apps as dangerous, including TrueCaller, UC Browser, Mi Store: Check if your phone has any of them". https://www.financialexpress.com/industry/technology/government-reportedly-lists-42-chinese-apps-as-dangerous-including-truecaller-uc-browser-mi-store-check-if-your-phone-has-any-of-them/954335/. Accessed April 11, 2018.

[iv] NIST. (2012). Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[v] NIST. (2013). Special Publication 800-124 Revision 1, Guidelines for Managing the Security of Mobile Devices in in the Enterprise. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf