MARK E. GREEN, MD, TENNESSEE
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

One Hundred Nineteenth Congress
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

June 5, 2025

The Honorable Kristi Noem
Secretary
U.S. Department of Homeland Security
Washington, D.C. 20528

Dear Secretary Noem:

As you review the structure of the Cybersecurity and Infrastructure Security Agency (CISA), I urge you to prioritize your review of CISA's role as Sector Risk Management Agency (SRMA) of the communications sector. CISA must be equipped with the right tools and able to provide relevant guidance to improve the security of mobile devices, which have been repeatedly targeted by the People's Republic of China (PRC). Whether it is PRC-owned apps or nation-state sponsored actors, such as Salt Typhoon, CISA must be prepared to address commercial telecommunications infrastructure vulnerabilities that impact the security of our government mobile devices—a role that is especially important given CISA's mandate to protect Federal Civilian Executive Branch (FCEB) networks.

CISA's responsibilities as SRMA of the communications sector are supported by the Mobile App Vetting (MAV) program, which prioritizes FCEB network protection. The MAV program is a free service for FCEB agencies to comprehensively evaluate vulnerabilities, risks, and potential flaws in government-developed and third-party apps intended for government-furnished devices.[1] With the rise of smart phones, mobile apps have become central to the way Americans work, communicate, and complete daily tasks—including government employees, who are prime targets for malicious actors seeking access to sensitive information. I was therefore concerned to hear that the program will terminate in June 2025.

The security risks posed by certain mobile apps—especially those with linkages to the PRC—are well-documented. For example, TikTok's user agreement permits the app to monitor

[1] "Mobile App Vetting Fact Sheet", Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/sites/default/files/publications/CSSO-MAV-fact%2520sheet-2022.12.18-FINAL%2520_0.pdf.

keystrokes,[2] and its parent company, ByteDance, has close ties to the Chinese Communist Party (CCP).[3] Additionally, the backdoors of DeepSeek, a PRC-owned generative artificial intelligence (AI) platform, were immediately uncovered by security researchers.[4] The U.S. Select Committee on the Strategic Competition between the United States and the Chinese Communist Party exposed in April 2025 how DeepSeek—in addition to being "owned and operated by a CCP-linked company"[5]—places Americans at risk by routing their data through networks connected to a Chinese military company.[6]

However, threats to U.S. mobile devices go beyond notable apps like TikTok and DeepSeek. A wide range of applications have connections to servers in China, Russia, and Belarus,[7] among other locations, and they can potentially access government private data, track government employees' location, and exhibit other malicious behaviors.[8] In fact, in October 2023, the DHS Office of Inspector General (OIG) identified thousands of applications originating from companies banned by the U.S. government that were installed on mobile devices managed by U.S. Immigration and Customs Enforcement (ICE).[9] In response to one of the report's recommendations, ICE said it would develop a process for using CISA's MAV program for third-party applications.[10]

The termination of mobile device security programs would not only create a void in the ability to assess vulnerabilities on mobile devices, but also send the wrong signal to FCEB agencies, which are currently on heightened alert about the cybersecurity posture of their mobile

[2] "TikTok Browser Can Track Users' Keystrokes, According to New Research", New York Times, August 21, 2022, https://www.nytimes.com/2022/08/19/technology/tiktok-browser-tracking.html.
[3] "5 Things to Know About ByteDance, TikTok's Parent Company", Foundation for Defense of Democracies, March 12, 2024, https://www.fdd.org/analysis/2024/03/12/5-things-to-know-about-bytedance-tiktoks-parent-company/.
[4] "Wiz Research Uncovers Exposed DeepSeek Database Leaking Sensitive Information, Including Chat History", Wiz, January 29, 2025, https://www.wiz.io/blog/wiz-research-uncovers-exposed-deepseek-database-leak.
[5] "Moolenaar, Krishnamoorthi Unveil Explosive Report on Chinese AI Firm DeepSeek—Demand Answers from Nvidia Over Chip Use", The Select Committee on the Strategic Competition between the United States and the Chinese Communist Party, April 16, 2025, https://selectcommitteeontheccp.house.gov/media/press-releases/moolenaar-krishnamoorthi-unveil-explosive-report-chinese-ai-firm-deepseek.
[6] "DeepSeek Unmasked: Exposing the CCP's Latest Tool for Spying, Stealing, and Subverting U.S. Export Control Restrictions", The Select Committee on the Strategic Competition between the United States and the Chinese Communist Party, April 16, 2025, https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/DeepSeek%20Final.pdf.
[7] "Apple Offers Apps With Ties to Chinese Military", Tech Transparency Project, April 1, 2025, https://www.techtransparencyproject.org/articles/apple-offers-apps-with-ties-to-chinese-military.
[8] OIG-24-02, *Management Alert – ICE Management and Oversight of Mobile Applications (REDACTED)*, Office of the Inspector General, October 30, 2023, https://www.oig.dhs.gov/sites/default/files/assets/2023-11/OIG-24-02-Oct23-mgmtalert-Redacted.pdf.
[9] *Id*.
[10] *Id*.

devices due to Salt Typhoon.[11] As such, I request a briefing on how you will strengthen CISA's role as SRMA of the communications sector by Friday, June 13, 2025 that addresses the following questions:

1. When can Congress expect an update of CISA's Sector-Specific Plan for the Communications Sector, which has not been updated since 2015?

2. How can CISA improve information sharing with the Communications Sector?

    a. Has CISA been an effective partner in the Communications Information Sharing Analysis Center (ISAC)? Why or why not?

3. What are the shared services, whether new or existing, that CISA is considering offering to fulfill its role as SRMA of the Communications Sector and to protect FCEB networks?

4. Why is CISA terminating the MAV program earlier than its initial three-year Authorization to Operate (ATO)?[12]

5. How much did the MAV program cost, and how much would it cost DHS/CISA to scale the program?

    a. How much would the MAV program cost if it were to become a mandatory service for DHS components?

Per Rule X of the U.S. House of Representatives, the Committee on Homeland Security is the principal committee of jurisdiction for overall homeland security policy and has special oversight of "all Government activities relating to homeland security, including the interaction of all departments and agencies with the Department of Homeland Security."

I appreciate your attention to this important matter and look forward to working with you to protect our nation's mobile devices and the data that they hold.

[11] Zak Doffman, "FBI Warns iPhone And Android Users—Stop Sending Texts", Forbes, Dec. 6, 2024, https://www.forbes.com/sites/zakdoffman/2024/12/06/fbi-warns-iphone-and-android-users-stop-sending-texts/.
[12] "Mobile App Vetting Fact Sheet", Cybersecurity and Infrastructure Security Agency, March 2024, https://www.cisa.gov/sites/default/files/2024-04/CSSO-MAV-FACT-SHEET_508c_0.pdf.

One Hundred Nineteenth Congress
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

Sincerely,

ANDREW R. GARBARINO
Chairman
Subcommittee on Cybersecurity and
Infrastructure Protection