United States Senate
WASHINGTON, DC 20510

December 4, 2024

The Honorable Robert P. Storch
Inspector General
Department of Defense
4800 Mark Center Drive
Alexandria, VA 22350-1500

Dear Mr. Storch:

We write to request that you investigate the Department of Defense's (DOD) failure to secure its unclassified telephone communications from foreign espionage, risking serious harm to U.S. national security.

On November 13, 2024, the Federal Bureau of Investigation and the Cybersecurity and Infrastructure Security Agency publicly confirmed that Chinese-government hackers compromised "multiple telecommunications companies," and that the data stolen included "customer call records data" as well as "private communications of a limited number of individuals who are primarily involved in government or political activity." The press has reported that the surveillance targets included President-elect Trump, Vice President-elect Vance, and Senate Majority Leader Schumer. This successful espionage campaign should finally serve as a wake-up call to officials across the federal government who failed to shore up the government's communications security, despite repeated warnings from experts and Congress.

On May 8, 2024, the Navy finalized a new DOD-wide contract for unclassified commercial wireless devices and services for soldiers and civilian employees. The contract can be extended up to 9 additional years, with a potential value of $2.67 billion. The wireless companies selected under the Spiral 4 contract include AT&T, Verizon, and T-Mobile, which were reportedly breached by China as part of the recently revealed "Salt Typhoon" hack.

In the two attached whitepapers, which DOD sent to Congress in July 2024 and October 2024, DOD confirmed that its contracted carriers have significant cybersecurity problems and are vulnerable to foreign surveillance. While DOD indicated that it has mitigated some of the risks posed by adversaries exploiting some of the carriers' vulnerabilities through encryption technology, it has also confirmed that other surveillance threats, such as foreign governments' ability to track the location of specific phones, can only be mitigated by the wireless carriers. This national security threat was publicly identified by the Department of Homeland Security in 2017, yet DOD has seemingly failed to include requirements in the Spiral 4 contract that the carriers address these vulnerabilities and protect DOD personnel from foreign espionage. As DOD considers the renewal of Spiral 4 contracts, DOD should require findings from third-party audits or conduct its own cybersecurity audits. DOD has communicated to Congress that it has

been unable to review third-party audits commissioned by carriers included in Spiral 4, which provide important information regarding the resiliency of carriers against foreign espionage

DOD's continued use of unencrypted landline phones and platforms like Microsoft Teams undermines secure communication at DOD. Teams and certain other platforms utilized by DOD are not end-to-end encrypted by default, causing concerning gaps in security that could easily be mitigated. End-to-end encrypted voice, video, and text messaging tools such as Signal, WhatsApp, and FaceTime better protect communications in the event that the company that offers the service is hacked. Despite the widespread availability of secure alternatives, agencies instead continue to use unencrypted phone lines and insecure communications platforms.

Some DOD components have begun to pilot, on a limited basis, a potentially more secure superior communications platform, known as Matrix, which is end-to-end encrypted by default, interoperable, not controlled by any one company, and widely used by multiple NATO allies. For example, the attached presentation, provided to Congress in July, describes the Navy's successful use of Matrix, including on 23 ships. While we commend DOD for piloting such secure, interoperable communications technology, its use remains the exception; insecure, proprietary tools remain far more widespread within DOD and the federal government generally. The widespread adoption of insecure, proprietary tools is the direct result of DOD leadership failing to require the use of default end-to-end encryption, a cybersecurity best practice, as well as a failure to prioritize communications security when evaluating different communications platforms.

DOD has defended its continued use of unencrypted landline phones, which it described as "acceptable from a risk-management perspective" in the attached whitepaper, dated August 29, 2024. DOD told Congress that it assessed "that there are no 'unnecessary' risks posed by such use" of landline phones. DOD further defended the practice as "balanc[ing] acceptable risk with operational requirements" and stated that "prohibiting [telephone] collaboration would have a significant negative effect on DOD's world-wide, real-time mission, and is unnecessary to protect unclassified communication." Less than three months after DOD provided that whitepaper to Congress, the press reported the Salt Typhoon hack of U.S. telecommunications companies, and several other federal agencies reportedly directed their employees to stop communicating via phone lines.

DOD's failure to secure its unclassified voice, video, and text communications with end-to-end encryption technology has left it needlessly vulnerable to foreign espionage. Moreover, although DOD is among the largest buyers of wireless telephone service in the United States, it has failed to use its purchasing power to require cyber defenses and accountability from wireless carriers. The responsibility for such failures cannot and should not be pinned on low-level procurement officials, but rather, reflects a failure by senior DOD leadership to prioritize cybersecurity, and communications security in particular. We urge you to investigate DOD's failure to secure its communications, and to recommend the changes in policy necessary to protect DOD communications from foreign adversaries. Further, DOD's Spiral 4 contracts are actually one-

year contracts, which the government can renew up to 9 more years at its discretion. We urge you to consider whether DOD should decline to renew these contracts and instead renegotiate with the contracted wireless carriers, to require them to adopt meaningful cyber defenses against surveillance threats, and if requested, to share their third-party cybersecurity audits with DOD.

Sincerely,

Ron Wyden
United States Senator

Eric S. Schmitt
United States Senator