United States Senate
COMMITTEE ON ARMED SERVICES
WASHINGTON, DC 20510–6050

November 15, 2023

The Honorable Lloyd J. Austin III
Secretary of Defense
1000 Defense Pentagon
Washington, DC 20301-1000

Dear Secretary Austin:

This month, researchers from Duke University released a study finding that U.S. data brokers are collecting and selling the sensitive personal information of active-duty members of the military, their families, and veterans. Sensitive personal information includes the geolocation, health, and financial data of service members, as well as information about their religious practices and more. This poses a significant national security risk. Unfettered access to the sensitive personal information of U.S. military personnel threatens their privacy and safety, jeopardizes the integrity and security of our cyber network defenses, and risks weakening U.S. military superiority, starting with the basic data security of our personnel.

The study further suggests that service members' data could be purchased from data brokers for cents on the dollar and some data brokers lacked any meaningful controls to limit or prevent the sale of this sensitive information to foreign entities. This troubling finding makes clear that adversaries have many tools at their disposal to breach U.S. networks, even beyond typical offensive capabilities. This ought to immediately change.

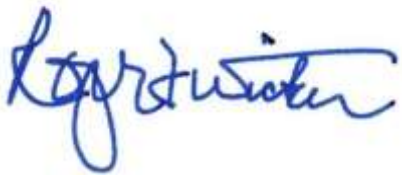
The United States is facing a persistent threat in cyberspace. Foreign adversaries and malicious cyber actors are continuously seeking ways to exploit our technological vulnerabilities and undermine our military's competitive edge on the battlefield. Recent intelligence reports and testimony from the Commander of U.S. Cyber Command, General Nakasone, before the Senate Armed Services Committee this year confirm that cyber threats from nation states and their surrogates will remain acute against the United States.

At a time when cyber threats are growing in number and intensity, I urge you to employ all available means at your disposal to protect the sensitive personal information of U.S. service members and their families. That starts with ensuring that military personnel implement strict privacy settings on their digital devices and enhancing internal Department of Defense (DoD) trainings on information security. Department leadership should also remove all unauthorized applications from DoD mobile devices and enforce strict cybersecurity protections throughout DoD's Bring Your Own Device Programs.

Simply put, the privacy and security of U.S. military personnel data is essential to DoD's ability to defend against hostilities in cyberspace and carry out its national security mission. I respectfully request

that you provide periodic updates about what actions the Department is taking to help reduce the exposure of service members' sensitive personal information to data brokers. A renewed focus on protecting the data of military personnel is imperative to securing cyberspace and defending the homeland. Thank you for your prompt attention to this matter.

Sincerely,



Roger F. Wicker
Ranking Member