Congress of the United States

Washington, DC 20515

May 28, 2026

The Honorable Kirsten A. Davies
Chief Information Officer
Department of Defense
6000 Defense Pentagon
Washington, D.C. 20301-6000

Dear Ms. Davies:

We write with serious concern that the Department of Defense (DoD) has not taken basic steps to protect U.S. military personnel from the serious counterintelligence and force protection threat posed by the collection and sale of personal information, including cell phone location data, by data brokers. DoD has known about this serious threat for over a decade, but has failed to adopt commonsense cyber defenses that are recommended by federal agencies. DoD has now confirmed to Congress that foreign adversaries are exploiting commercially available location data to target U.S. military personnel in war zones.

U.S. Central Command (USCENTCOM) told Congress that it "received multiple threat reports concerning adversary exploitation of commercial location data to target or surveil U.S. personnel in theater," for Operation Epic Fury, in the attached document on April 14, 2026. DoD has yet to provide further information on these reports requested by Congress.

This is the first time DoD has confirmed that adversaries are using commercial location data to target U.S. military personnel in an active war zone. Commercial location data can be used to identify where U.S. troops congregate and their pattern of life, which can be exploited by adversaries to target attacks such as missiles, drones, and roadside bombs, as well as for counterintelligence purposes. That foreign adversaries are still able to buy location data collected from the phones of U.S. personnel serving in military hotspots is a direct result of DoD leadership's failure to prioritize this threat and implement common sense cyber defenses recommended by federal cybersecurity experts.

DoD officials have reportedly known about the threat that commercial data brokers pose to national security for at least a decade. In 2016, a government contractor briefed senior military officials at the Joint Special Operations Command, which the contractor revealed to Wired in a 2024 article. The contractor's presentation, which was first reported publicly by the Wall Street Journal in 2021, showed how commercially available phone location data could be weaponized for pattern of life analysis. During the presentation, the contractor was able to track phones from U.S. military bases associated with special operations units to an abandoned cement factory in Syria, which was reportedly a staging area at the time for U.S. special operations and allied forces.

DoD officials have not treated this counterintelligence and force protection threat as a five-alarm fire. Instead, per press reports, DoD has encouraged the growth of this industry by buying location data from this contractor and other data brokers. As Motherboard reported in 2021, DoD was purchasing location data sourced from Muslim prayer and dating apps. In 2022, the Defense Intelligence Agency revealed to Congress that it buys and searches domestic location data without a warrant. DoD officials told the Wall Street Journal in 2021 that they had implemented policies to address this threat that protected "DoD personnel and operations while still

allowing flexibility to benefit from geolocation capabilities in certain low-risk situations." But those policies have not been effective.

Indeed, in 2024, an international consortium of journalists tracked U.S. military personnel at bases in Germany, including tracking their movements off-base. The journalists used a free sample of location data containing 3 billion data points from 11 million mobile devices that they received from a U.S.-based data broker. From this dataset, the journalists were able to track 12,313 devices that appeared to spend time at or near at least 11 military sites in Germany. DoD officials briefed Congress in January 2025 and shared copies of current policies related to the threat of commercial location data. While those policies are marked Controlled Unclassified Information and cannot be quoted in this letter, we remain deeply concerned that DoD is not doing enough, including by not requiring basic cyber defenses.

USCENTCOM further confirmed to Congress in April that DoD has still not adopted one of the most important cyber defenses against this threat. The two major smartphone operating systems — Apple's iOS and Google's Android — are both designed by those companies to assign a unique tracking number to each smartphone for use by the advertising industry and data brokers. Both iOS and Android also include an opt-in privacy setting to disable this unique advertising ID, which the National Security Agency and the Cybersecurity and Infrastructure Security Agency recommend. Unfortunately, USCENTCOM confirmed that the advertising ID is still not disabled on government-issued smartphones, but stated that the Defense Information Systems Agency is currently testing a capability to do so. USCENTCOM also revealed that it only rolled out the capability to administratively disable location sharing on smartphones in May, 2026.

DoD has known about this threat for over a decade, yet have failed to take meaningful steps to protect our men and women in uniform. That is simply unacceptable. DoD must immediately adopt common sense cyber protections to prevent the sale of location data that can undermine national security and risk the lives of U.S. personnel. To that end, we urge you to take the following actions:

1. Disable the advertising ID on all DoD issued smartphones and issue a policy mandating that DoD personnel disable the advertising ID on all personal phones brought onto DoD facilities or taken to overseas deployments.
2. Remove web browsers that are designed to facilitate data collection by Google and other advertising companies, such as Google Chrome, from DoD unclassified computers and smartphones. Instead, DoD should pre-install on DoD devices and require the use by DoD personnel of privacy-focused web browsers that protect users with anti-tracking cyber defenses, such as ad blocking and the Global Privacy Control (GPC), which is already enforced by law in 12 states.
3. Coordinate with the California Privacy Protection Agency to enroll all DoD personnel who are California residents in the state's universal data broker Delete Request and Opt-out Platform, and coordinate with other states that create similar systems.

Please also provide written answers to the following questions by June 26, 2026:

1. Does DoD contractually require vendors to restrict data collection and prohibit the transfer or sale of data collected from DoD personnel or DoD facilities to third parties? If not, will you commit to including such provisions in vendor contracts going forward?
2. What actions, if any, has DoD taken to implement the recommendations in the May 4, 2025 Army Cyber Institute Report on "Tracking The Trackers: Commercial Surveillance Occurring on U.S. Army Networks"? If DoD has not implemented these recommendations, please explain why, for each of the 6 recommendations.
3. How has DoD used the authorities under Sec. 1645 of the FY 2017 NDAA ("Cyber protection support for Department of Defense personnel in positions highly vulnerable to cyber attack.")? Specifically, which personnel has DoD designated as high risk, what cyber assistance is DoD providing, and what steps has DoD taken to assess the effectiveness of this assistance against cyber and force protection threats?
4. DoD has previously acknowledged purchasing location data, including domestic location data. What steps is DoD taking to analyze such purchased data to identify data brokers collecting and selling data of DoD personnel and DoD facilities where existing anti-tracking policies are not effective? If DoD has not taken such steps, why not?
5. Is DoD still funding research into commercial data threats to DoD personnel, including by the Digital Force Protection Lab at the Army Cyber Institute at West Point and the Threat Systems Management Office at Redstone Arsenal? If not, why not?

Thank you for your attention to this important matter.

Sincerely,

Ron Wyden
United States Senator

Pat Harrigan
Member of Congress

Robert Garcia
Ranking Member
Committee on Oversight and
Government Reform

Elijah Crane
Member of Congress

Martin Heinrich
United States Senator

Matt Van Epps
Member of Congress

Elizabeth Warren
United States Senator

Scott Perry
Member of Congress

Edward J. Markey
United States Senator

Keith Self
Member of Congress

Alex Padilla
United States Senator

Michael Cloud
Member of Congress

Sara Jacobs
Member of Congress

W. Gregory Steube
Member of Congress

CC: Bradley Hansell, Under Secretary of Defense for Intelligence and Security
Jennifer M. Urban, Chair, California Privacy Protection Agency Board

1. Are DOW personnel in theatre prohibited from using personal smartphones? If not, what steps has USCENTCOM taken to prevent the collection and sale of location data from these devices, such as by requiring DOW personnel to disable the advertising ID on their personal phones?

RESPONSE: (U) CENTCOM personnel are not prohibited from possessing or using personal smartphones within the USCENTCOM AOR. However, USCENTCOM maintains specific restrictions on geolocation features through Command Policy Letter Number 25-10, United States Central Command Geolocation Policy, December 4, 2025.

(U) USCENTCOM's geolocation risk guidance directs personnel to disable geolocation functionality when not needed; periodically review device and application privacy settings; and limit public sharing of information. The guidance notes that disabling geolocation capabilities does not always fully disable them on commercial products, requiring personnel to implement comprehensive device security measures including privacy setting reviews. The policy letter prescribes escalating geolocation restrictions tied to Force Protection Condition (FPCON) levels. The USCENTCOM Commander directed the immediate implementation of FPCON Delta, All Measures for the USCENTCOM AOR on 28 February 2026, which imposes the most restrictive geolocation controls across the theater.

2. Are government-issued phones used by DOW personnel in theatre all configured to disable the device's mobile advertising ID, consistent with the recommendations of CISA?

RESPONSE: (U) Yes, the Personalized Advertising setting is disabled by group policy on the Mobile Device Management Server. However, Ad Targeting Information is not disabled and can be edited by a user. DISA is currently testing implementation to disable the Ad Targeting Information setting on government-issued cell phones. USCENTCOM is currently migrating government-issued mobile devices to a new Mobile Device Management Server which will allow for location services to be completely disabled, estimated completion date is 6 May 26.

3. Has USCENTCOM received any reports about adversaries using commercial location data to target US personnel in theatre?

RESPONSE: (U) Yes, USCENTCOM has received multiple threat reports concerning adversary exploitation of commercial location data to target or surveil US personnel in

theater. The Threat Fusion Cell identified, tracked, and disseminated these threats through the USCENTCOM Threat Working Group and to component force protection personnel. Additionally, USCENTCOM has disseminated threat assessments to component force protection personnel demonstrating adversary capabilities to exploit commercial location data for targeting purposes. These assessments inform force protection measures across the AOR.

4. Are any government vehicles in theatre transmitting location data back to the manufacturers of those vehicles?

RESPONSE: (U) We defer to the individual Services as they are responsible for the contracts on the vehicles.