Congress of the United States

Washington, DC 20515

September 4, 2026

The Honorable Platte B. Moring III
Inspector General
U.S. Department of Defense
4800 Mark Center Drive
Alexandria, VA 22350

Dear Inspector General Moring:

We write to request that the Department of Defense (DoD) Office of the Inspector General (OIG) review the effectiveness of existing DoD policies, technical controls, and operational security (OPSEC) guidelines designed to protect military personnel and sensitive DoD operations from the counterintelligence and physical security threats posed by the sale of commercially available location data.

The sale of location data, particularly that of U.S. government personnel, poses a serious threat to national security. U.S. Central Command recently confirmed that foreign adversaries have used commercial location data to target U.S. military personnel, an admission that Representative Harrigan, 12 other Members of Congress and I revealed in a May 2026 letter to the DoD Chief Information Officer (CIO). This threat is further detailed in earlier press reports as well as the attached, non-public report produced by a U.S. defense contractor, which demonstrates how easily commercially harvested telemetry can be used to track movements to and from sensitive DoD facilities.

According to cybersecurity experts, including the National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA), one of the most effective ways to mitigate data broker threats is to disable the unique advertising IDs built into smartphones. Mobile advertising IDs (MAIDs) serve as the primary bridge linking advertising bidstream data and Software Development Kit location points to a single persistent profile, allowing data brokers to aggregate precise location trails and sell them to third parties. Indeed, as detailed in the attached memos, several DoD components— the Army, Air Force, Navy and Marine Corps, and Special Operations Command—confirm that they now disable advertising IDs on government-issued devices to protect their personnel from such threats. For example, the Navy CIO noted that "by blocking this identifier, the [Navy] curtails the ability of foreign adversaries to purchase bulk location data and metadata, which is frequently leveraged to track, profile, and target military and civilian personnel."

We commend these service branches for implementing this cybersecurity defensive best practice on government devices. However, recent reports regarding the continued availability of commercial location data originating from DoD facilities raise troubling questions. One possibility is that certain DoD components have not, in fact, fully disabled the advertising IDs on government devices or only recently implemented these policies. For example, the Air Force revealed its policy was implemented in July, after the congressional request for the memo. Another possibility is that disabling the advertising ID is no longer a sufficient defense on its own, as data brokers can still capture, correlate, and monetize unique location data using other information collected from phones. A third—and particularly alarming—possibility is that the commercial data currently available for sale originates entirely from personal devices brought into DoD facilities and operational areas by service members and government contractors.

We request that the DoD OIG examine location datasets already purchased by DoD and other federal agencies and use them to query DoD facilities and military bases and identify where DoD policies have not prevented the sale of location data. In particular, we request that you determine whether commercially available data is originating from personal phones. If personal devices are identified as the primary source of this data, your office should recommend concrete policy changes to eliminate this vulnerability, enforce technical controls on personal devices in sensitive areas, and safeguard DoD personnel and OPSEC from commercial surveillance.

Thank you for your attention to this important matter. Please provide a response to this letter no later than October 2, 2026, detailing the actions the OIG intends to take.

Sincerely,

Ron Wyden
United States Senator

Pat Harrigan
Member of Congress

DEPARTMENT OF THE ARMY
DEPARTMENT OF THE ARMY
OFFICE OF THE CHIEF INFORMATION OFFICER
107 ARMY PENTAGON
WASHINGTON, DC 20310-0107

The Honorable Ron Wyden
United States Senate
221 Dirksen Senate Office Building
Washington, DC 20002
ATTN: Dr. Chris Soghoian

08 Jul 26

MEMORANDUM FOR SENATOR RON WYDEN

SUBJECT: Confirmation of Disabling Mobile Advertising Identifiers (MAID)

Dear Senator Wyden:

This letter is in response to your staff's request for written confirmation of information provided during a previous briefing regarding the best cybersecurity practices for Army Mobile Device applications.

I can confirm that the Department of the Army disables the mobile advertising identifier (MA ID) within our secure application environment as standard security protocol. The disabling of MA ID is part of our standard configuration process for what in the Department of the Army is known as Mobile Application Management (MAM) suite of tools with Microsoft Intune.

The application of this disablement of MA ID is applied also to Government Furnished Equipment (GFE) configuration across all desktop Windows environments, Android, and Apple hardware utilized within the Department of the Army.

By disabling the MA ID within our MAM configurations, the Army strives to reduce risk to our warfighters and civilians of foreign adversaries looking to purchasing commercially available location data and other metadata to track, target, and/or compromise our soldiers. These measures allow the Army to offer flexibility and convenience to our personnel without sacrificing mission security or user privacy.

Thank you for your continued support of the Army's cybersecurity practices.

Sincerely,

Gabriel Chiulli
Acting Army Chief Information Officer

DEPARTMENT OF THE AIR FORCE
WASHINGTON DC

OFFICE OF THE SECRETARY

August 18, 2026

SAF/CN
1670 Air Force Pentagon
Washington, DC 20330-1670

The Honorable Ron Wyden
United States Senate
221 Dirksen Senate Office Building
Washington, DC 20002

Dear Senator Wyden,

Thank you for your inquiry regarding the Department of the Air Force's security protocols, specifically concerning the configuration of the Mobile Advertising Identifiers (MAID) and our alignment with the security standards implemented by the Department of the Army.

I can confirm the configuration to disable MAID is actively enforced at the tenant level for all iOS devices, encompassing both iPads and iPhones.

The DAF disabled tracking and advertising identifiers on Windows and Android enterprise devices via Group Policy Objects (GPOs) and mobile device management baselines to enhance operational security and mitigate data exposure risks. Implementation initiated July 23, 2026, with enterprise-wide compliance and deployment completed on July 27, 2026.

We remain committed to ensuring the highest levels of security across all our networks and devices. Please let us know if you require any further information.

Sincerely,

Ashley N. Devoto
Chief Information Officer

DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER
1000 NAVY PENTAGON
WASHINGTON, D.C. 20350-1000

July 22, 2026

The Honorable Ron Wyden
United States Senate
221 Dirksen Senate Office Building
Washington, DC 20002
ATTN: Dr. Chris Soghoian

Dear Senator Wyden:

This letter is in response to your staff's request for written confirmation regarding cybersecurity of Department of the Navy (DON) Mobile Devices.

I can confirm that the DON disables the Mobile Advertising Identifier (MAID) within its secure application environment as a standard cybersecurity protocol for Government Furnished Equipment (GFE) and Mobile Application Management (MAM) configurations.

Disabling the MAID restricts the generation of commercially available tracking data. By blocking this identifier, the DON curtails the ability of foreign adversaries to purchase bulk location data and metadata, which is frequently leveraged to track, profile, and target military and civilian personnel. Implementing these guardrails ensures that the DON can offer flexible, modern mobile capabilities to personnel without compromising mission security or individual user privacy.

If I may be of any further assistance, please let me know.

Sincerely,

M. BARRY TANNER
Performing the Duties of the
Chief Information Officer

RESPONSE TO CONGRESSIONAL INQUIRY
RFI 26-114
28 July 2026

SUBJECT: Cyber Defense Best Practice Implementation

PURPOSE: Respond to a request from Senator Wyden's office on implementation of a standardized cyber defense protocol that disables the Mobile Advertising Identifier.

Q1: Has USSOCOM implemented the same cyber defense described in the Army memo that disables the Mobile Advertising Identifier (MA ID) across all enterprise hardware and user profiles?

A1: USSOCOM disables the mobile advertising identifier (MA ID) using Microsoft Intune Mobile Application Manager (MAM) as standard security protocol for all managed mobile devices. This restriction is actively enforced for both Android and IOS devices across the Enterprise. To block content such as pop-ups and prevent Microsoft from collecting users browsing history on Windows 11 laptops, USSOCOM applies various Security Technical Implementation Guides (STIG) to browsers such as Firefox, Chrome, and Edge. Additionally, MA ID was recently disabled on Windows systems to improve our security posture and further reduce the opportunity for adversaries to purchase commercially available location and other metadata for use against USSOCOM personnel.