

**UNCLASSIFIED**

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

**UNCLASSIFIED**

**UNCLASSIFIED**

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.

**UNCLASSIFIED**