DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

AUG 0 3 2018

MEMORANDUM FOR CHIEF MANAGEMENT OFFICER OF THE DEPARTMENT OF DEFENSE
SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
CHIEF OF THE NATIONAL GUARD BUREAU
COMMANDERS OF THE COMBATANT COMMANDS
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF COST ASSESSMENT AND PROGRAM EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF OPERATIONAL TEST AND EVALUATION
CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE
ASSISTANT SECRETARY OF DEFENSE FOR LEGISLATIVE AFFAIRS
ASSISTANT TO THE SECRETARY OF DEFENSE FOR PUBLIC AFFAIRS
DIRECTOR OF NET ASSESSMENT
DIRECTORS OF DEFENSE AGENCIES
DIRECTORS OF DOD FIELD ACTIVITIES

SUBJECT: Use of Geolocation-Capable Devices, Applications, and Services

The rapidly evolving market of devices, applications, and services with geolocation capabilities (e.g., fitness trackers, smartphones, tablets, smartwatches, and related software applications) presents significant risk to Department of Defense (DoD) personnel both on and off duty, and to our military operations globally. These geolocation capabilities can expose personal information, locations, routines, and numbers of DoD personnel, and potentially create unintended security consequences and increased risk to the joint force and mission.

Effective immediately, DoD personnel are prohibited from using geolocation features and functionality on both non-government and government-issued devices, applications, and services while in locations designated as operational areas (OAs). Combatant Commanders or their designees:

- May authorize the use of geolocation capabilities on non-government devices, applications, and services in OAs after conducting a threat-based comprehensive Operations Security (OPSEC) survey, in accordance with DoD Directive 5205.02E, "DoD Operations Security Program."

OSD009823-18/CMD012429-18

- May authorize the use of geolocation capabilities on government-issued devices, applications, and services in OAs based upon mission necessity, taking into account the potential OPSEC risks.

- Will ensure all personnel under their purview receive training in accordance with this memorandum.

For all other locations, installations, and activities, the heads of DoD Components will consider the inherent risks associated with geolocation capabilities on devices, applications, and services, both non-government and government-issued, by personnel both on and off duty. When information derived from these capabilities poses a threat to personnel and operations, commanders and supervisors at all levels:

- Will provide OPSEC training and guidance, in accordance with DoD Directive 5205.02E, commensurate with the risk and local operating conditions.

- Should apply a tiered structure for categorizing location and operations sensitivity while incorporating risk factors to ensure restrictions are consistently and rationally applied.

No later than 30 days from the date of this memorandum the DoD Chief Information Officer (CIO) and the Under Secretary of Defense for Intelligence (USD(I)) will jointly develop geolocation risk management guidance and training to inform commanders and heads of DoD Components when making risk decisions regarding these devices. DoD CIO, in collaboration with USD(I), will update the annual Cybersecurity Awareness training to assist DoD personnel in identifying and understanding risks posed by geolocation capabilities embedded in devices and applications. The geolocation risk management guidance and training will be posted at https://iase.disa.mil.

My point of contact for this effort is Carrie Wibben, carrie.l.wibben.civ@mail.mil, (703) 692-3758.