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

MAY 2 2 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: Mobile Device Restrictions in the Pentagon

1. Purpose. This memorandum prescribes guidance and procedures for mobile device restrictions within the Pentagon.

2. Applicability.

a. This memorandum establishes restrictions for mobile devices anywhere within the Pentagon that is designated or accredited for the processing, handling, or discussion of classified information.

b. This memorandum applies to all Department of Defense (DoD) and Office of the Secretary of Defense (OSD) Components ("Components"), as well as military personnel, civilian employees, contractors, and visitors in the Pentagon. For purposes of this memorandum, the term "Pentagon" means the Pentagon Office Building and its supporting facilities located on that area of land (consisting of approximately 227 acres) located in Arlington County, Virginia.

c. This does not apply to approved medical devices. In evaluating requests to approve medical devices for civilian employees, an individualized assessment will be made consistent with the requirements of the Rehabilitation Act of 1973, as amended.

d. This does not apply to mobile devices having minimal storage and transmission capabilities such as key fobs used for medical alert, motor vehicles, or home security systems.

e. This does not apply to fitness trackers that do not contain camera, microphone, cellular, or Wi-Fi technology.

3. Policy.

a. Personal and Government mobile devices that transmit, store, or record data are prohibited inside secure spaces within the Pentagon.

b. Mobile devices may be used in common areas and spaces within the Pentagon that are not designated or accredited for the processing, handling, or discussion of classified information.

c. Components will comply with any applicable labor relations obligations when implementing this policy.

4. Control Procedures and Device Storage. .

a. Mobile devices must be stored in daily-use storage containers that are located outside the secure space.

b. Mobile devices must be powered off prior to being stored, and must remain powered off until retrieved.

c. Signs displaying the prohibition and control procedures must be posted outside all secure spaces.

5. Requests for Exceptions.

a. Component Senior Agency Officials will submit written requests for exceptions on behalf of their respective Component and will be responsible for compliance.

b. All requests for exceptions must be submitted to the Under Secretary of Defense for Intelligence (USD(I)).

c. Government-issued mobile devices.

(1) The USD(I) and the Department of Defense Chief Information Officer (DoD CIO), may jointly grant exceptions to this policy for government-issued mobile devices pursuant to DoD Manual 5200.01, Vol 1, "DoD Information Security Program: Overview, Classification and Declassification." USD(I) and DoD CIO will prescribe procedures for requesting exceptions and documenting approved exceptions.

(2) Exception requests for unclassified government-issued mobile devices that will regularly be present in secure spaces (for example, a laptop or tablet serving as a desktop

replacement) must have an approved process for disabling the camera and microphone functionality and have technical measures in place to disable Wi-Fi connectivity.

d. Personal mobile devices. Exceptions for personal mobile devices will not be granted. Note, however, that under paragraph 2.c, approved medical devices are not covered by this policy, and paragraphs 2.d and 2.e have further exclusions.

6. Security Violations and Enforcement.

a. Failure to abide by the rules promulgated in this memorandum and other applicable laws and regulations regarding security violations involving classified information may subject military members, civilian employees, and contractors to appropriate disciplinary and/or administrative actions, fines, or other appropriate actions, and may result in a review of the individual's security clearance eligibility. Also, military members may be subject to punishment under chapter 47 of the United States Code (also known as "the Uniform Code of Military Justice" or "UCMJ"). The Secretaries of the Military Departments will maintain regulations that make punishable, under Article 92 of the UCMJ, any violation of the restrictions imposed by this memorandum by persons subject to the UCMJ.

b. Pentagon Force Protection Agency (PFPA), in coordination with tenant space security managers, will randomly conduct security inspections in and around classified spaces to monitor compliance, to include the use of wireless detection capabilities.

c. Tenant managers and/or supervisors in Components will ensure prohibited devices are immediately removed from the space and under appropriate circumstances inspected for activities that could result in the loss or compromise of classified information, such as audio recordings of classified information discussions or photography of classified information from computer screens or paper documents. Security violations will be reported in accordance with DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information."

d. In accordance with applicable rules and regulations regarding physical access to the Pentagon, persons who violate this policy may be denied access thereto.

7. Responsibilities.

a. Tenant managers and/or supervisors in Components are responsible for:

(1) Enforcing the requirements in this memorandum;

(2) Ensuring that daily-use storage containers are available outside the entry control points to secure spaces within the Pentagon;

(3) Posting applicable signage delineating a space as a secure space and the restrictions for mobile devices;

(4) Coordinating with Washington Headquarters Services (WHS), Integrated Services Division at 703-693-3768 or https://my.whs.mil/services/mobile-devices to obtain information regarding the procurement and installation of identified standard daily-use storage containers to deconflict with fire, safety and construction requirements. Information can be found on the WHS website, and;

(5) Coordinating with USD(I) and DoD CIO for approved disabling instructions prior to introducing government-issued mobile devices into secure space.

b. All tenants will ensure their visitors are aware of the restrictions and requirements in this memorandum.

c. PFPA will report results of random screenings quarterly to senior leadership and brief the Pentagon Governance Council (PGC) on violations.

d. The DoD CIO will ensure the annual Cyber Awareness training includes information on the risks associated with mobile devices in areas processing classified information.

e. USD(I) and DoD CIO will establish a process for assessing technical capabilities of medical devices to inform component Human Resource officials on decisions regarding introduction of these into secure spaces.

f. WHS will issue a Pentagon Building Circular establishing guidance and procedures for WHS daily-use storage containers, including their installation within the Pentagon. In doing so, WHS will coordinate with PFPA regarding security standards and with the Pentagon fire marshal regarding fire safety.

8. Implementation.

a. Components will begin implementation immediately, with complete implementation no later than 180 days after the date of this memorandum.

(1) Government-issued unclassified mobile devices that function as a desktop replacement within a secure space must have approved interim mitigations applied until replaced with compliant devices, no later than 180 days after the date of this memorandum.

(2) Government-issued classified mobile devices may continue to operate as previously approved while a request for exception is submitted as described in Section 5 of this memorandum.

(3) All other government-issued and personal mobile devices must be removed from secure spaces immediately.

b. Components will immediately conduct a survey of mobile devices being used in secure spaces and coordinate with their service provider to implement any needed mitigations.

c. Components will update the PGC monthly on progress and issues until implementation is complete.

9. Definitions. For the purposes of this memorandum only, the following definitions apply:

a. Secure Space: An area that has been designated or accredited for the processing, handling, or discussion of classified information.

b. Senior Agency Official: An official appointed by the Head of a DoD or OSD Component to be responsible, within the Pentagon, for direction, administration, and oversight of the Component's Information Security Program, to include classification, declassification, safeguarding, and security education and training programs.

c. Mobile Device: Also referred to as a portable electronic device, a mobile device is a portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable data storage; and (iv) is powered-on for extended periods of time with a self-contained power source. Mobile devices include but are not limited to laptops, tablets, cellular phones, smartwatches, and other devices with these characteristics, but exclude those devices described in 2.c, 2.d, and 2.e.

d. Disabled: Rendering a capability inoperable in an USD(I)-approved manner that cannot be reversed in software.

e. Interim Mitigation: Examples include but are not limited to the following:

(1) Covering cameras on mobile devices in secure spaces.

(2) Disabling Wi-Fi and audio recording capability on mobile devices in secure spaces.

10. The USD(I) will incorporate this memorandum into a new or existing DoD issuance within 180 days.

11. Points of contact for this memorandum are Mr. Josh Freedman, 703-692-3724, for the USD(I), and Mr. Will Alberts, 571-372-4727, for the DoD CIO.

Patrick M. Shanahan

cc:
Director of National Intelligence