OFFICE OF THE SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
COMMANDERS OF THE COMBATANT COMMANDS
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Use of Non-Government Owned Mobile Devices

References: (a) DoD Instruction 5200.48, "Controlled Unclassified Information," March 6, 2020
(b) DISA Cloud Computing Security Requirements Guide v1R3, March 6, 2017
(c) DoD Instruction 8500.01, "Cybersecurity," October 7, 2019
(d) DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," December 29, 2020
(e) DoD Instruction 8520.03, "Identity Authentication for Information Systems," July 27, 2017
(f) DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information," July 28, 2020
(g) DoD Chief Information Officer Memorandum, "Mobile Application Security Requirements," October 6, 2017
(h) DoD Chief Information Officer Memorandum, "DoD Mobile Public Key Infrastructure (PKI) Credentials," December 20, 2019
(i) OMB Circular No. A-130, "Managing Information as a Strategic Resource," July 28, 2016
(j) DoD Instruction 5400.11, "DoD Privacy and Civil Liberty Programs," January 29, 2019
(k) DoD Instruction 5015.02, "DoD Records Management Program," August 17, 2017

This memorandum and attachment establish minimum requirements for the use of non-government owned mobile devices (e.g., personally or commercially owned), hereinafter "Approved Mobile Device" (AMD), to store, process, transmit, or display up to Department of Defense (DoD) Controlled Unclassified Information (CUI). This memorandum's scope is limited to mobile device information technology (IT) with mobile operating systems (OS) (e.g., Apple iOS, Android) used to access and process up to DoD CUI (e.g., Impact Level 5 data), as defined in references (a) and (b). Additional guidance will be provided by the DoD Chief Information Officer (CIO) to expand the scope to additional types of non-government owned devices (e.g., laptops, desktops), OS types (e.g., macOS, Windows), and capabilities (e.g., voice applications).

The benefits associated with the use of AMDs must be balanced carefully with associated operations security and cybersecurity risks. This guidance provides technical and programmatic requirements for Components managing and configuring AMDs to store, process, transmit, access, or display DoD CUI. This memorandum does not supersede, cancel, or change existing requirements for safeguarding, storage, handling, or transmission of DoD CUI.

DoD Component Heads and Authorizing Officials, in collaboration with Component CUI Senior Agency Officials and the DoD Senior Information Security Officer, are responsible for safeguarding DoD systems and CUI under their purview in accordance with references (c) and (d).

DoD Components must ensure solutions meet the requirements in the Attachment prior to procurement, testing, and fielding AMDs and associated systems. Previously approved AMD solutions must be compliant with this guidance within one (1) year following the effective date of this memorandum.

My point of contact for this matter is Ms. Sudha Vyas, sudha.vyas.civ@mail.mil, (703) 614-2332.

Ronald S. Moultrie
Under Secretary of Defense for
Intelligence and Security

John B. Sherman
Chief Information Officer of the
Department of Defense

Attachment:
As stated

DoD CIO Use of Non-Government Owned Mobile Devices – ATTACHMENT

1. Purpose & Scope

This attachment provides technical and programmatic requirements for approving, managing and configuring the use of AMDs to store, process, transmit, or display DoD Controlled Unclassified Information (CUI).

The scope of this guidance is limited to mobile devices with an approved mobile operating system (OS) (e.g., Apple iOS, Android) used to access up to DoD CUI and information technology (IT) authorized to process up to DoD CUI (e.g., IL5 data). DoD personnel, Mission Partners, and Contractors will comply with this guidance when allowing AMDs to store, process, transmit, or display DoD Controlled Unclassified Information (CUI). DoD information not approved for public release, including up to CUI, herein after is referred to as "DoD information."

This attachment is not applicable to personally owned devices and systems in which users will only access their personal information (e.g., health records), DoD information cleared for public release, or publically accessible DoD systems (e.g., https://dodcio.defense.gov/).

The references and other mobile-related issuances are located on the Mobile Collaboration Portal at the link located in 2.b. (6) below.

2. Responsibilities

   a. The DoD CIO will review and approve (or disapprove) exceptions to policy which may be required by Components to enable employment of AMDs in accordance with this guidance.

   b. DoD Components and entities employing AMD capabilities:

      (1) Will receive approval from the Component Senior Information Security Officer (SISO) in collaboration with the Component CUI Senior Agency Official and system Authorization Official (AO), and will consult legal counsel prior to implementing a solution to enable the use of AMDs to access DoD information and IT systems authorized to process up to DoD CUI.

      (2) Will maintain an acceptable endpoint security posture in accordance with references (c) thru (f) of this memorandum while managing risk and balancing user privacy in accordance with this guidance.

      (3) Will ensure compliance with references (c) through (j) to protect DoD information, IT systems and resources, and personnel and the DoD Records Management Program (reference (k)).

      (4) Must have a documented data spillage and mitigation plan, in accordance with reference (f), approved by the Component SISO. Incident response plans and training procedures must be updated to account for AMDs.

(5) Will ensure that an AMD program is voluntary. DoD personnel must not be directed or required to use personally owned devices to conduct official DoD business and DoD personnel will only use AMDs on a voluntary basis.

(6) Will provide updates (e.g., briefings) to the DoD CIO Commercial Mobile Device Working Group (CMDWG) (or relevant DoD CIO level forum) prior to implementation, after implementation, and annually, describing the solution capabilities, cybersecurity risk assessment, penetration testing, user adoption, number of devices and how they connect, device compliance (and non-compliance), and cost benefit analysis. CMDWG information is located at the following Intelink site: https://intelshare.intelink.gov/sites/mobile/default.aspx.

(7) Will request an Exception to Policy (E2P) for AMD capabilities that are not compliant with this memorandum. The E2P portal and resources are located at https://rmfks.osd.mil/dode2p. The E2P team will route exception requests to the appropriate policy office, as needed.

(8) Will develop a user agreement as described in section 3.c. and ensure that each user signs acknowledging they understand the responsibilities of operating an AMD to access DoD information and resources. The user agreement must outline procedures for foreign travel (i.e., AMDs are removed from the program and DoD information is wiped depending on travel location and risk to DoD information, IT resources, and personnel).
   i. Component AOs will maintain a signed user agreement for each user that has access to DoD information, IT, or resources from an AMD.
   ii. Components will have the user sign a new user agreement in the event the agreement is updated, a new device is enrolled in the program, or system capabilities change. Digital signatures and automation is encouraged.

(9) Will conduct semi-annual inventory documenting number of AMDs, number and location of AMDs used with international carriers, and other metrics associated with Office of Management and Budget Integrated Data Collection mobile record.

c. The Defense Information Systems Agency (DISA):

(1) Will develop applicable Security Technical Implementation Guides (STIGs) in collaboration with the National Security Agency (NSA).

d. DoD personnel, Mission Partners, and Contractors authorized to access DoD information and IT resources from AMDs will comply with and adhere to their organizational security, technical, and legal requirements governed by applicable law, policy, and user agreements. Conflicts will be adjudicated through the E2P process in accordance with 2.b. (7).

3. Requirements for AMD Programs

The following requirements must be met prior to enabling access to DoD information and IT resources from AMDs:

a. Enterprise Mobility Management (EMM) System Requirements

(1) Access to DoD information (i.e., CUI), IT, and resources must be managed by an EMM system (e.g., mobile device management (MDM), mobile application management (MAM), mobile content management (MCM), or virtual mobile infrastructure (VMI)).

i. Where applicable, associated applications, often referred as "containers," will be used to segregate personal and DoD data.

(2) The EMM system must be National Information Assurance Partnership (NIAP) validated and configured in accordance with applicable STIGs.

i. Mobile applications incorporated with EMM systems, or used as an MAM or MCM, and used to access, store, process, transmit, or display DoD information must be compliant with reference (g).

NOTE: When a STIG specific to the current OS or solution is not available, legacy STIGs may be applied, as applicable.

(3) The EMM system must be:

i. Configured to manage DoD information, applications, and maintain separation from personal data (e.g., personal apps, personal information) to ensure security and configuration settings of AMDs do not deviate from the approved configuration baseline (hereafter, DoD applications, information, and AMD segment managed by the EMM will be referred to as the "DoD-managed segment of the AMD").

ii. Capable of and configured for autonomous monitoring, compliance, and validation to ensure security and configuration settings of the DoD-managed segment of the AMDs do not deviate from the approved configuration baseline. DoD must only collect information to maintain an acceptable cybersecurity posture to protect DoD information, IT resources, and personnel. Specifically, DoD shall limit information collection of device telemetry in accordance with the requirements in Section 3.c. (User Agreement).

Note: Components must manage and monitor the DoD-managed segment of the AMD. Components have the flexibility to implement management controls based on mission need and capabilities offered and must balance management and monitoring of AMDs with user privacy. All non-DoD information (i.e., personal user data, device information) accessed, collected, monitored, tracked (i.e., location), or maintained must be outlined in the user agreement as stated in 3. c.

iii. Capable of collecting AMD generated logs for the DoD-managed segment of the AMD for analysis of indicators that the AMDs native security controls might have been disabled (e.g., jailbroken/rooted); preventing installation of blocked or prohibited applications or accessing non-approved third-party application stores by or within the DoD-managed segment of the AMD; and detecting if the AMD is running an outdated or unsupported operating system, as applicable. If detected, the EMM system must be configured to disable access to DoD information and IT resources, log events, disable user accounts, or wipe DoD information from the device, as applicable. This detection capability must be implemented prior to AMD enrollment, AMD access to DoD information and IT resources, and continuously monitored on the DoD-managed segment of the AMD enrolled in the program. If non-DoD information (i.e., personal user data, device information) outside the DoD-managed segment of the AMD is required to be accessed, collected, monitored, tracked (i.e., location), or maintained, the circumstances under which this may be done must be outlined in the user agreement as stated in 3.c.(3).

NOTE: The ability to detect compromise or malicious use of an AMD is not guaranteed. Components must balance the risks associated with AMDs with capabilities offered to users, and should document mitigations and risks associated with planned use of AMDs in accordance with the systems' authority to operate. Components must request an E2P, documenting mitigations and risks, when required capabilities are not possible or feasible in accordance with 2.b. (7).

(4) Enrollment and disenrollment of AMDs should leverage self-service portals to the greatest extent possible.

i. Self-service enrollment, once a user obtains approval, must be bound to successful authentication with a Common Access Card (CAC) or approved DoD authenticator (e.g., user authenticates to an EMM self-service portal leveraging their CAC and generates a unique short-lived enrollment code).

b. AMD Requirements

(1) AMDs must be approved by the Component Authorizing Official (AO).

i. Components must only approve devices listed on the NIAP product compliant list or products listed in evaluation at the following links respectfully:
- https://www.niap-ccevs.org/Product/
- https://www.niap-ccevs.org/Product/PINE.cfm

ii. Devices no longer capable of receiving security, software, operating system, or application updates must be removed from the program and access to DoD information and IT resources.

iii. Devices, carriers, and mobile service providers prohibited by law as described by the Department of Commerce Bureau of Industry and Security Entity List must not be enrolled in the program.

(2) The DoD-managed segment of AMDs will only be approved to store, process, transmit, or display information up to DoD CUI, including data stored in IL5 cloud environments within the DoD-managed segment of the AMD.

i. DoD systems and EMM must prevent AMDs from downloading DoD information to unmanaged applications or non-approved storage or application locations (i.e. outside the DoD-managed segment of the AMD).
ii. Enterprise IT, networks, and resources must have security controls in place to limit access from an AMD to backend enterprise resources. Examples of EMM security controls are as follows:
    1. Device access restrictions – Restrict or isolate access based on the devices access type (i.e., from the internet), authentication type (e.g., password), credential strength, etc.
    2. User and device activity monitoring – configured to detect anomalous activity, malicious activity, and unauthorized attempts to access DoD information.
    3. Device health tracking – monitor device attestation, health, and agents reporting compromised applications, connections, intrusions, and/or signatures.

NOTE: If non-DoD information (i.e., personal user data, device information) outside of the DoD-managed segment of the AMD is required to be accessed, collected, monitored, tracked (i.e., location), or maintained, the circumstances under which this may be done must be outlined in the user agreement in accordance with paragraph 3.c.

(3) AMDs that store and use DoD Mobile PKI Credentials must comply with reference (h). Alternative authentication solutions must be approved by the DoD CIO or Components must request and receive and approved E2P through the aforementioned E2P process.

i. Memorandums for approved DoD authentication solutions are located at the following Intelink site: https://intelshare.intelink.gov/sites/dodcioicamdocs/.

(4) AMDs must be configured by the EMM to protect users' privacy in accordance with references (i) and (j).

(5) All DoD data will be removed (e.g., wiped) and the AMD will no longer have access to DoD IT when the user's access is revoked, terminated, or no longer has the need to access DoD information, IT systems, or resources, or when the user reports a registered device as lost, stolen, or showing indicators of compromise.

i. Users' personal information and applications on the device should not be impacted in accordance with references (i) and (j).

ii. Components will develop an efficient process to identify and disconnect user's no longer requiring or authorized access to DoD information and IT resources.

c. User Agreements: User agreements outlining operational requirements, privacy, and user and government responsibilities must be approved by the Component privacy office, in consultation with legal counsel, and signed by the user prior to AMD enrollment in the program. User agreements will, at a minimum:

(1) Include the approved DoD legal consent to monitor notice (excluding personal information) and the user's and government's responsibilities, including but not limited to, wiping of DoD information, confiscation, search and seizure, destruction, and replacement costs if confiscated or destroyed, as applicable.

(2) Will inform the user that use of a personal device as an AMD is voluntary, established for the convenience of the user, and articulate the risks and responsibilities, such as government confiscation, device wipe, or destruction, as applicable in extreme circumstances in the event of a data spill or scanning the device for vulnerabilities to protect DoD information, IT, and resources.

(3) Will include an acknowledgement by the user that enrolling their personal device in an AMD program for access to DoD CUI does not change its status as a non-government owned device, and that it remains subject to any prohibitions and restrictions applied to privately-owned (to include both personally- and commercially-owned) devices.

(4) Will inform the user of the circumstances under which any non-DoD information (i.e., personal user data, device information) outside the DoD-managed segment of AMD may be accessed, collected, monitored, tracked (i.e., location), maintained and used for the benefit of the DoD Component, which may violate the user's privacy rights outlined in reference (j). Specifically, the User Agreement should clearly state what data and device telemetry DoD collects (e.g., browser version, operating system type/version, device name, IP address, and geolocation), along with a notice to the user that if monitoring reveals evidence of unauthorized use or criminal activity, such evidence may be provided to appropriate personnel for administrative, criminal, or other adverse action.

(5) Inform the user that they are responsible for AMD costs and carrier service fees (e.g., data usage, roaming charges) associated with their commercial wireless provider agreement(s) both locally and internationally.

(6) Inform the user of reporting requirements prior to foreign travel. Users will be trained on requirements to safeguard DoD information on AMDs during entry, exit, or checkpoints within foreign countries.

(7) Outline data spillage procedures and user requirements and associated responsibilities.

(8) Include mandatory reporting processes and procedures for the user in the event the AMD is believed to be lost, stolen, operates abnormally, or compromised (e.g.,

virus/malware infection).

(9) Identify mandatory device security controls (e.g., device password, data loss prevention, mobile threat detection, automatic updates of device OS and applications) required on AMDs.

(10) Prohibit user from jailbreaking, rooting, and/or disabling the devices' native security controls and functionality.

(11) Identify appropriate processes and procedures for users who intentionally try to subvert required DoD security controls (e.g., device root/jailbreak), mishandle DoD information, or attempt to or engage in actions that results in an unauthorized disclosure of DoD information.

(12) List approved and prohibited (not approved) external devices that can (or cannot) be plugged into or connected (i.e., Bluetooth) to the AMD (e.g., public USB-port charging station).

(13) Indicate that the user acknowledges they have received training on mobile device security, functionality, and capabilities including specific technologies that enable AMD access to DoD information, IT, and resources. The user must acknowledge they will not store DoD information outside the approved applications or locations on the AMD.

4. Technical Points of Contact

DoD CIO (for IT related inquiries):
Ms. Patricia Janssan, patricia.l.janssan.civ@mail.mil, 571-372-4221
Mr. Will Alberts, william.r.alberts.ctr@mail.mil, 571-372-4727

USD (I&S) (for CUI and OPSEC inquiries):
Mr. Michael Russo, michael.c.russo14.civ@mail.mil, 703-692-7836
Ms. Erica McLennan, erica.s.mclennan.civ@mail.mil, 571-242-0296