



DEPARTMENT OF DEFENSE

6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

OCT 06 2023

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

SUBJECT: Use of Unclassified Mobile Applications in Department of Defense

Mobile applications (apps) are software products designed to function on mobile devices. The misuse and mismanagement of mobile apps poses a cybersecurity and operations security (OPSEC) risk and may result in the unauthorized disclosure of controlled unclassified information (CUI) and unclassified Department of Defense (DoD) information that has not been approved for public release (hereinafter jointly referred to as “non-public DoD information”) and jeopardize operations, strategies, or missions, as described in references (b) and (c). This memorandum provides guidance on the use of mobile apps on unclassified DoD government owned, leased or issued, mobile devices (hereinafter referred to as “government owned mobile devices”) and on the managed partition of non-government owned mobile devices approved in accordance with reference (d) (hereinafter referred to as “Approved Mobile Device” (AMD)).

Numerous mobile apps access or use non-public DoD information (e.g., authorized email apps, collaboration apps, command/control apps). Other applications may be used in support of mission requirements but do not directly access non-public DoD information (e.g., travel and educational apps). Although mobile apps can provide ease of use and increased functionality for users across the Department, there are risks that must be considered. Mobile apps may contain malware or have vulnerabilities that can disclose CUI, personally identifiable information (PII), non-public DoD information not approved for public release, or other sensitive information. This is all possible without the user’s consent or knowledge.

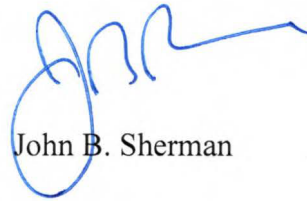
In accordance with DoD Instruction 5200.48, DoD personnel will not use non-DoD accounts or personal e-mail accounts, messaging systems or other non-public DoD information systems, except approved or authorized government contractor systems, to conduct official business involving CUI. In accordance with DoD Instruction 5200.01, DoD personnel will not use unclassified systems, government-issued or otherwise, for classified national security information. DoD CIO will continuously consult with all DoD Components to evaluate risks mobile applications may present to the DoD and update References (m), (n), and (o), as appropriate.

CLEARED
For Open Publication

Oct 11, 2023

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

DoD Components shall ensure proper implementation of the controls outlined in this policy and appendix B. The point of contact for this memorandum is Patricia Janssen,



John B. Sherman

Attachments:

1. References
2. Mobile Application Security Requirements
3. Glossary

Attachment 1: References

- (a) DoD CIO Memorandum, "Mobile Application Security Requirements," October 6, 2017
- (b) DoD Directive 5205.02E, "DoD Operations Security (OPSEC) Program," August 20, 2020
- (c) DoD Memorandum, "Information and Operations Security Risks Posed by Non-Government Websites and Applications," June 22, 2021
- (d) DoD CIO Memorandum, "Use of Non-Government Owned Mobile Devices," August 10, 2022
- (e) DoD Instruction 8500.01, "Cybersecurity," October 7, 2019
- (f) Deputy Secretary of Defense Memorandum, "Use of Geolocation-Capable Devices, Applications, and Services," August 3, 2018
- (g) DoD Instruction 5015.02, "DoD Records Management Program," August 17, 2017
- (h) DoD Instruction 8170.01 "Online Information Management and Electronic Messaging," August 24, 2021
- (i) DoD Directive 5500.7-R, "Joint Ethics Regulation" August 20, 1993
- (j) DoD Instruction 5230.09, "Clearance of DoD Information for Public Release," February 9, 2022
- (k) Deputy Secretary of Defense Memorandum, "Records Management Responsibilities for Text Messages," August 03, 2022
- (l) DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Systems," July 19, 2022
- (m) National Information Assurance Partnership (NIAP), "Requirements for Vetting Mobile Applications from the Protection Profile for Application Software," April 22, 2016
- (n) National Information Assurance Partnership, "Protection Profile for Mobile Device Fundamentals," June 10, 2016
- (o) DoD Instruction 5200.48, "Controlled Unclassified Information (CUI)" March 6, 2020

Attachment 2: Mobile Application Security Requirements

1: Purpose

The purpose of this appendix is to provide direction on the requirements and proper safeguards for use of all mobile applications (apps) on unclassified government-owned devices managed by a Mobility Service Provider and Approved Mobile Devices (AMDs). This guidance will enable the secure use of authorized mission-related mobile apps such as those used for official authorized email and collaboration capabilities, as well as allowing for the use of commercial third-party applications that may be used in support of mission requirements (e.g., travel, e-learning, and traffic/weather). Additionally, this memorandum will replace reference (a).

2: Scope

Applies to all DoD component civilians, military, and supporting contractors and all apps running on unclassified government-owned mobile devices (e.g., smartphones or tablet devices) and AMDs approved in accordance with reference (d). Devices within this scope will utilize only Mobile Operating Systems (OS), such as iOS and Android. Mobile code (e.g., web applications) and apps on traditional desktop operating systems are beyond the scope of this appendix.

3: Application Categories

Mobile apps are grouped into two categories (managed and unmanaged) as defined below. Apps from either category installed on government owned mobile devices or AMDs must comply with the requirements in the “Application Security Requirements” section. The configuration of AMDs authorized for DoD use must be compliant with reference (d).

- **Managed apps** are defined as mobile device applications controlled by an Enterprise Management System (e.g., Mobile Device Management (MDM), Enterprise Mobility Management (EMM), Mobile Application Management (MAM)). Managed apps on government owned mobile devices or AMDs may access, transmit, store, or process DoD information up to Controlled Unclassified Information (CUI). An Enterprise Management System can enforce controls on the application and data in a way that can reduce the risk of data compromise or exposure/spillage of data to unmanaged applications.
- **Unmanaged apps** are defined as mobile device applications that are **NOT** controlled and installed by an Enterprise Management System. Unmanaged apps are **NOT** authorized to access, transmit, store, or process non-public DoD information. These apps, which are often for personal use, include, but are not limited to, travel functions (e.g., hotels, airlines, rental cars), e-learning, non-mission related communications and non-DoD controlled messaging systems, social media, fitness, and geolocation tracking apps (e.g., maps, location service apps).

Organizational Definitions Used in this Document

- ***Mobility Service Providers*** are DoD organizations who provide an offering that enables the use of mobile devices to securely access DoD systems, applications, and data. Mobility Service Providers in this context should not be confused with commercial providers/carriers who provide mobile devices and networks such as AT&T, Sprint, and Verizon.
- ***Components*** as used in this memorandum refer to organizations who are obtaining unclassified mobile device services and capabilities from a Mobility Service Provider. A Component may also be serving as their own Mobility Service Provider.

4: Application Security Requirements

1. Managed apps must be evaluated under National Information Assurance Partnership (NIAP), “Requirements for Vetting Mobile Applications from the Protection Profile for Application Software,” April 22, 2016, in accordance with references (e) and (n) and must be approved by the Component’s Authorizing Official (AO) for organizational use.
2. Managed applications shall be used only on devices that have been validated as compliant with the Mobile Device Fundamentals Protection Profile (MDFPP).
3. Managed IA-Enabled apps (e.g., “Secure containers,” virtual private network (VPN) clients, virtual clients) require the Component AO and Mobility Service Provider to take appropriate security actions in accordance with DoD policy.
4. The use of a government-owned mobile device or AMD, and all apps on a government owned mobile device or AMD, must be “for official use and authorized purposes only” as defined in Section 3, 2-301 of reference (i).
5. All apps that access, transmit, store, or process non-public DoD information must comply with the DoD Records Management Program, in accordance with references (g), (h) and (k). Any DoD record created or received on any government owned mobile device or AMD and not captured in a DoD records system must be transferred to a DoD records system within 20 days of creation or receipt. Users of mobile apps, in addition to DoD Components and Mobility Service Providers who provide government mobile devices, are responsible for ensuring compliance.
6. The use of managed or unmanaged apps and devices with geolocation capabilities will be in accordance with reference (f), including the prohibitions related to such use in operational areas.
7. Acquisition of or within unmanaged applications is the responsibility of the user and shall not obligate the federal government for unapproved or unallowed expenses, subscriptions, or dues unless authorized. Personal use of mobile applications shall comply with reference (i). Additionally, users cannot be required to acquire unmanaged

applications that incur personal cost.

8. Unmanaged apps are **prohibited** from accessing, transmitting, storing, or processing non-public DoD information, including CUI, in accordance with DoD Instruction 5200.48.
9. Unmanaged applications shall be permitted only on mobile devices capable of segregating unmanaged and managed applications and data contained therein. AMDs that do not support this capability are **NOT** authorized to access, transmit, store, or process non-public DoD information.
10. Unmanaged 'messaging apps,' including any app with a chat feature, regardless of the primary function, are NOT authorized to access, transmit, process non-public DoD information. This includes but is not limited to messaging, gaming, and social media apps. (i.e., iMessage, WhatsApps, Signal). An Exception to Policy (E2P) request must be submitted by the appropriate Component for use of an unmanaged messaging app that is critical to fulfilling mission operations at <https://rmfks.osd.mil/dode2p>.
11. Mobility Service Providers have the option to use whitelisting for authorized unmanaged apps (e.g., only allowing an explicitly defined set of apps to be used on a mobile device) or restricting installation for prohibited unmanaged apps (e.g., prohibiting the execution of explicitly defined applications).
12. Each Component is responsible for establishing and communicating its policy regarding acceptable use of unmanaged apps in accordance with the restrictions in this memorandum.
13. On government owned mobile devices, DoD Mobility Service Providers must prohibit the installation and use of apps from app stores that are not native to the operating system (i.e., 3rd party app stores) or controlled by the Government.
14. Mobility Service Providers must adhere to all DoD orders and US Government Directives that direct actions restricting the use of specific apps on government owned mobile devices and AMDs, and where possible, prohibit internet traffic and access to prohibited sites that pose a risk to non-public DoD information.
15. In conjunction with their Mobility Service Provider, Components are responsible for ensuring appropriate user agreements are signed. Components will monitor user compliance with policy and user agreements, and appropriately enforce compliance.
16. The DoD CIO will establish a process to develop and maintain a list of unauthorized apps that are prohibited for installation and/or use on government owned mobile devices. DoD Mobility Service Providers must establish a process to prohibit the installation and/or use of prohibited apps, and/or enforce an action to restrict a device not compliant with DoD policy from accessing non-public DoD information.
17. Within one year of the date of signature of this memorandum, all Mobility Service Providers must implement an enterprise mobile security solution for all mobile devices, herein referred to as Mobile Threat Defense (MTD), that has the following requirements

at a minimum:

- Detection of mobile threats to the mobile operating system and device.
- Ability to continuously scan mobile devices for suspicious activity (e.g., malicious apps, man in the middle attacks).
- Enforce a restrictive or corrective action against mobile devices that are out of compliance.

18. DoD Components must update user agreements and training to include:

- Operations security concerns introduced by using unmanaged apps.
- Outline unacceptable application categories (e.g., pornography, gambling, gaming) that should not be downloaded to DoD mobile devices.
- Clarify user responsibilities and restrictions when using unmanaged and managed apps.
- Defines consequences for not complying with user agreement.
- Notify users that Mobility Service Providers will monitor and enforce noncompliance.
- Prohibition of the use of unmanaged apps for non-public DoD information.

19. Components must receive a DoD CIO-executed Exception to Policy (E2P) based on a stated mission requirement to use any mobile app 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.

5: Application Updates

1. DoD Component AOs have the latitude to determine their re-evaluation frequency in accordance with Reference (1) for managed applications. These procedures must include the requirements for reevaluation at a minimum of once annually.
2. Mobile Application updates occur frequently. DoD Component AOs should consider the available (existing) results and make a risk determination based on the age of the evaluation results and changes to the application since the evaluation. Retesting of only critical areas is acceptable in this instance.
3. Managed applications that are no longer supported by the developer, have been deemed end of life, or do not pass re-evaluation must be removed from all mobile devices.

Attachment 3: Glossary

1. **Approved Mobile Device” (AMD)** - The managed partition of non-government owned mobile devices approved in accordance with reference (d) DoD CIO Memorandum, “Use of Non-Government Owned Mobile Devices,” August 10, 2022.
2. **Malware** - Software designed to cause disruption to information technology or gain unauthorized access to information and systems.
3. **Managed apps** - Mobile device applications controlled by an Enterprise Management System (e.g., Mobile Device Management (MDM), Enterprise Mobility Management (EMM), Mobile Application Management (MAM)). Managed apps on unclassified mobile devices may access, transmit, store, or process DoD information up to Controlled Unclassified Information (CUI). Enterprise Management System can enforce controls on the application and data in a way that can reduce the risk of data compromise or exposure/spillage of data to unmanaged applications.
4. **Unmanaged apps** - Mobile device applications that are NOT controlled and installed by an Enterprise Management System. Unmanaged apps are NOT authorized to access, transmit, store, or process non-public DoD information. These apps, which are often for personal use, include, but are not limited to, travel functions (e.g., hotels, airlines, rental cars), e-learning, non-mission related communications and non-DoD controlled messaging systems, social media, fitness, and geolocation tracking apps (e.g., maps, location service apps).
5. **Mobility Service Providers** - Mobility Service Providers are DoD organizations who provide an offering that enables the use of mobile devices to securely access DoD systems, applications, and data. Mobility Service Providers in this context should not be confused with commercial providers/carriers who provide mobile devices and networks such as AT&T, Sprint, and Verizon.
6. **Components** - Components as used in this memorandum refer to organizations who are obtaining unclassified mobile device services and capabilities from a Mobility Service Provider. A Component may also be serving as their own Mobility Service Provider.
7. **Enterprise Management System** – A software solution that provides management of information technology across the organization.
8. **Mobile Device Management (MDM)** - The administration of mobile devices such as smartphones, tablets, computers, laptops, and desktop computers.
9. **Enterprise Mobility Management (EMM)** - A suite of services and processes to secure and manage mobile devices and information on mobile devices regardless of the device’s ownership.
10. **Mobile Application Management (MAM)** – Secure management of applications on mobile devices.

11. **Non-public DoD Information** - Department of Defense information that has not been approved for public release.
12. **Government-Owned Devices** - Unclassified DoD government owned, leased or issued, mobile devices.