

UNCLASSIFIED



GOOGLE ANDROID 14 BYOAD SUPPLEMENTAL PROCEDURES

13 March 2024

Developed by Google and DISA for the DOD

UNCLASSIFIED

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by the Defense Information Systems Agency (DISA) of any nonfederal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

	Page
1. REFERENCES	1
2. BYOAD DEPLOYMENT	2
2.1 Google Android BYOD Deployment.....	2
2.2 BYOAD Requirements.....	2
2.3 Conflicting Policy Guidance	3
2.5 Key BYOAD Operational Considerations	4
2.5.1 Operational Environment Risk.....	4
2.5.2 Additional Considerations.....	4

1. REFERENCES

- a. DOD CIO policy memorandum, “Use of Non-Government Owned Mobile Devices”, Aug 10, 2022
- b. Draft NIST SP 1800-22, Mobile Device Security: Bring Your Own Device (BYOD), Nov 2022

2. BYOAD DEPLOYMENT

2.1 Google Android BYOD Deployment

The Android Enterprise (AE) Bring Your Own Device (BYOD) deployment mode is called “work profile for employee-owned devices (BYOD)”. When using this deployment mode, a separate self-contained work profile will be installed on the mobile device to protect work data and apps from personal data and apps. The enterprise has complete control and visibility over the work profile but no visibility or access to the device’s personal profile.

2.2 BYOAD Requirements

Reference 1.a establishes minimum requirements for the use of nongovernment-owned mobile devices (i.e., personal- or corporate-owned; referred to as Bring Your Own Approved Device [BYOAD] in this STIG), to store, process, transmit, or display up to DOD Controlled Unclassified Information (CUI). The memorandum provides technical and policy controls that must be implemented for all BYOAD devices deployed in the DOD. Reference 1.b provides best practice requirements for deploying BYOD devices in the U.S. federal government.

This STIG provides required technical controls and key policy controls included in both references. The Authorizing Official (AO) is responsible for ensuring required policy controls are implemented before the deployment of BYOAD devices. The following list includes key policy requirements included in both references (see both references for a complete list):

- Approval must be received from Component CISO, AO, and legal counsel prior to implementation of BYOAD. (Reference 1.a, paragraph 2.b.(1)).
- Exception to Policy (E2P) for noncompliant systems must be requested. (Reference 1.a, paragraph 2.b.(7)).
- BYOAD users must sign a User Agreement. (Reference 1.a, paragraphs 2.b.(8) and 3.c).
- BYOAD device must be National Information Assurance Partnership (NIAP) validated (e.g., listed on the DOD Approved Products List). (Reference 1.a, paragraph 3.a.(2)).
- The Enterprise Mobility Management (EMM) system (i.e., mobile device management [MDM], mobile application management [MAM], or virtual mobile infrastructure [VMI]) must be NIAP validated. (Reference 1.a, paragraph 3.a.(2)).
- All apps on BYOAD device that access, store, process, transmit, or display DOD information must comply with DOD Chief Information Officer Memorandum, “Mobile Application Security Requirements,” October 6, 2017. (Reference 1.a, paragraph 3.a.(2)i).
- Devices, carrier, 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. (Reference 1.a, paragraph 3.b.(1)iii).
- Component must list what is being monitored, managed, and data collected on AMDs¹ in the user agreement. (Reference 1.a, paragraph 3.a.(3)ii).

¹ Approved Mobile Device (AMD) is the term used in the DOD policy (reference 1.a) for BYOAD (AMD = BYOAD)

- Participation in the DOD BYOAD program is voluntary. (Reference 1.a, paragraph 3.c.(2)).
- Organizations must provide a series of how-to guides, step-by-step instructions covering the initial setup (installation or provisioning), and configuration for each component of the architecture to help security and privacy engineers rapidly deploy and evaluate a mobile device solution in their environment. (Reference 1.b, paragraph 1.2).
- Organizations must provide users with access to protected business resources (managed or work profile apps) (e.g., SharePoint, knowledge base, internal wikis, application data). (Reference 1.b, paragraph 1.2).

2.3 Conflicting Policy Guidance

Reference 1.a contains conflicting policy requirements regarding BYOAD monitoring and protecting user privacy:

- Monitoring requirements:
 - The EMM system must be 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 nonapproved 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. (Paragraph 3.a.(3)iii).
- Protect user's privacy requirements:
 - Mobile devices must be configured by the EMM to protect users' privacy. (Paragraph 3.b.(4)).

It is impossible to meet all mobile device monitoring requirements listed in Reference 1.a without compromising user privacy. For example, the owner of the device may need to allow the installation of an agent or third-party monitoring app in the personal space to meet device monitoring requirements, which violates user privacy requirements.

Reference 1.a recognizes the conflict between device monitoring and user privacy:

- DOD Components will maintain an acceptable endpoint security posture while managing risk and balancing user privacy in accordance with this guidance. (Paragraph 2.b.(2)).

The STIG's position on device monitoring vs. user privacy is device monitoring controls will only be implemented to the extent possible without violating user privacy requirements, unless the AO has determined, based on mission needs and operational environment risk, device monitoring controls must take precedence.

2.5 Key BYOAD Operational Considerations

2.5.1 Operational Environment Risk

BYOAD is not appropriate for all operational environments. The DOD site and AO should evaluate the risk of BYOAD devices in their operational environment before approving BYOAD use. Key considerations include:

- Environments where microphone and camera must be disabled or where the use of personal devices is prohibited.
- Environments where location-based services cause an unacceptable OPSEC risk.
- Sites where the EMM system cannot support all STIG required controls.

2.5.2 Additional Considerations

- The Android Cross-profile calendar setting allows a single calendar view of the personal profile and work profile calendars without sharing calendar information between profiles. This setting is disabled by default. DOD sites might consider enabling this setting as a user convenience. The setting can be enabled by specifying allowed calendar apps from the personal side.
 - To enable this feature:
 - Set the Cross-profile calendar setting in the MDM. This API allows the work profile calendar to request access to the user calendar data to be displayed. It is also possible to restrict this to only specific apps in the work profile (such as the preferred calendar app, referenced by the package name).
 - Once the policy has been pushed to the device, the user must authorize the shared display. The Google Calendar app will automatically ask the user for this the first time it is launched after this is enabled, but it can be done at any point. The user can choose to set this by going to Settings >> Security & privacy >> More privacy settings >> Connected work & personal apps and selecting Calendar. This will enable or disable the feature for the user.
- Android provides “Onelock” as a capability to minimize the number of authentication prompts for a user on the device. When Onelock is enabled, the user is automatically logged into the work profile when they successfully login to the device. This allows the user to immediately access any work profile apps without an additional authentication prompt. This setting is disabled by default. DOD sites might consider enabling this setting as a user convenience.
 - To enable this feature:
 - Set the “Require separate challenge” control in the MDM (disable the API `DISALLOW_UNIFIED_PASSWORD`).
 - Once the policy has been pushed to the device, the user must enable the setting on the device. The user can choose to set this by going to Settings >> Security & privacy >> More security settings and enabling “Use Onelock”. This will enable or disable the feature for the user.