APPLE IOS/IPADOS 16
BRING YOUR OWN APPROVED DEVICE (BYOAD)
SUPPLEMENTAL PROCEDURES

17 August 2023

Developed by Apple and DISA for the DOD

Trademark Information

TABLE OF CONTENTS

1. REFERENCES

This Supplemental Procedures document refers to the following as "1.a" and "1.b":

a. DOD CIO Policy Memorandum, "Use of Non-Government Owned Mobile Devices", August 10, 2022.
b. Draft NIST SP 1800-22, "Mobile Device Security: Bring Your Own Device (BYOD)", November 2022.

2. BYOAD DEPLOYMENT

2.1 Device Enrollment vs. User Enrollment[1]

User Enrollment (UE) is Apple's standard enrollment mode for enterprise deployment of personally owned devices. The use of UE is problematic for most DOD sites for several reasons:

- UE requires the enterprise assign a managed Apple ID to each enrolled device. The only way to assign managed Apple IDs at scale is via a federated directory service. The public version of Azure Active Directory (AAD) meets this requirement, but the government version of AAD used in the DOD does not.
- UE assumes AD user authentication is configured for username/password. The DOD's standard implementation of AAD uses smart card authentication.

Therefore, the majority of DOD sites deploying personally owned iOS/iPadOS devices will use Device Enrollment[2] (DE) since Automated Device Enrollment (ADE) is not suitable for personally owned mobile devices.

Note: DOD sites deploying UE are primarily training and education organizations, which have not deployed DOD AAD.

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 the references (refer to both references for a complete list):

- Approval must be received from Component Senior Information Security Officer (SISO), 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.*
- The 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).*

[1] Refer to https://support.apple.com/en-gb/guide/deployment/dep23db2037d/web for a description of iOS enrollment types.
[2] Also called Manual Enrollment.

- The Enterprise Mobility Management (EMM) system (i.e., mobile device management [MDM], mobile application management [MAM], virtual mobile infrastructure [VMI]) must be NIAP validated. *Reference 1.a, paragraph 3.a.(2).*
- All apps on the 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.*
- The Component must list what is being monitored, managed, and data collected on AMDs[3] in the user agreement. *Reference 1.a, paragraph 3.a.(3)ii.*
- 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, section 1.2.*
- Organizations must provide users with access to protected business resources (managed or work profile apps), such as SharePoint, knowledge base, internal wikis, or application data. *Reference 1.b, section 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 AMD's 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.

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

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).*

This STIG takes the following position on device monitoring versus user privacy: 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, that device monitoring controls must take precedence.

2.4 Key BYOAD Operational Considerations

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 operational security (OPSEC) risk.
- Sites where the EMM system cannot support all STIG-required controls.