APPLE VISIONOS 26
SUPPLEMENTAL PROCEDURES

26 February 2026

Developed by Apple and DISA for the DOD

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. MOBILE DEVICE PROCEDURES 1
1.1 Federal Information Processing Standard (FIPS) 140-3 1
1.2 Antivirus Software 1
1.3 Software Updates 1
1.4 Configuration of Unmanaged Apps 1
1.5 DOD PKI Purebred 2
2. APPLE INTELLIGENCE INFORMATION 3
3. APPLE VISIONOS TERMINOLOGY AND BEST PRACTICES 5
3.1 Apps 5
3.1.1 Apple App Store 5
3.1.2 Managed Apps 5
3.1.3 Enterprise Apps 5
4. OPERATIONAL CONSIDERATIONS 7
4.1 Deprovisioning 7

1. MOBILE DEVICE PROCEDURES

1.1 Federal Information Processing Standard (FIPS) 140-3

FIPS 140-3 validation for Apple visionOS 26 cryptographic modules is in process.

For DOD organizations using visionOS 26 devices, visit the following website for updates on the validation status: https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Validated-Modules/Search.

In-process modules can be found at https://csrc.nist.gov/Projects/cryptographic-module-validation-program/modules-in-process/Modules-In-Process-List.

1.2 Antivirus Software

Apple visionOS devices do not require antivirus software. visionOS devices meet the virus protection requirement of DODI 8500.01 with a combination of security policies, application sandboxing, app containers, and code signing. These technologies help contain malware and control the ability to self-install on an Apple visionOS device to gain access to applications and data, device resources, and DOD networks.

1.3 Software Updates

Keeping visionOS up to date ensures the latest enhancements and security controls are in place. visionOS is signed and activated by Apple for each device to ensure integrity. This STIG requires that all updates come from an approved source. Apple is considered a DOD-approved source. Apple-provided updates must be installed on Apple iPhones and iPads when available. Apple provides the capability for DOD mobile service providers to test most updates before release via the AppleSeed program.

1.4 Configuration of Unmanaged Apps

Section 1.1 of the Overview document states that the scope of this STIG includes the Corporate Owned Personally Enabled (COPE) use case, where both managed and unmanaged apps are supported.

DOD mobile service providers may allow the user full access to the Apple App Store for downloading unmanaged (personal) apps and syncing personal data on the device with personal cloud data storage accounts when all the following conditions have been met:

- The site's authorizing official (AO) has approved full access to the Apple App Store, including downloading and installing unmanaged apps onto the visionOS device and syncing personal data on the device with personal cloud data storage accounts[1]. Written approval must be available for any system compliance review.

[1] It is recommended that the AO provide guidance on types of apps that should be avoided in the Apple App Store due to known risky functions or behaviors.

- The site AO has provided guidance on acceptable use and restrictions, if any, on downloading and installing personal apps and data (music, photos, etc.). Guidance can be added to the user training or the User Agreement.
- Site mobile devices are configured with a work-only container technology or application that is certified by the National Information Assurance Partnership (NIAP). Currently, NIAP has not developed a process for performing Common Criteria evaluations for spatial computing operating systems such as visionOS; therefore, this requirement is not applicable.
- The site Mobile Device Management (MDM) is configured to restrict the download of apps from all third-party app stores.
- Site mobile device users receive training on known Apple App Store application risks and STIG controls that must be enabled by the user (User-Based Enforcement)[2]. Refer to STIG requirement AVOS-26-011900 for more information.

1.5 DOD PKI Purebred

Purebred is a key management server and set of apps for mobile devices that provides a secure, scalable method of distributing software certificates for DOD PKI subscriber use on commercial mobile devices.

Requirements for Apple visionOS devices credentialed using DOD PKI Purebred are as follows:

- The Purebred Registration app must be installed as a managed app on visionOS devices via enterprise management, and the "Allow documents from managed sources in unmanaged destinations" restriction must be enforced by the policy to limit apps that can leverage key sharing.
- Users are responsible for maintaining positive control of their credentialed devices. The DOD PKI certificate policy requires subscribers to maintain positive control of the devices that contain private keys and report any loss of control so the credentials can be revoked.
- Upon device retirement, turn-in, or reassignment, ensure a factory data reset is performed prior to device handoff. Follow procedures in the Deprovisioning section and any other procedures defined by the DOD Management Service Provider.

More information is available at https://cyber.mil/pki-pke/.

[2] UBE controls cannot be managed by the site MDM server; therefore, must be managed by the mobile device user.

2. APPLE INTELLIGENCE INFORMATION

Apple Intelligence is Apple's implementation of artificial intelligence (AI) within the Apple ecosystem. Apple Intelligence uses generative AI to help users work, communicate, and express themselves. Apple Intelligence is built into iOS 18, iPadOS 18, macOS Sequoia, and visionOS 2 and later and is found in many Apple apps, including Writing tools, notifications, Mail, and Siri.

Apple Intelligence tasks are processed either on device or on Apple servers in the cloud in a private, Apple-managed area called Private Cloud Compute (PCC). Whether the Apple Intelligence request is processed on device or by PCC depends on the processing needs of the Apple Intelligence request. Apple Intelligence will support supplemental third-party AI services, with ChatGPT being the first one supported (late 2024). **The STIG requires that Apple Intelligence supplemental third-party AI services be disabled (refer to requirement AVOS-26-015400).**

As previously stated, Apple Intelligence is fully integrated into iOS, iPadOS, macOS, visionOS, and many Apple apps. The Enterprise cannot disable processing DOD data in the Apple PCC via an MDM server but can disable many individual Apple Intelligence tools via the MDM. In addition, the user can disable Apple Intelligence on the device.

Apple has released a PCC security guide that describes details of the security infrastructure Apple used when setting up PCC. The Private Cloud Compute Security Guide can be found at https://security.apple.com/documentation/private-cloud-compute. Some highlights of PCC security include:

- Stateless computation on personal user data:
  - A user's device sends data to PCC for the sole, exclusive purpose of fulfilling the user's inference request. PCC uses that data only to perform the operations requested by the user.
  - User data is encrypted directly to the PCC nodes that are processing the request, and the decrypted user data is retained only until the response is returned.
  - User data is never available to Apple, even to staff with administrative access to the production service or hardware.
  - End-to-end encryption is used between the mobile device and PCC.
  - The root of trust for PCC is Apple's compute node: custom-built server hardware that brings the power and security of Apple Silicon to the data center, with the same hardware security technologies used in iPhone, including the Secure Enclave and Secure Boot.
- Enforceable guarantees: PCC does not depend on external components for its core security and privacy guarantees.
  - The Secure Enclave randomizes the data volume's encryption keys on every reboot and does not persist these random keys, ensuring data written to the data volume cannot be retained across reboot.
- No privileged runtime access: PCC does not contain privileged interfaces that would enable Apple's site reliability staff to bypass PCC privacy guarantees, even when working to resolve an outage or other severe incident.

- Nontargetability: An attacker cannot attempt to compromise personal data that belongs to specific, targeted PCC users without attempting a broad compromise of the entire PCC system.
  - Technologies such as Pointer Authentication Codes and sandboxing act to resist such exploitation and limit an attacker's horizontal movement within the PCC node.
- Verifiable transparency: Apple will provide access to PCC to security researchers so they can verify, with a high degree of confidence, that Apple's privacy and security guarantees for Private Cloud Compute match their public promises.

3. APPLE VISIONOS TERMINOLOGY AND BEST PRACTICES

This section outlines best practices and recommendations for visionOS 26.

3.1 Apps

3.1.1 Apple App Store

The App Store is an application distribution platform for visionOS apps. Apps in the App Store are reviewed by Apple and digitally signed for use on Vision Pro. Because not all applications in the App Store are appropriate for use on GFE, DOD organizations must establish approval processes to determine which applications are permitted. DOD Chief Information Officer Memorandum "Mobile Application Security Requirements," 06 October 2017, provides guidance on app vetting/reviewing requirements for both management (work) and unmanaged (personal) apps.

Applications purchased with an Apple account are available to other Apple devices configured with the same Apple account. Previously purchased applications will not automatically download on a new device when an existing Apple account is associated with it. Users are discouraged from synchronizing applications across personally owned and government-furnished Apple Vision Pros. To prevent applications acquired for personal use from automatically downloading on government-furnished Vision Pros, the user must turn off **Apps** under **Automatic Downloads** in the **App Store** section of the **Settings** app on the Apple device.

3.1.2 Managed Apps

Managed apps are installed through an MDM. After installation, the MDM server can enforce additional restrictions on these apps. Apps that store DOD data must be managed via an MDM where possible. Managed apps give DOD organizations the ability to keep DOD documents contained within managed apps and prevent non-DOD documents from being opened in managed apps. Managed apps are subject to MDM control for:

- Use of iCloud document storage.
- Ability to back up application data via USB and iCloud.
- Per-app VPN.
- Single sign-on.
- App configuration.
- Removal on MDM unenrollment.

3.1.3 Enterprise Apps

Enterprise (or in-house) apps are visionOS apps developed for internal deployment within an organization. Enterprise apps are not reviewed by Apple and are deployed outside of the Apple App Store. Enterprise apps must be vetted and approved before installation on Apple devices. Enterprise apps can be deployed using MDM, Apple Configurator, email, or a web server. Deploying enterprise apps via MDM will designate them as managed apps and permit them to have access to DOD documents.

Custom Apps (previously known as B2B apps) are developed by organizations for internal use but distributed via the Apple App Store. Custom apps are reviewed by Apple (similar to consumer apps) but are not available without being explicitly assigned to the organization's Apps and Books account. These apps are not searchable on the app store. Custom apps can be made available to mission partners and other services within the guidelines of the Apple Custom App distribution agreement. Apps developed by one service can be shared with another service without having to transfer the App's source code. These apps can be distributed via an MDM and can also be managed.

4. OPERATIONAL CONSIDERATIONS

4.1 Deprovisioning

A deprovisioning process is required for Apple visionOS devices at end of life or when an employee transitions to another role. Deprovisioning is the act of unenrolling a device from management, deleting the current user's accounts, and wiping all data from the device.

The Apple feature Activation Lock makes it difficult for anyone to use or sell an Apple visionOS device that has been lost or stolen. Activation Lock is enabled by signing in to iCloud on a device. As part of the deprovisioning process, the end user must remove the iCloud account or turn off Activation Lock from the device. This can also be accomplished by selecting **Erase All Content and Settings** from within the **Settings** application on the device and completing a device wipe.