APPLE VISIONOS 26
SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

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. INTRODUCTION 1

1.1 Executive Summary 1
1.2 Authority 2
1.3 Vulnerability Severity Category Code Definitions 2
1.4 STIG Distribution 2
1.5 MDFPP Compliance Reporting 3
1.6 Document Revisions 3
1.7 Other Considerations 3
1.8 Product Approval Disclaimer 3

LIST OF TABLES

Page

Table 1-1: Vulnerability Severity Category Code Definitions 2

1. INTRODUCTION

1.1 Executive Summary

The Apple visionOS 26 Security Technical Implementation Guide (STIG) provides the technical security policies, requirements, and implementation details for applying security concepts to Apple devices running visionOS 26 that process, store, or transmit unclassified data marked as Controlled Unclassified Information (CUI) or below. The STIG is based on the Protection Profile for Mobile Device Fundamentals (MDFPP) version 3.3 STIG Template. Requirements compliance is achieved by leveraging a combination of configuration profiles, user-based enforcement (UBE), and reporting.

Note: This STIG requires Vision Pro users to be trained to not implement the Vision Pro Developer Mode or Guest User mode and to not install and use the Vision Pro developer strap. These use prohibitions should be added to the Vision Pro User Agreement.

The scope of this STIG covers only the Corporate Owned Personally Enabled (COPE) and Corporate Owned Business Only (COBO)[1] use cases.

The configuration requirements and controls implemented by this STIG allow the user unrestricted activity in downloading and installing personal (unmanaged) apps and data (music, photos, etc.) with authorizing official (AO) approval and within any restrictions imposed by the AO.

Note: If the AO has approved the use/storage of DOD data in one or more personal (unmanaged) apps, allowing unrestricted user activity in downloading and installing personal (unmanaged) apps on the Vision Pro device may not be warranted due to the risk of possible loss of or unauthorized access to DOD data.

This STIG assumes that if a DOD Wi-Fi network allows a Vision Pro device to connect to a DOD network, the Wi-Fi network complies with the Network Infrastructure STIG; for example, wireless access points and bridges must not be connected directly to the enclave network.

Supervision of visionOS, which provides the administrator more control of a Vision Pro device than is available for an unsupervised device, is required for all DOD Vision Pro deployments. Supervised mode is intended for institutionally owned devices. Supervised mode provides the DOD more control over managed visionOS by providing access to additional device management controls, including disabling a user from modifying installed accounts, removing the management profile (MDM profile), accessing the Apple App Store, and installing new versions of visionOS.

A device can be supervised using one of two methods: It can be enrolled in Apple's Automated Device Enrollment/Apple Business Management (ABM) and supervised during the activation of the device, or a Vision Pro can be placed in supervised mode by using the Apple Configurator (AC2) tool. Automated Device Enrollment registration of a Vision Pro can occur if the device is purchased directly from Apple (Apple Government Team or Apple's Retail Business Team), an Apple authorized reseller, or manually via AC2. The DOD procurement office must provide the third-

[1] Work data/apps only – no personal data/apps.

party reseller with the agency's ABM customer number, which can be obtained by applying at http://deploy.apple.com as a business.

1.2 Authority

Department of Defense Instruction (DODI) 8500.01 requires that "all IT [information technology] that receives, processes, stores, displays, or transmits DOD information will be […] configured […] consistent with applicable DOD cybersecurity policies, standards, and architectures." The instruction tasks that DISA "develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DOD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS [National Security Agency/Central Security Service], using input from stakeholders, and using automation whenever possible." This document is provided under the authority of DODI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provides an environment that contributes to the security requirements of DOD systems, applicable NIST SP 800-53 cybersecurity controls must be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

Category	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will **directly and immediately** result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity.

1.4 STIG Distribution

Parties within the DOD and federal government's computing environments can obtain the applicable STIG from the DOD Cyber Exchange website at https://cyber.mil/. This site contains the latest copies of STIGs, SRGs, and other related security information. Those without a Common Access Card (CAC) that has DOD Certificates can obtain the STIG from https://public.cyber.mil/.

1.5 MDFPP Compliance Reporting

All Mobile Device Fundamentals Protection Profile (MDFPP) and DOD Annex security functional requirements (SFRs) were considered while developing this STIG. In DOD environments, devices must implement SFRs as specified in the DOD Annex to the MDFPP.

Requirements that are applicable and configurable are included in this STIG.

1.6 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DOD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

1.7 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible AO. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided for the DOD. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied at both the device hardening level and the architectural level due to the fact that some settings may not be configurable in environments outside the DOD architecture.

1.8 Product Approval Disclaimer

STIGs provide configurable operational security guidance for products being used by the DOD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with cybersecurity controls/control enhancements, which supports system assessment and authorization (A&A) under the DOD Risk Management Framework (RMF). Department of Defense AOs may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect the vendor's proprietary information.

AOs have the purview to determine product use/approval in accordance with (IAW) DOD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (https://www.niap-ccevs.org/) IAW CNSSP #11.
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (https://csrc.nist.gov/groups/STM/cmvp/) IAW federal/DOD mandated standards.