carahsoft

Lookout™

DoW STIGs and NIST Recommendations for Mobile Platforms

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through GSA, NASA SEWP V, ITES-SW2 and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with Lookout, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.

To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com

Explore More Resources:
carah.io/LookoutResources

Join Events & Webinars:
carah.io/LookoutEvents

Discover Technology Solutions:
carah.io/Lookout

Learn About Procurement:
carah.io/LookoutContracts

Connect With Our Team:
Lookout@carahsoft.com
(844) 445-5688

DoW STIGs and NIST Recommendations for Mobile Platforms

Lookout

The Mandate for Absolute Mobile Security: Beyond Compliance—The Zero-Trust

The proliferation of mobile platforms—including iOS, Android, and their specialized enterprise derivatives—has fundamentally redrawn the perimeter of the Department of War (DoW) and Federal enterprise. This transition has introduced not merely a risk, but an **existential attack surface** that requires a commensurate level of defense. Compliance with the Security Technical Implementation Guides (STIGs) is therefore not a discretionary best practice; it is the **non-negotiable minimum baseline** for securing an Authorization to Operate (ATO). Failure to implement and continuously enforce these mandated controls is a form of institutional negligence that directly compromises national security interests.

Compliance is fundamentally not a passive, static checklist exercise. It is the **active, continuous, and dynamic application of these controls** throughout the device's lifecycle to ensure the operational resilience and security posture of DoD systems against increasingly sophisticated, nation-state-level Advanced Persistent Threats (APTs).iOS Security: STIG V-276214 is the Hard Line in Zero-Trust

The DISA **Apple iOS/iPadOS 18 STIG** makes the requirement for Mobile Threat Detection absolute and unambiguous. The Medium Severity finding **V-276214—DOD Apple iOS/iPadOS 18 devices must have a Mobile Threat Detection (MTD) app installed**—establishes the operational threshold for acceptable risk in the mobile environment.

This finding is not a recommendation; it is an immediate, mandatory requirement. Without an approved MTD solution installed, actively reporting its health and threat posture, and integrated bi-directionally with the MDM platform:

1. **The Device Is Operating Blind:** The endpoint is rendered fundamentally incapable of detecting sophisticated, fileless malware, zero-day exploits, unauthorized network man-in-the-middle (MITM) attacks, or critical device integrity compromises like rooting or jailbreaking. This constitutes an immediate and unacceptable risk.
2. **The Organization Is in a State of Non-Compliance:** This failure directly violates the STIG, effectively **jeopardizing the Authorization to Operate (ATO)** for the entire system the device connects to, creating an operational liability that could force an immediate mission halt.
3. **Risk Profile Skyrockets:** The probability of sensitive data exfiltration, credential harvesting, or network compromise skyrockets, making the organization's entire security posture acutely vulnerable to a single, unmanaged, and unmonitored endpoint.

The MDM is the critical, automated enforcement arm of the STIG within the Zero-Trust architecture. If the MDM cannot confirm the installation, health, active status, and compliance posture of the MTD agent, the core principle of **"Never Trust, Always Verify"** is violated. In such scenarios, **access to federal resources and networks must be immediately and automatically revoked.** This aggressive, automated enforcement posture is the only viable methodology for effectively managing and mitigating mobile risk at the federal level.

The NIST Framework: The Strategic Foundation for Security Discipline

While the Defense Information Systems Agency (DISA) STIGs provide the tactical, prescriptive configuration controls—the "how"—the overarching strategic foundation for all federal security measures, including the securing of mobile endpoints, is the National Institute of Standards and Technology (NIST) framework.

Specifically, NIST Special Publication 800-53 defines the comprehensive, authoritative catalog of security and privacy controls for federal information systems and organizations. The mobile security requirements enforced by the STIGs (such as mandatory Mobile Threat Detection (MTD) and Mobile Device Management (MDM) are direct, mandated interpretations and implementations of critical, high-impact NIST controls. The relationship is symbiotic, translating high-level policy into technical reality.

NIST Control Family	Relevance to Mobile Security Mandate	STIG Enforcement Mechanism and Technical Implementation
AC (Access Control)	Ensuring that only authenticated, authorized users and compliant devices can access sensitive data; enforcing robust session locks and granular password policies to prevent unauthorized access.	MDM policy enforcement of FIPS-validated password complexity, automatic screen lock and wipe policies, two-factor authentication, and secure device enrollment procedures.
CM (Configuration Management)	Establishing, documenting, and continuously maintaining the integrity of the security baseline configurations to prevent configuration drift and unauthorized changes.	Formal STIG compliance checks (e.g., specific vulnerability IDs like V-276214 for MTD) are rigorously enforced and audited by the MDM platform to ensure all endpoints adhere to the baseline.
SI (System and Information Integrity)	Detecting, reporting, and actively protecting against malicious code, system vulnerabilities, and unauthorized changes to the operating system or application environment.	**MTD Requirement:** Real-time, continuous threat monitoring, behavioral analytics, malware scanning, detection of system anomalies (e.g., rooting/ jailbreaking), and unauthorized application reporting.
SC (System and Communications Protection)	Protecting the confidentiality, integrity, and availability of transmitted data both in transit and at rest, across public and private networks.	MDM enforcement of mandatory always- on VPNs, requiring strong encryption (specifically FIPS 140-2 validated cryptographic modules), and utilizing secure connection protocols (e.g., TLS 1.3) for all communication.

Government-Furnished Equipment (GFE) vs. Bring Your Own Device (BYOD): The Threat is Universal!!!

The distinction between Government-Furnished Equipment (GFE) and Bring Your Own Device (BYOD) environments is one of control, not vulnerability. Lookout's MTD is essential to satisfy the explicit requirement for device-level threat detection found in both.

Environment	Primary Control	VMI's Role	MTD's Mandated Role	STIG Policy
Government-Furnished (GFE)	Full MDM control over device and OS, enforcing policies (e.g., *Apple iOS/iPadOS 18 STIG*).	Isolate classified/CUI mission data within a virtual session.	Provides mandatory, continuous device, app, and network monitoring to ensure the GFE endpoint remains compliant and uncompromised— a specific requirement of the device STIGs.	Apple iOS/iPadOS STIG (e.g., V-276204: *DOD Apple iOS/iPadOS devices must have an MTD app installed.*)
Bring Your Own Device (BYOD)	Limited MDM to a managed segment; user privacy must be maintained (per DoD policy).	Formal STIG compliance checks (e.g., specific vulnerability IDs like V-276214 for MTD) are rigorously enforced and audited by the MDM platform to ensure all endpoints adhere to the baseline.	Detects threats on the entire underlying personal device that could steal credentials, mirror the screen, or compromise the virtual session, ensuring the non-government device is a trusted viewer.	DoD CIO Use of Non-Government Owned Mobile Devices Memo (mandates protection/ isolation on personal devices).

MTD Requirement in DISA STIGs

- **iOS/iPadOS:** The STIG (V-276214) states: "DOD Apple iOS/iPadOS 18 devices must have a Mobile Threat Detection (MTD) app installed".
- **Android:** Requirements are enforced through broader device controls and the Google Android 16 STIG.

OS	MTD Requirement	STIG/Finding ID (Example)	Source STIG (Example)
iOS/iPadOS	**DOD Apple iOS/iPadOS devices must have a Mobile Threat Detection (MTD) app installed.**	**V-276214** (Medium Severity)	**Apple iOS/iPadOS 18 Security Technical Implementation Guide (STIG)**
Android	MTD is generally required under broader device and application security controls, and often implemented as a condition of compliance.	*No single MTD installation finding ID was available in the public snippets, but the requirement is enforced through other controls.*	**Google Android 16 STIG** or **Samsung Android OS STIGs**

Sources and Reference Material

The arguments and alignment strategies detailed in the previous document are derived from the following official federal publications and technical documentation.

1. National Institute of Standards and Technology (NIST)

Publication: NIST Special Publication 800-124 Revision 2: Guidelines for Managing the Security of Mobile Devices in the Enterprise

- **Relevance:** Defines the primary federal requirements for mobile security, specifically the necessity of Mobile Threat Defense (MTD) and distinct handling of GFE and BYOD scenarios.
- **Link:** https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r2.pdf

2. Department of Defense (DoD) Cyber Exchange - STIGs

Publication: Apple iOS/iPadOS 18 Security Technical Implementation Guide (STIG)

- **Relevance:** Provides the specific configuration standards for DoD mobile devices.
- **Key Finding Referenced:** V-276214 (Requirement for MTD installation).
- **Link:** https://public.cyber.mil/stigs/ (Note: STIGs are updated quarterly; users should always verify the latest Release on the Cyber Exchange).

3. Lookout Technical Documentation

Topic: Lookout Mobile Endpoint Security & MDM Integration

- **Relevance:** Details the technical capabilities of the Lookout Security Graph, the architecture of the integration with Microsoft Intune/VMware Workspace ONE, and privacy controls for BYOD.
- **Link:** https://www.lookout.com/products/mobile-endpoint-security
- **Link (FedRAMP Status):** https://marketplace.fedramp.gov/products/lookout-mobile-endpoint-security

4. Microsoft Learn (Integration Context)

Topic: Set up Lookout Mobile Endpoint Security connector with Intune

- **Relevance:** Validates the “Enforcement Mechanism” described in the document, explaining how risk signals are passed from Lookout to Intune to trigger Conditional Access.
- **Link:** https://learn.microsoft.com/en-us/mem/intune/protect/lookout-mobile-threat-defense-connector

Lookout®

To learn more, visit lookout.com