CIS Samsung Android 15 BYOAD STIG Benchmark

v1.0.0 – 04-22-2025

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

NOTE: It is ***NEVER*** acceptable to host a CIS Benchmark in ***ANY*** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Table of Contents

Overview

Target Technology Details

Samsung Android 15 BYOAD Secure Technical Implementation Guide (STIG)

Version: 1 Release: 1 Benchmark

Date: 22 Apr 2025

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Samsung Android 15 BYOAD and are looking to comply with the STIG guidance

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations (or rules) for securing a technology or a supporting platform. STIG Benchmark profiles are used to identify which Vulnerability Severity Category Code (CAT) each rule is associated with.

Description

The Rule Title from the STIG.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Additional Information

Supplementary information that does not correspond to any other field but may be useful to the user.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **SEVERITY: CAT I**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be high severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT II**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be medium severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT III**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be low severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

Acknowledgements

The Recommendations in this Benchmark are a representation of the Rules in the unclassified DISA STIG for Samsung Android 15 BYOAD

Recommendations

1 STIG RULES

Samsung Android 15

Samsung Android 15 BYOAD Secure Technical Implementation Guide (STIG)

Version: 1 Release: 1 Benchmark

Date: 22 Apr 2025

CLASSIFICATION unclassified

1.1 KNOX-15-800200 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The EMM system supporting the Samsung Android 15 BYOAD must be configured for autonomous monitoring, compliance, and validation to ensure security/configuration settings of mobile devices do not deviate from the approved configuration baseline.

```
GROUP ID: V-272498
RULE ID: SV-272498r1098267
```

Rationale:

DOD policy requires BYOAD devices with DOD data be managed by a DOD MDM server, MAM server, or VMI system. This ensures the device can be monitored for compliance with the approved security baseline and the work profile can be removed when the device is out of compliance, which protects DOD data from unauthorized exposure.

Examples of possible EMM security controls are as follows:

1. Device access restrictions: Restrict or isolate access based on the device access type (i.e., from the internet), authentication type (e.g., password), credential strength, etc.
2. User and device activity monitoring: Configured to detect anomalous activity, malicious activity, and unauthorized attempts to access DOD information.
3. Device health tracking: Monitor device attestation, health, and agents reporting compromised applications, connections, intrusions, and/or signatures.

Reference: DOD policy "Use of Non-Government Mobile Devices" (3.a.(3)ii, 3.b.(2)ii.1 & 2).

SFR ID: FMT_SMF_EXT.1.1 47

Audit:

Verify the EMM system supporting the Samsung Android 15 BYOAD has been configured to conduct autonomous monitoring, compliance, and validation to ensure security/configuration settings of mobile devices do not deviate from the approved configuration baseline. The exact procedure will depend on the EMM system used at the site.

If the EMM system supporting the Samsung Android 15 BYOAD has not been configured to conduct autonomous monitoring, compliance, and validation to ensure security/configuration settings of mobile devices, this is a finding.

Remediation:

Configure the EMM system supporting the Samsung Android 15 BYOAD to conduct autonomous monitoring, compliance, and validation to ensure security/configuration settings of mobile devices do not deviate from the approved configuration baseline. The exact procedure will depend on the EMM system used at the site.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.2 KNOX-15-800300 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The EMM system supporting the Samsung Android 15 BYOAD must be configured to initiate autonomous monitoring, compliance, and validation prior to granting the Samsung Android 15 BYOAD access to DOD information and IT resources.

```
GROUP ID: V-272499
RULE ID: SV-272499r1098270
```

Rationale:

DOD policy requires BYOAD devices with DOD data be managed by a DOD MDM server, MAM server, or VMI system. This ensures the device can be monitored for compliance with the approved security baseline and the work profile can be removed when the device is out of compliance, which protects DOD data from unauthorized exposure.

Reference: DOD policy "Use of Non-Government Mobile Devices" (3.a.(3)iii).

SFR ID: FMT_SMF_EXT.1.1 47

Audit:

Verify the EMM system supporting the Samsung Android 15 BYOAD has been configured to initiate autonomous monitoring, compliance, and validation prior to granting the BYOAD access to DOD information and IT resources. The exact procedure will depend on the EMM system used at the site.

If the EMM system supporting the Samsung Android 15 BYOAD has not been configured to initiate autonomous monitoring, compliance, and validation prior to granting the BYOAD access to DOD information and IT resources, this is a finding.

Remediation:

Configure the EMM system supporting the Samsung Android 15 BYOAD to initiate autonomous monitoring, compliance, and validation prior to granting the BYOAD access to DOD information and IT resources. The exact procedure will depend on the EMM system used at the site.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.3 KNOX-15-800400 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The EMM system supporting the Samsung Android 15 BYOAD must be configured to detect if the Samsung Android 15 BYOAD native security controls are disabled.

```
GROUP ID: V-272500
RULE ID: SV-272500r1098273
```

Rationale:

Examples of indicators that the native device security controls have been disabled include jailbroken or rooted devices.

DOD policy requires BYOAD devices with DOD data be managed by a DOD MDM server, MAM server, or VMI system. This ensures the device can be monitored for compliance with the approved security baseline and the work profile can be removed when the device is out of compliance, which protects DOD data from unauthorized exposure. Detection via collecting and analysis of BYOAD generated logs for noncompliance indicators is acceptable.

This detection capability must be implemented prior to BYOAD access to DOD information and IT resources and continuously monitored on the DOD-managed segment of the BYOAD enrolled in the program. If non-DOD information (i.e., personal user data, device information) outside the DOD-managed segment of the BYOAD is required to be accessed, collected, monitored, tracked (i.e., location), or maintained, the circumstances under which this may be done must be outlined in the user agreement.

Reference: DOD policy "Use of Non-Government Mobile Devices" (3.a.(3)iii).

SFR ID: FMT_SMF_EXT.1.1 47

Audit:

Verify the EMM system supporting the Samsung Android 15 BYOAD has been configured to detect if the BYOAD native security controls are disabled. The exact procedure will depend on the EMM system used at the site.

If the EMM system supporting the Samsung Android 15 BYOAD is not configured to detect if the BYOAD native security controls are disabled, this is a finding.

Remediation:

Configure the EMM system supporting the Samsung Android 15 BYOAD to detect if the BYOAD native security controls are disabled. The exact procedure will depend on the EMM system used at the site.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.4 KNOX-15-800500 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The EMM system supporting the Samsung Android 15 BYOAD must be configured to detect if known malicious applications, blocked, or prohibited applications are installed on the Samsung Android 15 BYOAD (DOD-managed segment only).

```
GROUP ID: V-272501
RULE ID: SV-272501r1098276
```

Rationale:

DOD policy requires BYOAD devices with DOD data be managed by a DOD MDM server, MAM server, or VMI system. This ensures the device can be monitored for compliance with the approved security baseline and the work profile can be removed when the device is out of compliance, which protects DOD data from unauthorized exposure. Detection via collecting and analysis of BYOAD generated logs for noncompliance indicators is acceptable.

This detection capability must be implemented prior to Approved Mobile Device (AMD) (called BYOAD device in the STIG) enrollment, AMD access to DOD information and IT resources, and continuously monitored on the DOD-managed segment of the AMD enrolled in the program. If non-DOD information (i.e., personal user data, device information) outside the DOD-managed segment of the AMD is required to be accessed, collected, monitored, tracked (i.e., location), or maintained, the circumstances under which this may be done must be outlined in the user agreement.

Reference: DOD policy "Use of Non-Government Mobile Devices" (3.a.(3)iii).

SFR ID: FMT_SMF_EXT.1.1 47

Audit:

Verify an app vetting process is being used to vet apps before work profile apps are placed in the MDM app repository.

If an app vetting process is not being used to vet apps before work profile apps are placed in the MDM app repository, this is a finding.

Remediation:

Implement an app vetting process before work profile apps are placed in the MDM app repository.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.5 KNOX-15-800700 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The EMM detection/monitoring system must use continuous monitoring of enrolled Samsung Android 15 BYOAD.

```
GROUP ID: V-272503
RULE ID: SV-272503r1098282
```

Rationale:

DOD policy requires BYOAD devices with DOD data be managed by a DOD MDM server, MAM server, or VMI system. This ensures the device can be monitored for compliance with the approved security baseline and the work profile can be removed when the device is out of compliance, which protects DOD data from unauthorized exposure. Continuous monitoring must be used to ensure all noncompliance events will be seen by the detection system.

Reference: DOD policy "Use of Non-Government Mobile Devices" (3.a.(3)iii).

SFR ID: FMT_SMF_EXT.1.1 47

Audit:

Verify the EMM detection/monitoring system is configured to use continuous monitoring of enrolled Samsung Android 15 BYOAD. The exact procedure will depend on the EMM system used at the site.

If the EMM detection/monitoring system is not configured to use continuous monitoring of enrolled Samsung Android 15 BYOAD, this is a finding.

Remediation:

Configure the EMM detection/monitoring system to use continuous monitoring of enrolled Samsung Android 15 BYOAD. The exact procedure will depend on the EMM system used at the site.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.6 KNOX-15-800800 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Samsung Android 15 BYOAD must be configured to either disable access to DOD data and IT systems and user accounts or wipe the work profile if the EMM system detects native security controls are disabled.

```
GROUP ID: V-272504
RULE ID: SV-272504r1098285
```

Rationale:

Examples of indicators that the native device security controls have been disabled include jailbroken or rooted devices.

When a BYOAD is out of compliance, DOD data and apps must be removed to protect against compromise of sensitive DOD information.

Note: The site should review DOD and local data retention policies before wiping the work profile of a BYOAD device.

Reference: DOD policy "Use of Non-Government Mobile Devices" (3.b.(4) 3.b.(5)i).

SFR ID: FMT_SMF_EXT.1.1 47

Audit:

Verify the EMM has been configured to either disable access to DOD data, IT systems, and user accounts on the Samsung Android 15 BYOAD or wipe the work profile if it has been detected that native BYOAD security controls are disabled (e.g., jailbroken/rooted). The exact procedure will depend on the EMM system used at the site.

If the EMM has not been configured to either disable access to DOD data, IT systems, and user accounts on the Samsung Android 15 BYOAD or wipe the work profile if it has been detected that native BYOAD security controls are disabled, this is a finding.

Remediation:

Configure the EMM to either disable access to DOD data and IT systems and user accounts on the Samsung Android 15 BYOAD or wipe the work profile if it has been detected that native BYOAD security controls are disabled (e.g., jailbroken/rooted). The exact procedure will depend on the EMM system used at the site.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.7 KNOX-15-800900 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Samsung Android 15 BYOAD must be configured to either disable access to DOD data and IT systems and user accounts or wipe the work profile if the EMM system detects the Samsung Android 15 BYOAD device has known malicious, blocked, or prohibited applications, or configured to access nonapproved third-party applications stores in the work profile.

```
GROUP ID: V-272505
RULE ID: SV-272505r1098288
```

Rationale:

When a BYOAD is out of compliance, DOD data and apps must be removed to protect against compromise of sensitive DOD information.

Reference: DOD policy "Use of Non-Government Mobile Devices" (3.a.(3)iii).

SFR ID: FMT_SMF_EXT.1.1 47

Audit:

Verify the EMM system has been configured to either disable access to DOD data and IT systems and user accounts or the work profile if it has detected the Samsung Android 15 BYOAD device has known malicious, blocked, or prohibited managed applications, or configured to access nonapproved third-party applications stores for managed apps. The exact procedure will depend on the EMM system used at the site.

If the EMM system has not been configured to either disable access to DOD data and IT systems and user accounts or wipe the work profile if it has detected the Samsung Android 15 BYOAD device has known malicious, blocked, or prohibited managed applications, or configured to access nonapproved third-party applications stores for managed apps, this is a finding.

Remediation:

Configure the EMM system to either disable access to DOD data and IT systems and user accounts or wipe the work profile if it has detected the Samsung Android 15 BYOAD device has known malicious, blocked, or prohibited managed applications, or configured to access nonapproved third-party applications stores for managed apps. The exact procedure will depend on the EMM system used at the site.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.8 KNOX-15-801000 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Samsung Android 15 BYOAD must be configured so that the work profile is removed if the device is no longer receiving security or software updates.

```
GROUP ID: V-272506
RULE ID: SV-272506r1098291
```

Rationale:

When a BYOAD is out of compliance, DOD data and apps must be removed to protect against compromise of sensitive DOD information.

Reference: DOD policy "Use of Non-Government Mobile Devices" (3.b.(1)ii).

SFR ID: FMT_SMF_EXT.1.1 47

Audit:

Verify the EMM system is configured to wipe the work profile if the Samsung Android 15 BYOAD is no longer receiving security or software updates. The exact procedure will depend on the EMM system used at the site.

If the EMM system is not configured to wipe the work profile if the Samsung Android 15 BYOAD is no longer receiving security or software updates, this is a finding.

Remediation:

Configure the EMM system so the work profile is removed if the Samsung Android 15 BYOAD is no longer receiving security or software updates. The exact procedure will depend on the EMM system used at the site.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.9 KNOX-15-801100 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Samsung Android 15 BYOAD and DOD enterprise must be configured to limit access to only AO-approved, corporate-owned enterprise IT resources.

```
GROUP ID: V-272507
RULE ID: SV-272507r1098766
```

Rationale:

Note: IT resources includes DOD networks and applications (for example, DOD email).

The system administrator must have the capability to limit access of the BYOAD to DOD networks and DOD IT resources based on mission needs and risk. An adversary could exploit vulnerabilities created by the weaker configuration to compromise DOD sensitive information. The AO should document networks, IT resources, and enterprise applications that BYOAD can access.

Examples of EMM security controls are as follows:

1. Device access restrictions: Restrict or isolate access based on the device access type (i.e., from the internet), authentication type (e.g., password), credential strength, etc.
2. User and device activity monitoring: Configured to detect anomalous activity, malicious activity, and unauthorized attempts to access DOD information.
3. Device health tracking: Monitor device attestation, health, and agents reporting compromised applications, connections, intrusions, and/or signatures.

Reference: DOD policy "Use of Non-Government Mobile Devices" (3.b.(2)ii).

SFR ID: FMT_SMF_EXT.1.1 47

Audit:

Verify the EMM system and DOD enterprise have been configured to limit the Samsung Android 15 BYOAD access to only AO-approved enterprise IT resources. The exact procedure will depend on the EMM system used and IT resources at the site.

If the EMM system and DOD enterprise have not been configured to limit Samsung Android 15 BYOAD access to only AO-approved enterprise IT resources, this is a finding.

Remediation:

Configure the EMM system and DOD enterprise to limit the Samsung Android 15 BYOAD access to only AO-approved enterprise IT resources. The exact procedure will depend on the EMM system used and IT resources at the site.

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

1.10 KNOX-15-802000 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The EMM system supporting the Samsung Android 15 BYOAD must be NIAP validated (included on the NIAP list of compliant products or products in evaluation) unless the DOD CIO has granted an Approved Exception to Policy (E2P).

```
GROUP ID: V-272516
RULE ID: SV-272516r1098321
```

Rationale:

Note: For a VMI solution, both the client and server must be NIAP compliant.

Nonapproved EMM systems may not include sufficient controls to protect work data, applications, and networks from malware or adversary attack. EMM: mobile device management (MDM), mobile application management (MAM), mobile content management (MCM), or virtual mobile infrastructure (VMI).

Components must only approve devices listed on the NIAP list of compliant products or products listed in evaluation at the following links respectfully:

- https://www.niap-ccevs.org/Product/
- https://www.niap-ccevs.org/Product/PINE.cfm

Reference: DOD policy "Use of Non-Government Mobile Devices" (3.a.(2)).

SFR ID: FMT_SMF_EXT.1.1 47

Audit:

Verify the EMM system supporting the Samsung Android 15 BYOAD is NIAP-validated (included on the NIAP list of compliant products or products in evaluation). If not, verify the DOD CIO has granted an Approved Exception to Policy (E2P).

Note: For a VMI solution, both the client and server components must be NIAP compliant.

If the EMM system supporting the Samsung Android 15 BYOAD is not NIAP-validated (included on the NIAP list of compliant products or products in evaluation) and the DOD CIO has not granted an Approved Exception to Policy (E2P), this is a finding.

Remediation:

Only use an EMM system supporting the Samsung Android 15 BYOAD that is NIAP-validated (included on the NIAP list of compliant products or products in evaluation), unless the DOD CIO has granted an Approved Exception to Policy (E2P).

Note: For a VMI solution, both the client and server components must be NIAP compliant.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.11 KNOX-15-802100 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The user agreement must include a description of what personal data and information is being monitored, collected, or managed by the EMM system or deployed agents or tools.

```
GROUP ID: V-272517
RULE ID: SV-272517r1098324
```

Rationale:

DOD policy states BYOAD owners must sign a user agreement and be made aware of what personal data and activities will be monitored by the Enterprise by including this information in the user agreement.

Reference: DOD policy "Use of Non-Government Mobile Devices" (3.a.(3)ii, and 3.c.(4)).

SFR ID: FMT_SMF_EXT.1.1 47

Audit:

Verify the user agreement includes a description of what personal data and information is being monitored, collected, or managed by the EMM system or deployed agents or tools.

If the user agreement does not include a description of what personal data and information is being monitored, collected, or managed by the EMM system or deployed agents or tools, this is a finding.

Remediation:

Include a description of what personal data and information is being monitored, collected, or managed by the EMM system or deployed agents or tools in the user agreement.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.12 KNOX-15-802200 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The DOD Mobile Service Provider must not allow Samsung Android 15 BYOADs in facilities where personally owned mobile devices are prohibited.

```
GROUP ID: V-272518
RULE ID: SV-272518r1098327
```

Rationale:

DOD policy requires BYOAD devices with DOD data be managed by a DOD MDM server, MAM server, or VMI system. This ensures the device can be monitored for compliance with the approved security baseline and the work profile can be removed when the device is out of compliance, which protects DOD data from unauthorized exposure.

Follow local physical security procedures regarding allowing or prohibiting personally owned mobile devices in a DOD facility. If BYOAD devices are brought into facilities where the AO has determined the risk of using personal devices is unacceptable, this could lead to the exposure of sensitive DOD data.

SFR ID: FMT_SMF_EXT.1.1 47

Audit:

Verify the DOD Mobile Service Provider or information system security officer (ISSO)/information system security manager (ISSM) do not allow BYOADs in facilities where personally owned mobile devices are prohibited.

If the DOD Mobile Service Provider or ISSO/ISSM allows BYOADs in facilities where personally owned mobile devices are prohibited, this is a finding.

Remediation:

Do not allow BYOADs in facilities where personally owned mobile devices are prohibited.

Additional Information:

CCI-000382 Configure the system to prohibit or restrict the use of organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (iii)
- NIST SP 800-53 Revision 4::CM-7 b
- NIST SP 800-53 Revision 5::CM-7 b

1.13 KNOX-15-802300 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Samsung Android 15 BYOAD must be configured to disable device cameras and/or microphones when brought into DOD facilities where mobile phone cameras and/or microphones are prohibited.

```
GROUP ID: V-272519
RULE ID: SV-272519r1098330
```

Rationale:

In some DOD operational environments, the use of the mobile device camera or microphone could lead to a security incident or compromise of DOD information. The system administrator must have the capability to disable the mobile device camera and/or microphone based on mission needs. Alternatively, mobile devices with cameras or microphones that cannot be disabled must be prohibited from the facility by the information system security officer (ISSO)/information system security manager (ISSM).

If BYOAD devices are brought into facilities where the AO has determined the risk of using mobile device cameras or microphones is unacceptable, this could lead to the exposure of sensitive DOD data.

SFR ID: FMT_SMF_EXT.1.1 47

Audit:

Verify Samsung Android 15 BYOADs are prohibited in DOD facilities that prohibit mobile devices with cameras and microphones.

If for DOD sites that prohibit mobile devices with cameras and microphones, Samsung Android 15 BYOADs have not been prohibited from the facility by the ISSO/ISSM, this is a finding.

Remediation:

It is not possible to disable phone cameras and/or microphones when in BYOD mode. Therefore, do not allow Samsung Android 15 BYOADs in DOD facilities where mobile phone cameras and/or microphones are prohibited.

Additional Information:

CCI-000382 Configure the system to prohibit or restrict the use of organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (iii)
- NIST SP 800-53 Revision 4::CM-7 b
- NIST SP 800-53 Revision 5::CM-7 b

1.14 KNOX-15-802800 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The mobile device used for BYOAD must be NIAP validated.

```
GROUP ID: V-272524
RULE ID: SV-272524r1098767
```

Rationale:

Nonapproved mobile devices may not include sufficient controls to protect work data, applications, and networks from malware or adversary attack.

Components must only approve devices listed on the NIAP list of compliant products or products listed in evaluation at the following links respectively:

- https://www.niap-ccevs.org/Product/
- https://www.niap-ccevs.org/Product/PINE.cfm

Reference: DOD policy "Use of Non-Government Mobile Devices" (3.b.(1)i).

SFR ID: FMT_SMF_EXT.1.1 47

Audit:

Verify the mobile device used for BYOAD is NIAP-validated (included on the NIAP list of compliant products or products in evaluation).

If the mobile device used for BYOAD is not NIAP-validated (included on the NIAP list of compliant products or products in evaluation), this is a finding.

Remediation:

Use only mobile devices for BYOAD that are NIAP-validated (included on the NIAP list of compliant products or products in evaluation).

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	KNOX-15-800200 (Manual)	☐	☐
1.2	KNOX-15-800300 (Manual)	☐	☐
1.3	KNOX-15-800400 (Manual)	☐	☐
1.4	KNOX-15-800500 (Manual)	☐	☐
1.5	KNOX-15-800700 (Manual)	☐	☐
1.6	KNOX-15-800800 (Manual)	☐	☐
1.7	KNOX-15-800900 (Manual)	☐	☐
1.8	KNOX-15-801000 (Manual)	☐	☐
1.9	KNOX-15-801100 (Manual)	☐	☐
1.10	KNOX-15-802000 (Manual)	☐	☐
1.11	KNOX-15-802100 (Manual)	☐	☐
1.12	KNOX-15-802200 (Manual)	☐	☐
1.13	KNOX-15-802300 (Manual)	☐	☐
1.14	KNOX-15-802800 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
08-27-2025	1.0.0	Initial CIS Release