CIS Apple iOS/iPadOS 18 STIG Benchmark

v1.0.0 - 09-12-2025

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

Target Technology Details

Apple iOS/iPadOS 18 Secure Technical Implementation Guide (STIG)

Version: 2 Release: 1 Benchmark

Date: 08 Aug 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 Apple iOS/iPadOS 18 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

References from the STIG Rule if applicable.

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 Apple iOS/iPadOS 18

Recommendations

1 STIG RULES

Apple iOS 18.x

Apple iOS/iPadOS 18 Secure Technical Implementation Guide (STIG)

Version: 2 Release: 1 Benchmark

Date: 08 Aug 2025

CLASSIFICATION unclassified

1.1 AIOS-18-001000 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Apple iOS/iPadOS 18 must allow the administrator (MDM) to perform the following management function: enable/disable VPN protection across the device and [selection: on a per-app basis, on a per-group of applications processes basis].

```
GROUP ID: V-267937
RULE ID: SV-267937r1120908
```

Rationale:

The system administrator must have the capability to configure VPN access to meet organization-specific policies based on mission needs. Otherwise, a user could inadvertently or maliciously set up a VPN and connect to a network that poses unacceptable risk to DOD information systems. An adversary could exploit vulnerabilities created by the weaker configuration to compromise DOD sensitive information.

```
SFRID: FMT_SMF.1.1 #3
```

Audit:

Review the list of unmanaged apps installed on the iPhone and iPad and determine if any unmanaged third-party VPN clients are installed. If so, verify the VPN app is not configured with a DOD network (work) VPN profile.

This validation procedure is performed on the iOS device only.

On the iPhone and iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap the "VPN and Device Management" line and determine if any "Personal VPN" exists.
4. If not, the requirement has been met.
5. If there are personal VPNs, open each VPN app. Review the list of VPN profiles configured on the VPN client.
6. Verify no DOD network VPN profiles are configured on the VPN client.

If any third-party unmanaged VPN apps are installed (personal VPN) and they have a DOD network VPN profile configured on the client, this is a finding.

Note: This setting cannot be managed by the MDM administrator and is a User-Based Enforcement (UBE) requirement.

Remediation:

If a third-party unmanaged VPN app is installed on the iOS 18 device, do not configure the VPN app with a DOD network VPN profile.

Additional Information:

CCI-000068

Implement cryptographic mechanisms to protect the confidentiality of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

CCI-000370 Manage configuration settings for organization-defined system components using organization-defined automated mechanisms.

- NIST SP 800-53::CM-6 (1)
- NIST SP 800-53A::CM-6 (1).1
- NIST SP 800-53 Revision 4::CM-6 (1)
- NIST SP 800-53 Revision 5::CM-6 (1)

1.2 AIOS-18-003000 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must not allow backup to remote systems (iCloud).

```
GROUP ID: V-267958
RULE ID: SV-267958r1117267
```

Rationale:

If a user is able to configure the security setting, the user could inadvertently or maliciously set it to a value that poses unacceptable risk to DOD information systems. An adversary could exploit vulnerabilities created by the weaker configuration to compromise DOD sensitive information.

```
SFRID: FMT_MOF_EXT.1.2 #40
```

Audit:

Note: This requirement is not applicable if the authorizing official (AO) has approved users' 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. The site must have an AO-signed document showing the AO has assumed the risk for users' full access to the Apple App Store.

Review configuration settings to confirm iCloud Backup is disabled.

This check procedure is performed on both the Apple iOS/iPadOS management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the Apple iOS/iPadOS management tool, verify "Allow iCloud backup" is unchecked.

Alternatively, verify the text `<key>allowCloudBackup</key> <false/>` appears in the configuration profile (`.mobileconfig` file).

On the iPhone and iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the policy.

5. Tap "Restrictions".
6. Verify "iCloud backup not allowed".

If "Allow iCloud backup" is checked in the Apple iOS/iPadOS management tool, `<key>allowCloudBackup</key><true/>` appears in the configuration profile, or the restrictions policy on the iPhone and iPad does not list "iCloud backup not allowed", this is a finding.

Remediation:

Install a configuration profile to disable iCloud backup.

Additional Information:

CCI-001090

Prevent unauthorized and unintended information transfer via shared system resources.

- NIST SP 800-53::SC-4
- NIST SP 800-53A::SC-4.1
- NIST SP 800-53 Revision 4::SC-4
- NIST SP 800-53 Revision 5::SC-4

1.3 AIOS-18-003200 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must not allow backup to remote systems (iCloud document and data synchronization).

```
GROUP ID: V-267959
RULE ID: SV-267959r1117267
```

Rationale:

If a user is able to configure the security setting, the user could inadvertently or maliciously set it to a value that poses unacceptable risk to DOD information systems. An adversary could exploit vulnerabilities created by the weaker configuration to compromise DOD sensitive information.

```
SFRID: FMT_MOF_EXT.1.2 #40
```

Audit:

Note: This requirement is not applicable if the authorizing official (AO) has approved users' 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. The site must have an AO-signed document showing the AO has assumed the risk for users' full access to the Apple App Store.

This is a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding.

If the iPhone or iPad being reviewed is supervised by the MDM, review configuration settings to confirm "Allow iCloud documents & data" is disabled.

This check procedure is performed on both the Apple iOS/iPadOS management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the Apple iOS/iPadOS management tool, verify "Allow iCloud documents & data" is unchecked.

Alternatively, verify the text `<key>allowCloudDocumentSync</key> <false/>` appears in the configuration profile (`.mobileconfig` file).

On the iPhone and iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the policy.
5. Tap "Restrictions".
6. Verify "Documents in the Cloud not allowed" is listed.

Note: This also verifies that iCloud Drive and iCloud Photo Library are disabled.

If "Allow iCloud documents & data" is checked in the Apple iOS/iPadOS management tool, `<key>allowCloudDocumentSync</key> <true/>` appears in the configuration profile, or the restrictions policy on the iPhone and iPad does not list "Documents in the Cloud not allowed", this is a finding.

Remediation:

Install a configuration profile to disable iCloud documents and data. This a supervised-only control.

Additional Information:

CCI-001090

Prevent unauthorized and unintended information transfer via shared system resources.

- NIST SP 800-53::SC-4
- NIST SP 800-53A::SC-4.1
- NIST SP 800-53 Revision 4::SC-4
- NIST SP 800-53 Revision 5::SC-4

1.4 AIOS-18-003300 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must not allow backup to remote systems (iCloud Keychain).

```
GROUP ID: V-267960
RULE ID: SV-267960r1117267
```

Rationale:

If a user is able to configure the security setting, the user could inadvertently or maliciously set it to a value that poses unacceptable risk to DOD information systems. An adversary could exploit vulnerabilities created by the weaker configuration to compromise DOD sensitive information.

```
SFRID: FMT_MOF_EXT.1.2 #40
```

Audit:

Note: This requirement is not applicable if the authorizing official (AO) has approved users' 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. The site must have an AO-signed document showing the AO has assumed the risk for users' full access to the Apple App Store.

This is a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding.

If the iPhone or iPad being reviewed is supervised by the MDM, review configuration settings to confirm iCloud keychain is disabled.

This check procedure is performed on both the Apple iOS/iPadOS management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the Apple iOS/iPadOS management tool, verify "Allow iCloud keychain" is unchecked.

Alternatively, verify the text `<key>allowCloudKeychainSync</key><false/>` appears in the configuration profile (`.mobileconfig` file).

On the iPhone and iPad:

1. Open the Settings app.

2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the management policy.
5. Verify "iCloud Keychain not allowed" is listed.

If "Allow iCloud keychain" is checked in the Apple iOS/iPadOS management tool, `<key>allowCloudKeychainSync</key><true/>` appears in the configuration profile, or "iCloud Keychain not allowed" is not listed on the iPhone and iPad, this is a finding.

Remediation:

Install a configuration profile to disable iCloud keychain. This a supervised-only control.

Additional Information:

CCI-001090

Prevent unauthorized and unintended information transfer via shared system resources.

- NIST SP 800-53::SC-4
- NIST SP 800-53A::SC-4.1
- NIST SP 800-53 Revision 4::SC-4
- NIST SP 800-53 Revision 5::SC-4

1.5 AIOS-18-003450 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must not allow backup to remote systems (Cloud Photo Library).

```
GROUP ID: V-267961
RULE ID: SV-267961r1117267
```

Rationale:

If a user is able to configure the security setting, the user could inadvertently or maliciously set it to a value that poses unacceptable risk to DOD information systems. An adversary could exploit vulnerabilities created by the weaker configuration to compromise DOD sensitive information.

```
SFRID: FMT_MOF_EXT.1.2 #40
```

Audit:

Note: This requirement is not applicable if the authorizing official (AO) has approved users' 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. The site must have an AO-signed document showing the AO has assumed the risk for users' full access to the Apple App Store.

This is a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding.

If the iPhone or iPad being reviewed is supervised by the MDM, review configuration settings to confirm "Allow Cloud Photo Library" is disabled.

This check procedure is performed on both the Apple iOS/iPadOS management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the Apple iOS/iPadOS management tool, verify "Allow Cloud Photo Library" is unchecked.

Alternatively, verify the text `<key>allowCloudPhotoLibrary</key><false/>`" appears in the configuration profile (`.mobileconfig` file).

On the iPhone and iPad:

1. Open the Settings app.

2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the Apple iOS/iPadOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "iCloud Photos not allowed" is listed.

If "Allow Cloud Photo Library" is checked in the Apple iOS/iPadOS management tool, `<key>allowCloudPhotoLibrary</key> <true/>` appears in the configuration profile, or the restrictions policy on the iPhone and iPad does not list "iCloud Photos not allowed", this is a finding.

Remediation:

Install a configuration profile to disable Cloud Photo Library. This a supervised-only control.

Additional Information:

CCI-001090

Prevent unauthorized and unintended information transfer via shared system resources.

- NIST SP 800-53::SC-4
- NIST SP 800-53A::SC-4.1
- NIST SP 800-53 Revision 4::SC-4
- NIST SP 800-53 Revision 5::SC-4

1.6 AIOS-18-003500 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must not allow backup to remote systems (iCloud Photo Sharing, also known as Shared Stream or Shared Photo Stream).

```
GROUP ID: V-267962
RULE ID: SV-267962r1117267
```

Rationale:

If a user is able to configure the security setting, the user could inadvertently or maliciously set it to a value that poses unacceptable risk to DOD information systems. An adversary could exploit vulnerabilities created by the weaker configuration to compromise DOD sensitive information.

```
SFRID: FMT_MOF_EXT.1.2 #40
```

Audit:

Note: This requirement is not applicable if the authorizing official (AO) has approved users' 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. The site must have an AO-signed document showing the AO has assumed the risk for users' full access to the Apple App Store.

This is a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding.

If the iPhone or iPad being reviewed is supervised by the MDM, review configuration settings to confirm "Allow Shared Stream" is disabled.

This check procedure is performed on both the Apple iOS/iPadOS management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the Apple iOS/iPadOS management tool, verify "Allow Shared Stream" is unchecked.

Alternatively, verify the text `<key>allowSharedStream</key><false/>` appears in the configuration profile (`.mobileconfig` file).

On the iPhone and iPad:

1. Open the Settings app.

2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the Apple iOS/iPadOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "Shared Streams not allowed" is listed.

If "AllowShared Photo Stream" is checked in the Apple iOS/iPadOS management tool, `<key>allowSharedStream</key><true/>` appears in the configuration profile, or the restrictions policy on the iPhone and iPad does not list "Shared Streams not allowed", this is a finding.

This requirement will become "Supervised only" in a future iOS/iPadOS release.

Remediation:

Install a configuration profile to disable "Allow Shared PhotoStream". This a supervised-only control.

Additional Information:

CCI-001090

Prevent unauthorized and unintended information transfer via shared system resources.

- NIST SP 800-53::SC-4
- NIST SP 800-53A::SC-4.1
- NIST SP 800-53 Revision 4::SC-4
- NIST SP 800-53 Revision 5::SC-4

1.7 AIOS-18-003600 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must not allow backup to remote systems (managed applications data stored in iCloud).

```
GROUP ID: V-267963
RULE ID: SV-267963r1117267
```

Rationale:

If a user is able to configure the security setting, the user could inadvertently or maliciously set it to a value that poses unacceptable risk to DOD information systems. An adversary could exploit vulnerabilities created by the weaker configuration to compromise DOD sensitive information.

```
SFRID: FMT_MOF_EXT.1.2 #40
```

Audit:

Review configuration settings to confirm "Allow managed apps to store data in iCloud" is disabled.

This check procedure is performed on both the Apple iOS/iPadOS management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the Apple iOS/iPadOS management tool, verify "Allow managed apps to store data in iCloud" is unchecked.

Alternatively, verify the text `<key>allowManagedAppsCloudSync</key> <false/>` appears in the configuration profile (`.mobileconfig` file).

On the iPhone and iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the Apple iOS/iPadOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "Managed apps cloud sync not allowed" is listed.

If "Allow managed apps to store data in iCloud" is checked in the Apple iOS/iPadOS management tool, `<key>allowManagedAppsCloudSync</key> <true/>` appears in the configuration profile, or the restrictions policy on the iPhone and iPad does not list "Managed apps cloud sync not allowed", this is a finding.

Remediation:

Install a configuration profile to prevent DOD applications from storing data in iCloud.

Additional Information:

CCI-001090

Prevent unauthorized and unintended information transfer via shared system resources.

- NIST SP 800-53::SC-4
- NIST SP 800-53A::SC-4.1
- NIST SP 800-53 Revision 4::SC-4
- NIST SP 800-53 Revision 5::SC-4

1.8 AIOS-18-003700 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must not allow backup to remote systems (enterprise books).

```
GROUP ID: V-267964
RULE ID: SV-267964r1117267
```

Rationale:

If a user is able to configure the security setting, the user could inadvertently or maliciously set it to a value that poses unacceptable risk to DOD information systems. An adversary could exploit vulnerabilities created by the weaker configuration to compromise DOD sensitive information.

```
SFRID: FMT_MOF_EXT.1.2 #40
```

Audit:

Review configuration settings to confirm "Allow backup of enterprise books" is disabled.

This check procedure is performed on both the Apple iOS/iPadOS management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the Apple iOS/iPadOS management tool, verify "Allow backup of enterprise books" is unchecked.

Alternatively, verify the text `<key>allowEnterpriseBookBackup</key> <false/>` appears in the configuration profile (`.mobileconfig` file).

On the iPhone and iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the Apple iOS/iPadOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "Backing up enterprise books not allowed" is listed.

If "Allow backup of enterprise books" is checked in the Apple iOS/iPadOS management tool, `<key>allowEnterpriseBookBackup</key> <true/>` appears in the configuration profile, or the restrictions policy on the iPhone and iPad does not list "Backing up enterprise books not allowed", this is a finding.

Remediation:

Install a configuration profile to prevent backup of enterprise books that could contain DOD sensitive information.

Additional Information:

CCI-001090

Prevent unauthorized and unintended information transfer via shared system resources.

- NIST SP 800-53::SC-4
- NIST SP 800-53A::SC-4.1
- NIST SP 800-53 Revision 4::SC-4
- NIST SP 800-53 Revision 5::SC-4

1.9 AIOS-18-006500 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must be configured to enforce a minimum password length of six characters.

```
GROUP ID: V-267987
RULE ID: SV-267987r1031167
```

Rationale:

Password strength is a measure of the effectiveness of a password in resisting guessing and brute force attacks. The ability to crack a password is a function of how many attempts an adversary is permitted, how quickly an adversary can do each attempt, and the size of the password space. The longer the minimum length of the password is, the larger the password space. Having a too-short minimum password length significantly reduces password strength, increasing the chance of password compromise and resulting device and data compromise.

```
SFRID: FMT_SMF.1.1 #1
```

Audit:

Review configuration settings to confirm the minimum passcode length is six or more characters.

This procedure is performed in the Apple iOS/iPadOS management tool and on the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the Management tool, verify the "Minimum passcode length" value is set to six or greater.

Alternatively, verify the text `<key>minLength</key> <integer>6</integer>` appears in the configuration profile (`.mobileconfig` file). It also is acceptable for the integer value to be greater than six.

On the iPhone and iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".

4. Tap the Configuration Profile from the Apple iOS/iPadOS management tool containing the password policy.
5. Tap "Restrictions".
6. Tap "Passcode".
7. Verify "Minimum length" is listed as "six or greater".

If the "Minimum passcode length" is less than six characters in the iOS management tool, `<key>minLength</key>` has an integer value of less than six, or the password policy on the iPhone and iPad from the Apple iOS/iPadOS management tool does not list "Minimum length" of six or more, this is a finding.

Remediation:

Install a configuration profile to enforce a minimum passcode length value of six or greater.

Additional Information:

CCI-004066

For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

1.10 AIOS-18-006600 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must be configured to not allow passwords that include more than four repeating or sequential characters.

```
GROUP ID: V-267988
RULE ID: SV-267988r1031168
```

Rationale:

Password strength is a measure of the effectiveness of a password in resisting guessing and brute force attacks. Passwords that contain repeating or sequential characters are significantly easier to guess than those that do not contain repeating or sequential characters. Therefore, disallowing repeating or sequential characters increases password strength and decreases risk.

```
SFRID: FMT_SMF.1.1 #1
```

Audit:

Review configuration settings to confirm simple passcodes are not allowed.

This check procedure is performed on both the Apple iOS/iPadOS management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the Apple iOS/iPadOS management tool, verify "Allow simple value" is unchecked. Alternatively, verify the text `<key>allowSimple</key> <false/>` appears in the configuration profile (`.mobileconfig` file).

On the iPhone and iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the password policy.
5. Tap "Restrictions".
6. Tap "Passcode".
7. Verify "Simple passcodes allowed" is set to "No".

If "Allow simple value" is checked in the Apple iOS/iPadOS management tool, `<key>allowSimple</key> <true/>` appears in the Configuration Profile, or the password policy on the iPhone and iPad does not have "Simple passcodes allowed" set to "No", this is a finding.

Remediation:

Install a configuration profile to disallow more than four sequential or repeating numbers or letters in the device unlock password.

Additional Information:

CCI-004066

For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

1.11 AIOS-18-006800 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must be configured to lock the display after 15 minutes (or less) of inactivity.

```
GROUP ID: V-267990
RULE ID: SV-267990r1031170
```

Rationale:

The screen lock timeout must be set to a value that helps protect the device from unauthorized access. Having a too-long timeout would increase the window of opportunity for adversaries who gain physical access to the mobile device through loss, theft, etc. Such devices are much more likely to be in an unlocked state when acquired by an adversary, thus granting immediate access to the data on the mobile device. The maximum timeout period of 15 minutes has been selected to balance functionality and security; shorter timeout periods may be appropriate depending on the risks posed to the mobile device.

```
SFRID: FMT_SMF.1.1 #2
```

Audit:

Review configuration settings to confirm the screen lock timeout is set to 15 minutes or less.

This check procedure is performed on both the Apple iOS/iPadOS management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the management tool, verify the sum of the values assigned to "Maximum Auto-Lock time" and "Grace period for device lock" is between 1 and 15 minutes.

Alternatively, locate the text `<key>maxGracePeriod</key>` and `<key>maxInactivity</key>` and ensure the sum of their integer value is between `1` and `15` in the configuration profile (`.mobileconfig` file). For example:

```
"<key>maxGracePeriod</key>
<integer>5</integer>
<key>maxInactivity</key>
<integer>5</integer>"
```

Here, `5 + 5 = 10;` this meets the requirement.

On the iPhone and iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the password policy.
5. Tap "Restrictions".
6. Tap "Passcode".
7. Verify the sum of the "Max grace period" and "Max inactivity" values is less than 15 minutes.

Note: On some iOS/iPadOS devices, it is not possible to have a sum of exactly `15`. In these cases, the sum must be less than `15`. A sum of `16` does not meet the requirement.

On the management server, if the sum of the "Max grace period" and "Max inactivity" values is not between 1 and 15 minutes in the iOS/iPadOS management tool or the sum of the values assigned to `<key>maxGracePeriod</key>` and `<key>maxInactivity</key>` is not between 1 and 15 minutes in the configuration profile, or if on the iPhone/iPad, the sum of the values assigned to "Max grace period" and "Max inactivity" is not between 1 and 15 minutes, this is a finding.

Remediation:

Install a configuration profile to lock the device display after 15 minutes (or less) of inactivity. This is done by setting "Maximum Auto-Lock time" and "Grace Period for device lock" so the sum of their values is between 1 and 15 minutes.

Additional Information:

CCI-000057

Prevent further access to the system by initiating a device lock after organization-defined time period of inactivity; and/or requiring the user to initiate a device lock before leaving the system unattended.

- NIST SP 800-53::AC-11 a
- NIST SP 800-53A::AC-11.1 (ii)
- NIST SP 800-53 Revision 4::AC-11 a
- NIST SP 800-53 Revision 5::AC-11 a

1.12 AIOS-18-006900 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must be configured to not allow more than 10 consecutive failed authentication attempts.

```
GROUP ID: V-267991
RULE ID: SV-267991r1031171
```

Rationale:

The more attempts an adversary has to guess a password, the more likely the adversary will enter the correct password and gain access to resources on the device. Setting a limit on the number of attempts mitigates this risk. Setting the limit at 10 or less gives authorized users the ability to make a few mistakes when entering the password but still provides adequate protection against dictionary or brute force attacks on the password.

```
SFRID: FMT_SMF.1.1 #2, FIA_AFL_EXT.1.5
```

Audit:

Review configuration settings to confirm that consecutive failed authentication attempts is set to 10 or fewer.

This procedure is performed in the Apple iOS/iPadOS management tool and on the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the Management tool, verify the "Maximum number of failed attempts" value is set to `10` or fewer.

Alternatively, verify the text `<key>maxFailedAttempts</key>` `<integer>10</integer>` appears in the configuration profile (`.mobileconfig` file). It also is acceptable for the integer value to be less than `10`.

On the iPhone and iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the password policy.

5. Tap "Restrictions".
6. Tap "Passcode".
7. Verify "Max failed attempts" is listed as `10` or fewer.

If the "Maximum number of failed attempts" is more than `10` in the iOS management tool, `<key>maxFailedAttempts</key>` has an integer value of more than 10, or the password policy on the iPhone and iPad does not list "Max failed attempts" of `10` or fewer, this is a finding.

Remediation:

Install a configuration profile to allow only 10 or fewer consecutive failed authentication attempts.

Additional Information:

CCI-000044

Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53::AC-7 a
- NIST SP 800-53A::AC-7.1 (ii)
- NIST SP 800-53 Revision 4::AC-7 a
- NIST SP 800-53 Revision 5::AC-7 a

1.13 AIOS-18-006950 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Apple iOS/iPadOS 18 must be configured to enforce a passcode reuse prohibition of at least two generations.

```
GROUP ID: V-267992
RULE ID: SV-267992r1031172
```

Rationale:

iOS-iPadOS 17 and later versions include a feature that allows the previous passcode to be valid for 72 hours after a passcode change. If the previous passcode has been compromised and the attacker has access to it and the Apple device, enterprise data and the enterprise network can be compromised. Currently there is no MDM control to force the old passcode to expire immediately after passcode change. The previous passcode will expire immediately after a passcode change if the MDM password history control is implemented.

```
SFRID: FMT_SMF.1.1 #47
```

Audit:

Review configuration settings to confirm the Apple iOS or iPadOS device has a passcode reuse prohibition of at least two generations.

This procedure is performed in the Apple iOS/iPadOS management tool and on the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the Management tool, verify the "Passcode History" value is set to `two` or greater.

On the iPhone and iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the Apple iOS/iPadOS management tool containing the password policy.
5. Tap "Restrictions".
6. Tap "Passcode".
7. Verify "Number of unique recent passcodes required" is listed as `two` or greater.

If the Apple iOS or iPadOS device does not enforce a passcode reuse prohibition of at least two generations, this is a finding.

Remediation:

Install a configuration profile to enforce a passcode reuse prohibition of at least two generations (passcode history).

Additional Information:

CCI-004061

For password-based authentication, verify when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5 (1) (a).

- NIST SP 800-53 Revision 5::IA-5 (1) (b)

1.14 AIOS-18-007000 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must be configured to enforce an application installation policy by specifying one or more authorized application repositories, including [selection: DOD-approved commercial app repository, MDM server, mobile application store].

```
GROUP ID: V-267993
RULE ID: SV-267993r1031173
```

Rationale:

Forcing all applications to be installed from authorized application repositories can prevent unauthorized and malicious applications from being installed and executed on mobile devices. Allowing such installations and executions could cause a compromise of DOD data accessible by these unauthorized/malicious applications.

```
SFRID: FMT_SMF.1.1 #8
```

Audit:

Review configuration settings to confirm "Allow Trusting New Enterprise App Authors" is disabled.

This procedure is performed in the Apple iOS/iPadOS management tool and on the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the Management tool, verify "Allow Trusting New Enterprise App Authors" is disabled.

On the iPhone and iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the Apple iOS/iPadOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "Trusting enterprise apps not allowed" is listed.

If "Allow Trusting New Enterprise App Authors" is not disabled in the iOS/iPadOS management tool or on the iPhone and iPad, this is a finding.

Remediation:

Install a configuration profile to disable "Allow Trusting New Enterprise App Authors".

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

1.15 AIOS-18-007200 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must not include applications with the following characteristics: access to Siri when the device is locked.

```
GROUP ID: V-267995
RULE ID: SV-267995r1032950
```

Rationale:

Requiring all authorized applications to be in an application allow list prevents the execution of any applications (e.g., unauthorized, malicious) that are not part of the allow list. Failure to configure an application allow list properly could allow unauthorized and malicious applications to be downloaded, installed, and executed on the mobile device, causing a compromise of DOD data accessible by these applications. Applications with the listed characteristics have features that can cause the compromise of sensitive DOD data or have features with no known application in the DOD environment.

Application note: The application allow list, in addition to controlling the installation of applications on the MD, must control user access/execution of all core and preinstalled applications, or the MD must provide an alternate method of restricting user access/execution to core and preinstalled applications.

Core application: Any application integrated into the OS by the OS or MD vendors.

Preinstalled application: Additional noncore applications included in the OS build by the OS vendor, MD vendor, or wireless carrier.

```
SFRID: FMT_SMF.1.1 #8
```

Audit:

Review configuration settings to confirm that Siri is disabled on the Lock screen.

This check procedure is performed on both the Apple iOS/iPadOS management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the Apple iOS/iPadOS management tool, verify "Allow Siri while device is locked" is unchecked.

Alternatively, verify the text `<key>allowAssistantWhileLocked</key><false/>` appears in the configuration profile (`.mobileconfig` file).

On the iPhone and iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the Apple iOS/iPadOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "Siri while locked not allowed" is listed.

If "Allow Siri while device is locked" is checked in the Apple iOS/iPadOS management tool, or `<key>allowAssistantWhileLocked</key><true/>` appears in the configuration profile, or the restrictions policy on the iPhone and iPad from the Apple iOS/iPadOS management tool does not list "Siri while locked not allowed", this is a finding.

Remediation:

Install a configuration profile to disable Siri while the device is locked.

Additional Information:

CCI-000803

Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

- NIST SP 800-53::IA-7
- NIST SP 800-53A::IA-7.1
- NIST SP 800-53 Revision 4::IA-7
- NIST SP 800-53 Revision 5::IA-7

1.16 AIOS-18-007400 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Apple iOS/iPadOS 18 allow list must be configured to not include applications with the following characteristics:

- Backs up MD data to non-DOD cloud servers (including user and application access to cloud backup services);
- Transmits MD diagnostic data to non-DOD servers;
- Allows synchronization of data or applications between devices associated with user;
- Allows unencrypted (or encrypted but not FIPS 140-3 validated) data sharing with other MDs or printers;
- Backs up its own data to a remote system; and
- Uses artificial intelligence (AI), which processes data in the cloud (off device). Exception: Apple Intelligence Private Cloud Compute (PCC).

```
GROUP ID: V-267997
RULE ID: SV-267997r1042532
```

Rationale:

Requiring all authorized applications to be in an application allow list prevents the execution of any applications (e.g., unauthorized, malicious) that are not part of the allow list. Failure to configure an application allow list properly could allow unauthorized and malicious applications to be downloaded, installed, and executed on the mobile device, causing a compromise of DOD data accessible by these applications. Applications with the listed characteristics have features that can cause the compromise of sensitive DOD data or have features with no known application in the DOD environment.

Application note: The application allow list, in addition to controlling the installation of applications on the MD, must control user access/execution of all core and preinstalled applications, or the MD must provide an alternate method of restricting user access/execution to core and preinstalled applications.

Core application: Any application integrated into the OS by the OS or MD vendors.

Preinstalled application: Additional noncore applications included in the OS build by the OS vendor, MD vendor, or wireless carrier.

```
SFRID: FMT_SMF.1.1 #8
```

Audit:

Verify no apps with the following prohibited characteristics are included in the configuration profile:

- Backs up MD data to non-DOD cloud servers (including user and application access to cloud backup services);
- Transmits MD diagnostic data to non-DOD servers;
- Allows synchronization of data or applications between devices associated with user;
- Allows unencrypted (or encrypted but not FIPS 140-3 validated) data sharing with other MDs or printers;
- Backs up its own data to a remote system; and
- Uses AI, which processes data in the cloud (off device). Exception: Apple Intelligence Private Cloud Compute (PCC).

This check procedure is performed on the Apple iOS/iPadOS management tool.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the Apple iOS/iPadOS management tool, verify "Allow Listed App" (`allowlistedAppBundleIDs`) is configured and there are no apps with prohibited characteristics.

If "Allow listed apps" is not configured and contains apps with prohibited characteristics, this is a finding.

Remediation:

Install a configuration profile with an allow list of approved apps (`allowlistedAppBundleIDs`). Ensure the allow list does not include apps with the following characteristics:

- Backs up MD data to non-DOD cloud servers (including user and application access to cloud backup services);
- Transmits MD diagnostic data to non-DOD servers;
- Allows synchronization of data or applications between devices associated with user;
- Allows unencrypted (or encrypted but not FIPS 140-3 validated) data sharing with other MDs or printers;
- Backs up its own data to a remote system; and
- Uses AI, which processes data in the cloud (off device). Exception: Apple Intelligence Private Cloud Compute (PCC).

Additional Information:

CCI-000803

Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

- NIST SP 800-53::IA-7
- NIST SP 800-53A::IA-7.1
- NIST SP 800-53 Revision 4::IA-7
- NIST SP 800-53 Revision 5::IA-7

1.17 AIOS-18-007500 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must be configured to not display notifications when the device is locked.

```
GROUP ID: V-267998
RULE ID: SV-267998r1031178
```

Rationale:

Many mobile devices display notifications on the lock screen so users can obtain relevant information in a timely manner without having to frequently unlock the phone to determine if there are new notifications. However, in many cases, these notifications can contain sensitive information. When they are available on the lock screen, an adversary can see them merely by being in close physical proximity to the device. Configuring the mobile operating system to not send notifications to the lock screen mitigates this risk.

```
SFRID: FMT_SMF.1.1 #18
```

Audit:

Review configuration settings to confirm the display of notifications when the device is locked has been disabled.

This check procedure is performed on the Apple iOS/iPadOS management tool and mobile device.

In the Apple iOS/iPadOS management tool, for each managed app, verify the app is configured to disable Notifications preview.

On the iPhone and iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the management policy.
5. Tap "Apps".
6. Tap an app and verify "Disallow notification view in locked screen" is listed.

Repeat steps 5 and 6 for each managed app in the list.

If one or more managed apps are not set to disable showing notification view on locked screen, this is a finding.

Remediation:

Install a configuration profile to disable the display of notifications when the device is locked.

Install a configuration profile to disable Notification Center from the device Lock screen.

Additional Information:

CCI-000060

Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

- NIST SP 800-53::AC-11 (1)
- NIST SP 800-53A::AC-11 (1).1
- NIST SP 800-53 Revision 4::AC-11 (1)
- NIST SP 800-53 Revision 5::AC-11 (1)

1.18 AIOS-18-007600 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must not display notifications (calendar information) when the device is locked.

```
GROUP ID: V-267999
RULE ID: SV-267999r1031179
```

Rationale:

Many mobile devices display notifications on the lock screen so users can obtain relevant information in a timely manner without having to frequently unlock the phone to determine if there are new notifications. However, in many cases, these notifications can contain sensitive information. When they are available on the lock screen, an adversary can see them merely by being in close physical proximity to the device. Configuring the mobile operating system to not send notifications to the lock screen mitigates this risk.

```
SFRID: FMT_SMF.1.1 #18
```

Audit:

Review configuration settings to confirm "Show Today view in Lock screen" is disabled.

This check procedure is performed on both the Apple iOS/iPadOS management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the Apple iOS/iPadOS management tool, verify "Show Today view in Lock screen" is unchecked.

Alternatively, verify the text `<key>allowLockScreenTodayView</key><false/>` appears in the configuration profile (`.mobileconfig` file).

On the iPhone and iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap "Profiles & Device Management" or Profiles".
4. Tap the Configuration Profile from the iOS management tool containing the management policy.
5. Tap "Restrictions".

6. Verify "Today view on lock screen not allowed" is present.

If "Show Today view in Lock screen" is checked in the Apple iOS/iPadOS management tool, `<key>allowLockScreenTodayView</key><true/>` appears in the configuration profile, or the restrictions policy on the iPhone and iPad does not list "Today view on lock screen not allowed", this is a finding.

Remediation:

Install a configuration profile to disable "Show Today view in Lock screen" from the device Lock screen.

Additional Information:

CCI-000060

Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

- NIST SP 800-53::AC-11 (1)
- NIST SP 800-53A::AC-11 (1).1
- NIST SP 800-53 Revision 4::AC-11 (1)
- NIST SP 800-53 Revision 5::AC-11 (1)

1.19 AIOS-18-008400 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Apple iOS/iPadOS 18 must be configured to display the DOD advisory warning message at startup or each time the user unlocks the device.

```
GROUP ID: V-268007
RULE ID: SV-268007r1031187
```

Rationale:

Before granting access to the system, the mobile operating system is required to display the DOD-approved system use notification message or banner that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Required banners help ensure that DOD can audit and monitor the activities of mobile device users without legal restriction.

System use notification messages can be displayed when individuals first access or unlock the mobile device. The banner must be implemented as a "click-through" banner at device unlock (to the extent permitted by the operating system). A "click-through" banner prevents further activity on the information system unless and until the user executes a positive action to manifest agreement by clicking on a box indicating "OK".

The approved DOD text must be used exactly as required in the Knowledge Service referenced in DODI 8500.01. For devices accommodating banners of 1300 characters, the banner text is:

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions: -The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. -At any time, the USG may inspect and seize data stored on this IS. -Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose. -This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy. -Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

For devices with severe character limitations, the banner text is:

I've read & consent to terms in IS user agreem't.

The administrator must configure the banner text exactly as written without any changes.

```
SFRID: FMT_SMF.1.1 #36
```

Audit:

The DOD warning banner can be displayed by either of the following methods (required text is found in the Vulnerability Discussion):

1. By placing the DOD warning banner text in the user agreement signed by each iPhone and iPad user.
2. By installing a Lock Screen Message payload with the required text (preferred method).

Determine which method is used at the iOS device site and follow the appropriate validation procedure below.

Validation Procedure for Method #1:

Review the signed user agreements for several iOS device users and verify the agreement includes the required DOD warning banner text.

Validation Procedure for Method #2:

In the Apple iOS/iPadOS management tool, verify a Lock Screen Message payload has been installed on each managed device. The LockScreenFootnote string should include required text.

If, for Method #1, the required warning banner text is not on all signed user agreements reviewed, or for Method #2, the DOD warning banner text is not set as the lock screen footnote, this is a finding.

Remediation:

Configure the DOD warning banner by either of the following methods (required text is found in the Vulnerability Discussion):

1. By placing the DOD warning banner text in the user agreement signed by each iOS device user.
2. By installing a Lock Screen Message payload with the required text (preferred method).

Additional Information:

CCI-000048

Display an organization-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

- NIST SP 800-53::AC-8 a
- NIST SP 800-53A::AC-8.1 (ii)
- NIST SP 800-53 Revision 4::AC-8 a
- NIST SP 800-53 Revision 5::AC-8 a

1.20 AIOS-18-009200 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must be configured to not allow backup of [all applications, configuration data] to locally connected systems.

```
GROUP ID: V-268013
RULE ID: SV-268013r1117267
```

Rationale:

Data on mobile devices is protected by numerous mechanisms, including user authentication, access control, and cryptography. When the data is backed up to an external system (either locally connected or cloud based), many if not all of these mechanisms are no longer present. This leaves the backed-up data vulnerable to attack. Disabling backup to external systems mitigates this risk.

```
SFRID: FMT_SMF.1.1 #40
```

Audit:

Review configuration settings to confirm backup in management apps is disabled and "Encrypt local backup" is enabled in iTunes (for Windows computer) and in Finder on Mac.

Note: iTunes Backup/Finder backup is implemented by the configuration policy rule "Force encrypted backups", which is included in AIOS-18-010700 and therefore not included in the procedure below.

This check procedure is performed on both the Apple iOS/iPadOS management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the Apple iOS/iPadOS management tool, verify backing up app data is disabled.

On the iPhone and iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the Apple iOS/iPadOS management tool containing the restrictions policy.
5. Tap "Apps".

6. Tap a managed app.
7. Verify "App data will not be backed up" is listed.

Note: Steps 6 and 7 must be performed for each managed app.

If backing up app data is not disabled in the Apple iOS/iPadOS management tool or "app data will not be backed up" is not listed for each managed app on the iPhone and iPad, this is a finding.

Remediation:

Install a configuration profile to disable backup of managed apps.

Additional Information:

CCI-001090

Prevent unauthorized and unintended information transfer via shared system resources.

- NIST SP 800-53::SC-4
- NIST SP 800-53A::SC-4.1
- NIST SP 800-53 Revision 4::SC-4
- NIST SP 800-53 Revision 5::SC-4

1.21 AIOS-18-009700 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must not allow non-DOD applications to access DOD data.

```
GROUP ID: V-268017
RULE ID: SV-268017r1117274
```

Rationale:

App data sharing gives apps the ability to access the data of other apps for enhanced user functionality. However, sharing also poses a significant risk that unauthorized users or apps will obtain access to sensitive DOD information. To mitigate this risk, there are data sharing restrictions. If a user is allowed to make exceptions to the data sharing restriction policy, the user could enable unauthorized sharing of data, leaving it vulnerable to breach. Limiting the granting of exceptions to either the administrator or common application developer mitigates this risk.

Copy/paste of data between applications in different application processes or groups of application processes is considered an exception to the access control policy; therefore, the administrator must be able to enable/disable the feature. Other exceptions include allowing any data or application sharing between process groups.

```
SFRID: FMT_SMF.1.1 #42, FDP_ACF_EXT.1.2
```

Audit:

Review configuration settings to confirm "Allow documents from managed apps in unmanaged apps" is disabled.

This check procedure is performed on both the Apple iOS/iPadOS management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS management tool, verify "Allow documents from managed apps in unmanaged apps" is unchecked.

Alternatively, verify the text `<key>allowOpenFromManagedToUnmanaged</key><false/>` appears in the configuration profile (`.mobileconfig` file).

On the iOS device:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "Opening documents from managed to unmanaged apps not allowed" is listed.

If "Allow documents from managed apps in unmanaged apps" is checked in the iOS management tool, `<key>allowOpenFromManagedToUnmanaged</key><true/>` appears in the configuration profile, or the restrictions policy on the iPhone and iPad does not list "Opening documents from managed to unmanaged apps not allowed", this is a finding.

Remediation:

Install a configuration profile to prevent non-DOD applications from accessing DOD data.

Additional Information:

CCI-002530

Maintain a separate execution domain for each executing system process.

- NIST SP 800-53 Revision 4::SC-39
- NIST SP 800-53 Revision 5::SC-39

CCI-002233

Prevent the organization-defined software from executing at higher privilege levels than users executing the software.

- NIST SP 800-53 Revision 4::AC-6 (8)
- NIST SP 800-53 Revision 5::AC-6 (8)

1.22 AIOS-18-009800 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iPadOS 18 must be configured to disable multiuser modes.

```
GROUP ID: V-268018
RULE ID: SV-268018r1031198
```

Rationale:

Multiuser mode allows multiple users to share a mobile device by providing a degree of separation between user data. To date, no mobile device with multiuser mode features meets DOD requirements for access control, data separation, and nonrepudiation for user accounts. In addition, the MDFPP does not include design requirements for multiuser account services. Disabling multiuser mode mitigates the risk of not meeting DOD multiuser account security policies.

```
SFRID: FMT_SMF.1.1 #47a
```

Audit:

Verify multiuser mode (shared iPad) is disabled in the MDM console for iPadOS devices. This requirement is not applicable for iOS devices.

If multiuser mode is not disabled in the MDM console for iPadOS devices, this is a finding.

Remediation:

Disable multiuser mode (shared iPad) in the MDM console for iPadOS devices.

Additional Information:

CCI-002110

The organization defines the information system account types that support the organizational missions/business functions.

- NIST SP 800-53 Revision 4::AC-2 a

1.23 AIOS-18-009900 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must be configured to [selection: wipe protected data, wipe sensitive data] upon unenrollment from MDM.

```
GROUP ID: V-268019
RULE ID: SV-268019r1031199
```

Rationale:

When a mobile device is no longer going to be managed by MDM technologies, its protected/sensitive data must be sanitized because it will no longer be protected by the MDM software, putting it at much greater risk of unauthorized access and disclosure. At least one of the two options must be selected.

```
SFRID: FMT_SMF_EXT.2.1
```

Audit:

Note: Not all Apple iOS/iPadOS deployments involve MDM. If the site uses an authorized alternative to MDM for distribution of configuration profiles (Apple Configurator), this check procedure is not applicable.

This check procedure is performed on the Apple iOS/iPadOS management tool or on the iOS device.

In the Apple iOS/iPadOS management tool, for each managed app, verify the app is configured to be removed when the MDM profile is removed.

On the iPhone and iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the management policy.
5. Tap "Apps".
6. Tap an app and verify "App and data will be removed when device is no longer managed" is listed.

Repeat steps 5 and 6 for each managed app in the list.

If one or more managed apps are not set to be removed upon device MDM unenrollment, this is a finding.

Remediation:

Install a configuration profile to delete all managed apps upon device unenrollment.

Additional Information:

CCI-001033

Defines circumstances requiring sanitization of portable storage devices prior to connecting such devices to the system.

- NIST SP 800-53::MP-6 (3)
- NIST SP 800-53A::MP-6 (3).1 (i)
- NIST SP 800-53 Revision 4::MP-6 (3)
- NIST SP 800-53 Revision 5::MP-6 (3)

1.24 AIOS-18-010000 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must be configured to [selection: remove Enterprise applications, remove all noncore applications (any nonfactory-installed application)] upon unenrollment from MDM.

```
GROUP ID: V-268020
RULE ID: SV-268020r1031200
```

Rationale:

When a mobile device is no longer going to be managed by MDM technologies, its protected/sensitive data must be sanitized because it will no longer be protected by the MDM software, putting it at much greater risk of unauthorized access and disclosure. At least one of the two options must be selected.

```
SFRID: FMT_SMF_EXT.2.1
```

Audit:

Note: Not all Apple iOS/iPadOS deployments involve MDM. If the site uses an authorized alternative to MDM for distribution of configuration profiles (Apple Configurator), this check procedure is not applicable.

This check procedure is performed on the Apple iOS/iPadOS management tool or on the iOS device.

In the Apple iOS/iPadOS management tool, for each managed app, verify the app is configured to be removed when the MDM profile is removed.

On the iPhone and iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the management policy.
5. Tap "Apps".
6. Tap an app and verify "App and data will be removed when device is no longer managed" is listed.

Repeat steps 5 and 6 for each managed app in the list.

If one or more managed apps are not set to be removed upon device MDM unenrollment, this is a finding.

Remediation:

Install a configuration profile to delete all managed apps upon device unenrollment.

Additional Information:

CCI-001033

Defines circumstances requiring sanitization of portable storage devices prior to connecting such devices to the system.

- NIST SP 800-53::MP-6 (3)
- NIST SP 800-53A::MP-6 (3).1 (i)
- NIST SP 800-53 Revision 4::MP-6 (3)
- NIST SP 800-53 Revision 5::MP-6 (3)

1.25 AIOS-18-010200 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must be configured to disable ad hoc wireless client-to-client connection capability.

```
GROUP ID: V-268022
RULE ID: SV-268022r1115587
```

Rationale:

Ad hoc wireless client-to-client connections allow mobile devices to communicate with each other directly, circumventing network security policies and making the traffic invisible. This could allow the exposure of sensitive DOD data and increase the risk of downloading and installing malware on the DOD mobile device.

```
SFRID: FMT_SMF_EXT.1.1/WLAN
```

Audit:

Review configuration settings to confirm AirDrop is disabled.

This is a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding.

If the iPhone or iPad being reviewed is supervised by the MDM, follow these procedures:

This check procedure is performed on both the device management tool and the iPhone and iPad device.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS/iPadOS management tool, verify "Allow AirDrop" is unchecked.

On the iPhone/iPad device:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "AirDrop not allowed" is listed.

If "AirDrop not allowed" is not listed in the management tool and on the Apple device, this is a finding.

Remediation:

Install a configuration profile to disable the AllowAirDrop control in the management tool. This is a supervised-only control.

Additional Information:

CCI-002536

Protect organization-defined external and internal wireless links from organization-defined types of signal parameter attacks or references to sources for such attacks.

- NIST SP 800-53 Revision 4::SC-40
- NIST SP 800-53 Revision 5::SC-40

1.26 AIOS-18-010400 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Apple iOS/iPadOS 18 must require a valid password be successfully entered before the mobile device data is unencrypted.

```
GROUP ID: V-268024
RULE ID: SV-268024r1031204
```

Rationale:

Passwords provide a form of access control that prevents unauthorized individuals from accessing computing resources and sensitive data. Passwords may also be a source of entropy for generation of key encryption or data encryption keys. If a password is not required to access data, this data is accessible to any adversary who obtains physical possession of the device. Requiring that a password be successfully entered before the mobile device data is unencrypted mitigates this risk.

Note: MDF PP requires a Password Authentication Factor and requires management of its length and complexity. It leaves open whether the existence of a password is subject to management. This requirement addresses the configuration to require a password, which is critical to the cybersecurity posture of the device.

```
SFRID: FIA_UAU_EXT.1.1
```

Audit:

Review configuration settings to confirm the device is set to require a passcode before use.

This procedure is performed on the iOS and iPadOS device.

On the iPhone and iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the password policy.
5. Tap "Restrictions".
6. Tap "Passcode".
7. Verify "Passcode required" is set to "Yes".

If "Passcode required" is not set to "Yes", this is a finding.

Remediation:

Install a configuration profile to require a password to unlock the device.

Additional Information:

CCI-001199

Protects the confidentiality and/or integrity of organization-defined information at rest.

- NIST SP 800-53::SC-28
- NIST SP 800-53A::SC-28.1
- NIST SP 800-53 Revision 4::SC-28
- NIST SP 800-53 Revision 5::SC-28

1.27 AIOS-18-010500 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Apple iOS/iPadOS 18 must implement the management setting: limit Ad Tracking.

```
GROUP ID: V-268026
RULE ID: SV-268026r1031206
```

Rationale:

Ad Tracking refers to the advertisers' ability to categorize the device and spam the user with ads that are most relevant to the user's preferences. By not "Force limiting ad tracking", advertising companies are able to gather information about the user and device's browsing habits. If "Limit Ad Tracking" is not limited, a database of browsing habits of DOD devices can be gathered and stored under no supervision of the DOD. Limiting ad tracking does not completely mitigate the risk but does limit the amount of information gathering.

```
SFRID: FMT_SMF.1.1 #47
```

Audit:

Review configuration settings to confirm "Force limited ad tracking" is checked.

This check procedure is performed on both the Apple iOS/iPadOS management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the Apple iOS/iPadOS management tool, verify "Force limited ad tracking" is checked.

Alternatively, verify the text `<key>forceLimitAdTracking</key><true/>` appears in the configuration profile (`.mobileconfig` file).

On the iPhone and iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the management policy.
5. Tap "Restrictions".

6. Verify "Limit ad tracking enforced" or "Requests to track from apps not allowed" is present.

If "limited ad tracking enforced" is missing in the Apple iOS/iPadOS management tool, `<key>forceLimitAdTracking</key><false/>` does not appear in the configuration profile, or the restrictions policy on the iPhone and iPad does not list "Limit ad tracking enforced", this is a finding.

Remediation:

Install a configuration profile to limit advertisers' ability to track the user's web browsing preferences.

Additional Information:

CCI-001199

Protects the confidentiality and/or integrity of organization-defined information at rest.

- NIST SP 800-53::SC-28
- NIST SP 800-53A::SC-28.1
- NIST SP 800-53 Revision 4::SC-28
- NIST SP 800-53 Revision 5::SC-28

1.28 AIOS-18-010600 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Apple iOS/iPadOS 18 must implement the management setting: not allow automatic completion of Safari browser passcodes.

```
GROUP ID: V-268027
RULE ID: SV-268027r1031207
```

Rationale:

The AutoFill functionality in the Safari web browser allows the user to complete a form that contains sensitive information, such as PII, without previous knowledge of the information. By allowing the use of the AutoFill functionality, an adversary who learns a user's iPhone or iPad passcode, or who otherwise is able to unlock the device, may be able to further breach other systems by relying on the AutoFill feature to provide information unknown to the adversary. By disabling the AutoFill functionality, the risk of an adversary gaining additional information about the device's user or compromising other systems is significantly mitigated.

```
SFRID: FMT_SMF.1.1 #47
```

Audit:

Review configuration settings to confirm "Enable autofill" is unchecked.

This check procedure is performed on both the Apple iOS/iPadOS management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the Apple iOS/iPadOS management tool, verify "Enable autofill" is unchecked.

Alternatively, verify the text `<key>safariAllowAutoFill</key><false>` appears in the configuration profile (`.mobileconfig` file).

On the iPhone and iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the management policy.
5. Tap "Restrictions".

6. Verify "Auto-fill in Safari not allowed" is present.

If "Enable autofill" is checked in the Apple iOS/iPadOS management tool, `<key>safariAllowAutoFill</key><true>` appears in the configuration profile, or the restrictions policy on the iPhone and iPad does not list "Auto-fill in Safari not allowed", this is a finding.

Remediation:

Install a configuration profile to disable the AutoFill capability in the Safari app.

Additional Information:

CCI-000381

Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

1.29 AIOS-18-010700 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must implement the management setting: encrypt backups/Encrypt local backup.

```
GROUP ID: V-268028
RULE ID: SV-268028r1031208
```

Rationale:

If iCloud backups are not encrypted, this could lead to the unauthorized disclosure of DOD sensitive information if non-DOD personnel are able to access that machine. Forcing the backup to be encrypted greatly mitigates the risk of compromising sensitive data. Work data iCloud backup and USB connections to computers are not authorized, but this control provides defense-in-depth for cases in which a user violates policy either intentionally or inadvertently.

```
SFRID: FMT_SMF.1.1 #47
```

Audit:

Review configuration settings to confirm "Force encrypted backups" is enabled.

This check procedure is performed on both the Apple iOS/iPadOS management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the Apple iOS/iPadOS management tool, verify "Encrypt local backup" is checked.

Alternatively, verify the text `<key>forceEncryptedBackup</key><true/>` appears in the configuration profile (.mobileconfig file).

On the iPhone and iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the Apple iOS/iPadOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "Encrypt backups enforced" is listed.

If "Encrypt local backup" is unchecked in the Apple iOS/iPadOS management tool, `<key>forceEncryptedBackup</key><false/>` appears in the configuration profile, or the restrictions policy on the iPhone and iPad does not list "Encrypt backups enforced", this is a finding.

Remediation:

Install a configuration profile to force encrypted backups to iCloud.

Additional Information:

CCI-000381

Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

1.30 AIOS-18-010800 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Apple iOS/iPadOS 18 must implement the management setting: not allow use of Handoff.

```
GROUP ID: V-268029
RULE ID: SV-268029r1031209
```

Rationale:

Handoff permits a user of an iPhone and iPad to transition user activities from one device to another. Handoff passes sufficient information between the devices to describe the activity, but app data synchronization associated with the activity is handled though iCloud, which should be disabled on a compliant iPhone and iPad. If a user associates both DOD and personal devices to the same Apple ID, the user may improperly reveal information about the nature of the user's activities on an unprotected device. Disabling Handoff mitigates this risk.

```
SFRID: FMT_SMF.1.1 #47
```

Audit:

This is a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding.

If the iPhone or iPad being reviewed is supervised by the MDM, review configuration settings to confirm "Allow Handoff" is disabled.

This check procedure is performed on both the Apple iOS/iPadOS management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the Apple iOS/iPadOS management tool, verify "Allow Handoff" is unchecked.

Alternatively, verify the text `<key>allowActivityContinuation</key> <false/>` appears in the configuration profile (`.mobileconfig` file).

On the iPhone and iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".

4. Tap the Configuration Profile from the Apple iOS/iPadOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "Handoff not allowed" is listed.

If "Allow Handoff" is checked in the Apple iOS/iPadOS management tool, `<key>allowActivityContinuation</key> <true/>` appears in the configuration profile, or the restrictions policy on the iPhone and iPad does not list "Handoff not allowed", this is a finding.

Remediation:

Install a configuration profile to disable continuation of activities among devices and workstations. This a supervised-only control.

Additional Information:

CCI-000381

Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

1.31 AIOS-18-010850 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Apple iOS/iPadOS 18 must implement the management setting: not allow use of iPhone widgets on Mac.

```
GROUP ID: V-268030
RULE ID: SV-268030r1031210
```

Rationale:

iPhone widgets on Mac use Handoff. Handoff permits a user of an iPhone and iPad to transition user activities from one device to another. Handoff passes sufficient information between the devices to describe the activity, but app data synchronization associated with the activity is handled though iCloud, which should be disabled on a compliant iPhone and iPad. If a user associates both DOD and personal devices to the same Apple ID, the user may improperly reveal information about the nature of the user's activities on an unprotected device. Disabling Handoff mitigates this risk.

```
SFRID: FMT_SMF.1.1 #47
```

Audit:

Review configuration settings to confirm "Allow iPhone Widget on Mac" is disabled.

This a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding.

This check procedure is performed only on the Apple iOS/iPadOS management tool.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the Apple iOS/iPadOS management tool, verify "iPhone Widget on Mac" is unchecked.

If "Allow iPhone Widget on Mac" is checked in the Apple iOS/iPadOS management tool, this is a finding.

Remediation:

Install a configuration profile to disable the installation of iPhone widgets on Mac. This a supervised-only control.

Additional Information:

CCI-000381

Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

1.32 AIOS-18-010900 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Apple iOS/iPadOS 18 must implement the management setting: require the user to enter a password when connecting to an AirPlay-enabled device.

```
GROUP ID: V-268031
RULE ID: SV-268031r1031211
```

Rationale:

When a user is allowed to use AirPlay without a password, it may mistakenly associate the iPhone and iPad with an AirPlay-enabled device other than the one intended (i.e., by choosing the wrong one from the AirPlay list displayed). This creates the potential for someone in control of a mistakenly associated device to obtain DOD sensitive information without authorization. Requiring a password before such an association mitigates this risk. Passwords do not require any administration and are not required to comply with any complexity requirements.

```
SFRID: FMT_SMF.1.1 #40
```

Audit:

Review configuration settings to confirm "Require passcode on outgoing AirPlay request" is enabled.

This check procedure is performed on both the Apple iOS/iPadOS management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the Apple iOS/iPadOS management tool, verify "Require passcode on outgoing AirPlay request" is checked.

Alternatively, verify the text `<key>forceAirPlayOutgoingRequestsPairingPassword</key><false/>` appears in the configuration profile (`.mobileconfig` file).

On the iPhone and iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the Apple iOS/iPadOS management tool containing the restrictions policy.

5. Tap "Restrictions".
6. Verify "AirPlay outgoing requests pairing password enforced" is listed.

If "Require passcode on outgoing AirPlay request" is unchecked in the Apple iOS/iPadOS management tool, `<key>forceAirPlayOutgoingRequestsPairingPassword</key><true/>` appears in the configuration profile, or the restrictions policy on the iPhone and iPad does not list "AirPlay outgoing requests pairing password enforced", this is a finding.

Remediation:

Install a configuration profile to require the user to enter a password when connecting to an AirPlay-enabled device.

Additional Information:

CCI-000067

Employ automated mechanisms to monitor remote access methods.

- NIST SP 800-53::AC-17 (1)
- NIST SP 800-53A::AC-17 (1).1
- NIST SP 800-53 Revision 4::AC-17 (1)
- NIST SP 800-53 Revision 5::AC-17 (1)

1.33 AIOS-18-010950 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Apple iOS/iPadOS 18 must implement the management setting: require passcode for incoming Airplay connection requests.

```
GROUP ID: V-268032
RULE ID: SV-268032r1031212
```

Rationale:

When an incoming AirPlay request is allowed without a password, it may mistakenly associate the iPhone and iPad with an AirPlay-enabled device other than the one intended (i.e., by choosing the wrong one from the AirPlay list displayed). This creates the potential for someone in control of a mistakenly associated device to obtain DOD sensitive information without authorization. Requiring a password before such an association mitigates this risk. Passwords do not require any administration and are not required to comply with any complexity requirements.

```
SFRID: FMT_SMF.1.1 #40
```

Audit:

Review configuration settings to confirm "Require passcode for incoming AirPlay connection requests" is enabled.

This check procedure is performed on both the Apple iOS/iPadOS management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the Apple iOS/iPadOS management tool, verify "Require passcode for incoming AirPlay connection requests" is checked.

On the iPhone and iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the Apple iOS/iPadOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "AirPlay incoming requests pairing password enforced" is listed.

If "Require passcode for incoming AirPlay connection requests" is unchecked in the Apple iOS/iPadOS management tool or the restrictions policy on the iPhone and iPad does not list "AirPlay incoming requests pairing password enforced", this is a finding.

Remediation:

Install a configuration profile to require that incoming AirPlay connection requests enter a password when connecting to a DOD iOS/iPadOS device.

Additional Information:

CCI-000067

Employ automated mechanisms to monitor remote access methods.

- NIST SP 800-53::AC-17 (1)
- NIST SP 800-53A::AC-17 (1).1
- NIST SP 800-53 Revision 4::AC-17 (1)
- NIST SP 800-53 Revision 5::AC-17 (1)

1.34 AIOS-18-011000 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must implement the management setting: disable Allow MailDrop.

```
GROUP ID: V-268033
RULE ID: SV-268033r1031213
```

Rationale:

MailDrop allows users to send large attachments (up to 5 GB) via iCloud. Storing data with a non-DOD cloud provider may leave the data vulnerable to breach. Disabling non-DOD cloud services mitigates this risk.

```
SFRID: FMT_SMF.1.1 #47
```

Audit:

Review configuration settings to confirm "Allow MailDrop" is disabled.

This validation procedure is performed on both the Apple iOS/iPadOS management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the Apple iOS/iPadOS management tool, verify "Allow MailDrop" is not checked.

On the iPhone and iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the Apple iOS/iPadOS management tool containing the restrictions policy.
5. Tap "Mail".
6. Tap the mail account.
7. Verify "Mail Drop Enabled" is set to "No".

If "Allow MailDrop" is not disabled in the Apple iOS/iPadOS management tool or the restrictions policy on the iPhone and iPad lists "Mail Drop Enabled" as "Yes", this is a finding.

Remediation:

Configure the Apple iOS/iPadOS configuration profile to disable "Allow MailDrop".

Additional Information:

CCI-002314

Employ automated mechanisms to control remote access methods.

- NIST SP 800-53 Revision 4::AC-17 (1)
- NIST SP 800-53 Revision 5::AC-17 (1)

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

1.35 AIOS-18-011200 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

iPhone and iPad must have the latest available iOS/iPadOS operating system installed.

```
GROUP ID: V-268034
RULE ID: SV-268034r1031214
```

Rationale:

Required security features are not available in earlier OS versions. In addition, earlier versions may have known vulnerabilities.

```
SFRID: FMT_SMF.1.1 #47
```

Audit:

Review configuration settings to confirm the most recently released version of iOS is installed.

This validation procedure is performed on both the Apple iOS/iPadOS management tool and the iPhone and iPad. Go to https://www.apple.com and determine the most current version of iOS released by Apple.

In the MDM management console, review the version of iOS installed on a sample of managed devices. This procedure will vary depending on the MDM product.

On the iPhone and iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap "About" and view the installed version of iOS.
4. Go back to the "General" screen. Tap "Software Update" and verify the following message is shown on the screen: "Your software is up to date."

If the installed version of iOS on any reviewed iOS/iPadOS devices is not the latest released by Apple, this is a finding.

Remediation:

Install the latest release version of Apple iOS/iPadOS on all managed iOS devices.

Additional Information:

CCI-000381

Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

1.36 AIOS-18-011300 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must implement the management setting: use SSL for Exchange ActiveSync.

```
GROUP ID: V-268035
RULE ID: SV-268035r1031215
```

Rationale:

Exchange email messages are a form of data in transit and thus are vulnerable to eavesdropping and man-in-the-middle attacks. Secure Sockets Layer (SSL), also referred to as Transport Layer Security (TLS), provides encryption and authentication services that mitigate the risk of breach.

```
SFRID: FMT_SMF.1.1 #47
```

Audit:

Review configuration settings to confirm "Use SSL" for the Exchange account is enabled for incoming mail.

This check procedure is performed on both the Apple iOS/iPadOS management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the Apple iOS/iPadOS management tool, verify "Use SSL for incoming mail" is checked under the Exchange payload.

On the iPhone and iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the Apple iOS/iPadOS management tool containing the Exchange policy.
5. Tap "Mail".
6. Tap the name of the Exchange account.
7. Verify "SSL for incoming mail" is set to "Yes".

If "Use SSL for incoming mail" is unchecked in the Apple iOS/iPadOS management tool or the Exchange policy on the iPhone and iPad has "SSL for incoming mail" set to "No", this is a finding.

Remediation:

Install a configuration profile to use SSL for Exchange ActiveSync incoming mail.

Additional Information:

CCI-000764

Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

- NIST SP 800-53::IA-2
- NIST SP 800-53A::IA-2.1
- NIST SP 800-53 Revision 4::IA-2
- NIST SP 800-53 Revision 5::IA-2

1.37 AIOS-18-011400 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must implement the management setting: not allow messages in an ActiveSync Exchange account to be forwarded or moved to other accounts in the Apple iOS/iPadOS 18 Mail app.

```
GROUP ID: V-268036
RULE ID: SV-268036r1031216
```

Rationale:

The Apple iOS/iPadOS Mail app can be configured to support multiple email accounts concurrently. These email accounts are likely to involve content of varying degrees of sensitivity (e.g., both personal and enterprise messages). To prevent the unauthorized and undetected forwarding or moving of messages from one account to another, Mail ActiveSync Exchange accounts can be configured to block such behavior. While users may still send a message from the Exchange account to another account, these transactions must involve an Exchange server, enabling audit records of the transaction, filtering of mail content, and subsequent forensic analysis.

```
SFRID: FMT_SMF.1.1 #47
```

Audit:

Review configuration settings to confirm "Allow messages to be moved" is disabled.

This check procedure is performed on both the Apple iOS/iPadOS management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the Apple iOS/iPadOS management tool, verify "Allow messages to be moved" is unchecked under the Exchange payload.

On the iPhone and iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the Apple iOS/iPadOS management tool containing the Exchange policy.
5. Tap "Mail".
6. Tap the name of the Exchange account.

7. Verify "Prevent Move" is set to "Yes".

If "Allow messages to be moved" is checked in the Apple iOS/iPadOS management tool or the Exchange policy on the iPhone and iPad has "Prevent Move" set to "No", this is a finding.

Remediation:

Install a configuration profile to prevent Exchange messages from being moved or forwarded between email accounts.

Additional Information:

CCI-000764

Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

- NIST SP 800-53::IA-2
- NIST SP 800-53A::IA-2.1
- NIST SP 800-53 Revision 4::IA-2
- NIST SP 800-53 Revision 5::IA-2

1.38 AIOS-18-011500 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must implement the management setting: treat AirDrop as an unmanaged destination.

```
GROUP ID: V-268037
RULE ID: SV-268037r1031217
```

Rationale:

AirDrop is a way to send contact information or photos to other users with AirDrop enabled. This feature enables a possible attack vector for adversaries to exploit. Once the attacker has gained access to the information broadcast by this feature, the attacker may distribute this sensitive information very quickly and without DOD's control or awareness. By disabling this feature, the risk of mass data exfiltration will be mitigated.

Note: If the site uses Apple's optional Automatic Device Enrollment, this control is available as a supervised MDM control.

```
SFRID: FMT_SMF.1.1 #47
```

Audit:

Review configuration settings to confirm "Treat AirDrop as an unmanaged destination" is enabled.

This check procedure is performed on both the Apple iOS/iPadOS management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the Apple iOS/iPadOS management tool, verify "Treat AirDrop as unmanaged destination" is checked.

On the iPhone and iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "Sharing managed documents using AirDrop not allowed" is listed.

If "Treat AirDrop as unmanaged destination" is disabled in the Apple iOS/iPadOS management tool or the restrictions policy on the iPhone and iPad does not list "Sharing managed documents using AirDrop not allowed", this is a finding.

Remediation:

Install a configuration profile to treat AirDrop as an unmanaged destination.

Additional Information:

CCI-002007

Prohibit the use of cached authenticators after an organization-defined time period.

- NIST SP 800-53 Revision 4::IA-5 (13)
- NIST SP 800-53 Revision 5::IA-5 (13)

1.39 AIOS-18-011600 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Apple iOS/iPadOS 18 must implement the management setting: not have any Family Members in Family Sharing.

```
GROUP ID: V-268038
RULE ID: SV-268038r1031218
```

Rationale:

Apple's Family Sharing service allows Apple iOS/iPadOS users to create a Family Group whose members have several shared capabilities, including the ability to lock, wipe, play a sound on, or locate the iPhone and iPads of other members. Each member of the group must be invited to the group and accept that invitation. A DOD user's iPhone and iPad may be inadvertently or maliciously wiped by another member of the Family Group. This poses a risk that the user could be without a mobile device for a period of time or lose sensitive information that has not been backed up to other storage media. Configuring iPhone and iPads so their associated Apple IDs are not members of Family Groups mitigates this risk.

Note: If the site uses Apple's optional Automatic Device Enrollment, this control is available as a supervised MDM control.

```
SFRID: FMT_SMF.1.1 #47
```

Audit:

Review configuration settings to confirm Family Sharing is disabled. Note that this is a User-Based Enforcement (UBE) control, which cannot be managed by an MDM server.

This check procedure is performed on the iPhone and iPad.

On the iPhone and iPad:

1. Open the Settings app.
2. At the top of the screen, if "Sign in to your iPhone" is listed, this requirement has been met.
3. If the user profile is signed into iCloud, tap the username.
4. Tap "Family Sharing".
5. Verify no accounts are listed other than the "Organizer".

Note: The iPhone and iPad must be connected to the internet to conduct this validation procedure. Otherwise, the device will display the notice "Family information is not available", in which case configuration compliance cannot be determined.

If accounts (names or email addresses) are listed under "FAMILY MEMBERS" on the iPhone and iPad, this is a finding.

Remediation:

The user must either remove all members from the Family Group on the iPhone and iPad or associate the device with an Apple ID that is not a member of a Family Group.

Additional Information:

CCI-002007

Prohibit the use of cached authenticators after an organization-defined time period.

- NIST SP 800-53 Revision 4::IA-5 (13)
- NIST SP 800-53 Revision 5::IA-5 (13)

1.40 AIOS-18-011700 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must implement the management setting: not share location data through iCloud.

```
GROUP ID: V-268039
RULE ID: SV-268039r1031219
```

Rationale:

Sharing of location data is an operational security (OPSEC) risk because it potentially allows an adversary to determine a DOD user's location, movements, and patterns in those movements over time. An adversary could use this information to target the user or gather intelligence on the user's likely activities. Using commercial cloud services to store and handle location data could leave the data vulnerable to breach, particularly by sophisticated adversaries. Disabling the use of such services mitigates this risk.

```
SFRID: FMT_SMF.1.1 #47
```

Audit:

Review configuration settings to confirm "Share My Location" is disabled. Note that this is a User-Based Enforcement (UBE) control, which cannot be managed by an MDM server.

This check procedure is performed on the iPhone and iPad only.

On the iPhone and iPad:

1. Open the Settings app.
2. Tap "Privacy & Security".
3. Tap "Location Services".
4. If the authorizing official (AO) has not approved use of personal iCloud accounts on the device, verify "Share My Location" is grayed out (cannot be selected).
5. If the AO has approved the use of personal iCloud accounts on the device, tap "Share My Location".
6. Verify "Share My Location" is off.

If "Share My Location" is not grayed out (cannot be selected) when the AO has not approved use of personal iCloud accounts on the device, this is a finding.

If "Share My Location" is toggled to the right and appears green on the iPhone and iPad when the AO has approved the use of personal iCloud accounts, this is a finding.

Remediation:

The user must configure Apple iOS/iPadOS to disable location sharing through iCloud.

Additional Information:

CCI-000048

Display an organization-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

- NIST SP 800-53::AC-8 a
- NIST SP 800-53A::AC-8.1 (ii)
- NIST SP 800-53 Revision 4::AC-8 a
- NIST SP 800-53 Revision 5::AC-8 a

1.41 AIOS-18-011800 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Apple iOS/iPadOS 18 must implement the management setting: force Apple Watch wrist detection.

```
GROUP ID: V-268040
RULE ID: SV-268040r1031220
```

Rationale:

Because Apple Watch is a personal device, it is key that any sensitive DOD data displayed on the Apple Watch cannot be viewed when the watch is not in the immediate possession of the user. This control ensures the Apple Watch screen locks when the user takes the watch off, thereby protecting sensitive DOD data from possible exposure.

```
SFRID: FMT_SMF.1.1 #47
```

Audit:

Review configuration settings to confirm "Force Apple Watch wrist detection" is enabled.

This check procedure is performed on both the Apple iOS/iPadOS management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the Apple iOS/iPadOS management tool, verify "Wrist detection enforced on Apple Watch" is enforced.

On the iPhone and iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the Apple iOS/iPadOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "Wrist detection enforced on Apple Watch" is listed.

If "Wrist detection enforced on Apple Watch" is not enforced in the Apple iOS/iPadOS management tool or the restrictions policy on the iPhone and iPad does not list "Wrist detection enforced on Apple Watch", this is a finding.

Remediation:

Install a configuration profile to force Apple Watch wrist detection.

Additional Information:

CCI-000381

Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

1.42 AIOS-18-011900 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 users must complete required training.

```
GROUP ID: V-268041
RULE ID: SV-268041r1031221
```

Rationale:

The security posture on iOS devices requires the device user to configure several required policy rules on their device. User-Based Enforcement (UBE) is required for these controls. In addition, if the authorizing official (AO) has approved users' full access to the Apple App Store, users must receive training on risks. If a user is not aware of their responsibilities and does not comply with UBE requirements, the security posture of the iOS mobile device and DOD sensitive data may become compromised.

```
SFRID: NA
```

Audit:

Review a sample of site User Agreements for iOS device users or similar training records and training course content. Verify iPhone and iPad users have completed required training.

If any iPhone/iPad user has not completed required training, this is a finding.

Remediation:

Have all iPhone and iPad users complete training on the following topics. Users must acknowledge receipt of training via a signed User Agreement or similar written record.

Training topics:

- Operational security concerns introduced by unmanaged applications, including applications using global positioning system (GPS) tracking.
- Must ensure no DOD data is saved in an unmanaged app or transmitted from a personal app (for example, from personal email).
- If the Purebred key management app is used, users are responsible for maintaining positive control of their credentialed device at all times. 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 mobility service provider decommissioning procedures as applicable.

- How to configure the following UBE controls (users must configure the control) and other controls on the iPhone and iPad:
    - Remove Family Sharing.
    - Disable Shared Location.
    - Disable Wi-Fi Assist.
    - Use AirPrint only with AO-approved printers and print servers (see the Multifunction Device and Network Printers STIG for requirements).
    - Turn off "Apps" under "Automatic Downloads" in the "iTunes & App Store" section of the Settings app on the iPhone and iPad.
    - Secure use of Calendar Alarm.
    - Do not configure a DOD network (work) VPN profile on any third-party unmanaged VPN app.
    - Disable iPhone and iPad radios using controls under "Settings" instead of "Control Center".
- AO guidance on acceptable use and restrictions, if any, on downloading and installing personal apps and data (music, photos, etc.).

Additional Information:

CCI-000381

Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

1.43 AIOS-18-012000 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

A managed photo app must be used to take and store work-related photos.

```
GROUP ID: V-268042
RULE ID: SV-268042r1031222
```

Rationale:

The iOS Photos app is unmanaged and may sync photos with a device or user's personal iCloud account. Therefore, work-related photos must not be taken via the iOS camera app or stored in the Photos app. A managed photo app must be used to take and manage work-related photos.

```
SFRID: NA
```

Audit:

Review configuration settings to confirm a managed photos app is installed on the iOS device.

This check procedure is performed on the iPhone and iPad.

On the iPhone and iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the DOD Configuration Profile from the Apple iOS/iPadOS management tool.
5. Tap "Apps".
6. Verify a photo capture and management app is listed.

If a managed photo capture and management app is not installed on the iPhone and iPad, this is a finding.

Remediation:

Install a managed photos app to take and manage work-related photos.

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

1.44 AIOS-18-012200 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must implement the management setting: enable USB Restricted Mode.

```
GROUP ID: V-268044
RULE ID: SV-268044r1031224
```

Rationale:

The USB port on an iOS device can be used to access data on the device. The required settings ensure the Apple device password is entered before a previously trusted USB accessory can connect to the device.

```
SFRID: FMT_SMF.1.1 #47
```

Audit:

This is a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding.

If the iPhone or iPad being reviewed is supervised by the MDM, review configuration settings to confirm "Allow USB Restricted Mode" is enabled.

This check procedure is performed on both the device management tool and the iPhone and iPad device.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS management tool, verify "Allow USB Restricted Mode" is checked (set to "True").

On the iPhone/iPad device:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify there is no listing for "USB Accessories while locked allowed".

If "Allow USB Restricted Mode" is not enabled in the management tool and there is a restriction listed in the profile on the Apple device, this is a finding.

Note: The default configuration setting for "allow USB Restricted Mode" is "True" in most MDM products. This is the required setting. When set correctly, nothing will be listed in the Restrictions profile, and the user will be able to toggle USB accessories on/off.

Note: "Allow USB Restricted Mode" may be called "Allow USB accessories while device is locked" in some MDM consoles. The required logic is to disable USB accessory connections when the device is locked.

Remediation:

Install a configuration profile to configure "Allow USB Restricted Mode" to "True" in the management tool. This a supervised-only control.

Note: The default configuration setting for "allow USB Restricted Mode" is "True" in most MDM products. This is the required setting. When set correctly, nothing will be listed in the Restrictions profile, and the user will be able to toggle USB accessories on/off.

Note: This control is called "Allow USB accessories while device is locked" in Apple Configurator, and the control logic is opposite to what is listed here. Ensure the MDM policy rule is set correctly (to disable USB accessory connections when the device is locked).

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

1.45 AIOS-18-012300 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Apple iOS/iPadOS 18 must not allow managed apps to write contacts to unmanaged contacts accounts.

```
GROUP ID: V-268045
RULE ID: SV-268045r1031225
```

Rationale:

Managed apps have been approved for the handling of DOD sensitive information. Unmanaged apps are provided for productivity and morale purposes but are not approved to handle DOD sensitive information. Examples of unmanaged apps include those for news services, travel guides, maps, and social networking. If a document were to be viewed in a managed app and the user had the ability to open this same document in an unmanaged app, this could lead to the compromise of sensitive DOD data. In some cases, the unmanaged apps are connected to cloud backup or social networks that would permit dissemination of DOD sensitive information to unauthorized individuals. Not allowing data to be opened within unmanaged apps mitigates the risk of compromising sensitive data.

```
SFRID: FMT_SMF.1.1 #42, FDP_ACF_EXT.1.2
```

Audit:

Review configuration settings to confirm "Allow managed apps to write contacts to unmanaged contacts accounts" is disabled.

This check procedure is performed on both the Apple iOS/iPadOS management tool and the Apple iOS/iPadOS device.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS/iPadOS management tool, verify "Allow managed apps to write contacts to unmanaged contacts accounts" is unchecked.

On the iPhone and iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS/iPadOS management tool containing the restrictions policy.

5. Tap "Restrictions".
6. Verify "Allow managed apps to write contacts to unmanaged contacts accounts" is not listed.

If "Allow managed apps to write contacts to unmanaged contacts accounts" is checked in the iOS/iPadOS management tool or the restrictions policy on the iPhone and iPad lists "Allow managed apps to write contacts to unmanaged contacts accounts", this is a finding.

Remediation:

Install a configuration profile to prevent managed apps from writing contacts to unmanaged contacts accounts.

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

1.46 AIOS-18-012400 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Apple iOS/iPadOS 18 must not allow unmanaged apps to read contacts from managed contacts accounts.

```
GROUP ID: V-268046
RULE ID: SV-268046r1031226
```

Rationale:

Managed apps have been approved for the handling of DOD sensitive information. Unmanaged apps are provided for productivity and morale purposes but are not approved to handle DOD sensitive information. Examples of unmanaged apps include those for news services, travel guides, maps, and social networking. If a document were to be viewed in a managed app and the user had the ability to open this same document in an unmanaged app, this could lead to the compromise of sensitive DOD data. In some cases, the unmanaged apps are connected to cloud backup or social networks that would permit dissemination of DOD sensitive information to unauthorized individuals. Not allowing data to be opened within unmanaged apps mitigates the risk of compromising sensitive data.

```
SFRID: FMT_SMF.1.1 #42, FDP_ACF_EXT.1.2
```

Audit:

Review configuration settings to confirm "Allow unmanaged apps to read contacts from managed contacts accounts" is disabled.

This check procedure is performed on both the Apple iOS/iPadOS management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS management tool, verify "Allow unmanaged apps to read contacts from managed contacts accounts" is unchecked.

On the iPhone and iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS/iPadOS management tool containing the restrictions policy.

5. Tap "Restrictions".
6. Verify "Allow unmanaged apps to read contacts from managed contacts accounts" is not listed.

If "Allow unmanaged apps to read contacts from managed contacts accounts" is checked in the iOS/iPadOS management tool or the restrictions policy on the iPhone and iPad lists "Allow unmanaged apps to read contacts from managed contacts accounts", this is a finding.

Remediation:

Install a configuration profile to prevent unmanaged apps from reading contacts from managed contacts accounts.

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

1.47 AIOS-18-012600 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must implement the management setting: disable paired Apple Watch.

```
GROUP ID: V-268048
RULE ID: SV-268048r1116197
```

Rationale:

Sensitive DOD information could be exposed if an unauthorized Apple Watch is paired to a DOD iPhone.

```
SFRID: FMT_SMF.1.1 #47
```

Audit:

Review configuration settings to confirm "Allow Paired Watch" is disabled.

This a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding.

If the iPhone or iPad being reviewed is supervised by the MDM, follow these procedures:

This check procedure is performed on both the device management tool and the iPhone.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS management tool, verify "Allow Paired Watch" is unchecked.

On the iPhone:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "Paired Apple Watch not allowed" is listed.

If "Paired Apple Watch not allowed" is not listed both in the management tool and on the Apple device, this is a finding.

Remediation:

Install a configuration profile to disable the Apple Watch control in the management tool. This a supervised-only control.

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

1.48 AIOS-18-012500 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must implement the management setting: disable AirDrop.

```
GROUP ID: V-268047
RULE ID: SV-268047r1115590
```

Rationale:

AirDrop is a way to send contact information or photos to other users with this same feature enabled. This feature enables a possible attack vector for adversaries to exploit. Once the attacker has gained access to the information broadcast by this feature, the attacker may distribute this sensitive information very quickly and without DOD's control or awareness. By disabling this feature, the risk of mass data exfiltration will be mitigated.

Note: If the site uses Apple's optional Automatic Device Enrollment, this control is available as a supervised MDM control.

```
SFRID: FMT_SMF.1.1 #47
```

Audit:

Review configuration settings to confirm AirDrop is disabled.

This is a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding.

If the iPhone or iPad being reviewed is supervised by the MDM, follow these procedures:

This check procedure is performed on both the device management tool and the iPhone and iPad device.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS/iPadOS management tool, verify "Allow AirDrop" is unchecked.

On the iPhone/iPad device:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".

4. Tap the Configuration Profile from the iOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "AirDrop not allowed" is listed.

If "AirDrop not allowed" is not listed in the management tool and on the Apple device, this is a finding.

Remediation:

Install a configuration profile to disable the AllowAirDrop control in the management tool. This is a supervised-only control.

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

1.49 AIOS-18-012650 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must implement the management setting: approved Apple Watches must be managed by an MDM.

```
GROUP ID: V-268049
RULE ID: SV-268049r1031229
```

Rationale:

Authorizing official (AO) approval is required before an Apple Watch (DOD-owned or personally owned) can be paired with a DOD-owned iPhone to ensure the AO has evaluated the risk in having sensitive DOD data transferred to and stored on an Apple Watch in their operational environment.

```
SFRID: FMT_SMF.1.1 #47
```

Audit:

Determine if the site AO has approved the use of Apple Watch with DOD-owned iPhones. Look for a document showing approval. If not approved, this requirement is not applicable.

If approved, verify on the MDM server that the Apple Watch is being managed by the MDM. Have the MDM system administrator show that the Apple Watch is being managed by the MDM.

If the AO has approved pairing an Apple Watch with a DOD-owned iPhone and the Apple Watch is not being managed by the site MDM server, this is a finding.

Note: The iPhone paired to the Apple Watch must be supervised for the MDM to manage the Apple Watch.

Remediation:

If the AO has not approved the use of Apple Watch with DOD-owned iPhones, this requirement is not applicable.

If the AO has approved the use of Apple Watch with DOD-owned iPhones, enroll the Apple Watch in MDM management.

Note: The iPhone paired to the Apple Watch must be supervised for the MDM to manage the Apple Watch.

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

1.50 AIOS-18-012700 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must disable "Password AutoFill" in browsers and applications.

```
GROUP ID: V-268050
RULE ID: SV-268050r1031230
```

Rationale:

The AutoFill functionality in browsers and applications allows the user to complete a form that contains sensitive information, such as PII, without previous knowledge of the information. By allowing the use of the AutoFill functionality, an adversary who learns a user's iPhone and iPad passcode, or who otherwise is able to unlock the device, may be able to further breach other systems by relying on the AutoFill feature to provide information unknown to the adversary. By disabling the AutoFill functionality, the risk of an adversary gaining further information about the device's user or compromising other systems is significantly mitigated.

```
SFRID: FMT_SMF.1.1 #47
```

Audit:

This a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding.

If the iPhone or iPad being reviewed is supervised by the MDM, review configuration settings to confirm "Password AutoFill is not allowed" is disabled.

This check procedure is performed on both the iOS/iPadOS device management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS/iPadOS management tool, verify "Password AutoFill is not allowed" is unchecked.

On the iPhone/iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the restrictions policy.

5. Tap "Restrictions".
6. Verify "Password AutoFill is not allowed" is listed.

If "Password AutoFill is not allowed" is not enabled in the iOS/iPadOS management tool and on the Apple device, this is a finding.

Remediation:

Install a configuration profile to disable allow Password AutoFill in the management tool. This a supervised-only control.

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

1.51 AIOS-18-012800 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must disable "Allow setting up new nearby devices".

```
GROUP ID: V-268051
RULE ID: SV-268051r1031231
```

Rationale:

This control allows Apple device users to request passwords from nearby devices. This could lead to a compromise of the device password with an unauthorized person or device. DOD Apple device passwords must not be shared.

```
SFRID: FMT_SMF.1.1 #47
```

Audit:

This a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding.

If the iPhone or iPad being reviewed is supervised by the MDM, review configuration settings to confirm "Allow setting up new nearby devices" is disabled.

This check procedure is performed on both the iOS/iPadOS device management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS/iPadOS management tool, verify "Proximity setup to a new device is not allowed" is unchecked.

On the iPhone and iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "Proximity setup to a new device is not allowed" is not listed.

If "Proximity setup to a new device is not allowed" is disabled in the iOS/iPadOS management tool and on the Apple device, this is a finding.

Remediation:

Install a configuration profile to disable allow setting up new nearby devices in the management tool. This a supervised-only control.

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

1.52 AIOS-18-012900 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must disable password proximity requests.

```
GROUP ID: V-268052
RULE ID: SV-268052r1031232
```

Rationale:

This control allows one Apple device to be notified to share its password with a nearby device. This could lead to a compromise of the device password with an unauthorized person or device. DOD Apple device passwords must not be shared.

```
SFRID: FMT_SMF.1.1 #47
```

Audit:

This a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding.

If the iPhone or iPad being reviewed is supervised by the MDM, review configuration settings to confirm "Allow Password Proximity Requests" is disabled.

This check procedure is performed on both the device management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS management tool, verify "Allow Password Proximity Requests" is unchecked.

On the iPhone and iPad device:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "Proximity password requests not allowed" is listed.

If "Proximity password requests not allowed" is not listed in the management tool and on the Apple device, this is a finding.

Remediation:

Install a configuration profile to disable "allow password proximity requests" in the management tool. This a supervised-only control.

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

1.53 AIOS-18-013000 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must disable password sharing.

```
GROUP ID: V-268053
RULE ID: SV-268053r1031233
```

Rationale:

This control allows sharing passwords between Apple devices using AirDrop. This could lead to a compromise of the device password with an unauthorized person or device. DOD Apple device passwords must not be shared.

```
SFRID: FMT_SMF.1.1 #47
```

Audit:

This a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding.

If the iPhone or iPad being reviewed is supervised by the MDM, review configuration settings to confirm "Password Sharing is not allowed" is enabled.

This check procedure is performed on both the device management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS/iPadOS management tool, verify "Password Sharing is not allowed" is checked.

On the iPhone/iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "Password Sharing is not allowed" is listed.

If "Password Sharing is not allowed" is not enabled in the management tool and on the Apple device, this is a finding.

Remediation:

Install a configuration profile to disable allow password proximity sharing in the management tool. This a supervised-only control.

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

1.54 AIOS-18-013100 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Apple iOS/iPadOS 18 must disable "Find My Friends" in the "Find My" app.

```
GROUP ID: V-268054
RULE ID: SV-268054r1031234
```

Rationale:

This control does not share a DOD user's location but encourages location sharing between DOD mobile device users, which can lead to operational security (OPSEC) risks. Sharing the location of a DOD mobile device is a violation of AIOS-17-011700.

```
SFRID: FMT_SMF.1.1 #47
```

Audit:

This a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding.

If the iPhone or iPad being reviewed is supervised by the MDM, review configuration settings to confirm "Find My Friends" is disabled.

This check procedure is performed on both the device management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS/iPadOS management tool, verify "Allow Find My Friends" and "Allow modifying Find My Friends" are unchecked.

On the iPhone/iPad:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "Allow Find My Friends" is not listed and "Changing Find My Friends settings not allowed" is listed.

If "Allow Find My Friends" and "Allow modifying Find My Friends" are not disabled in the management tool and on the Apple device "Allow Find My Friends" is listed and "Changing Find My Friends settings not allowed" is not listed, this is a finding.

Remediation:

Install a configuration profile to disable "Find My Friends" in the Find My app and "Allow modifying Find My Friends" in the management tool. This a supervised-only control.

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

1.55 AIOS-18-013200 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Apple iOS/iPadOS 18 must be supervised by the MDM.

```
GROUP ID: V-268055
RULE ID: SV-268055r1031235
```

Rationale:

When an iOS/iPadOS is not supervised, the DOD mobile service provider cannot control when new iOS/iPadOS updates are installed on site-managed devices. Most updates should be installed immediately to mitigate new security vulnerabilities, while some sites need to test each update prior to installation to ensure critical missions are not adversely impacted by the update.

Several password and data protection controls can be implemented only when an Apple device is supervised.

```
SFRID: FMT_SMF.1.1 #47
```

Audit:

Review configuration settings to confirm site-managed iOS/iPadOS devices are supervised.

This check procedure is performed on both the Apple iOS/iPadOS management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS management tool, verify all managed Apple devices are supervised (verification procedure will vary by MDM product).

Note: If the Apple device is not managed by an MDM and supervision is set up via Apple Configurator, this procedure is not applicable.

On the iPhone and iPad:

1. Open the Settings app.
2. Verify a message similar to the following appears on the screen: "This iPad is supervised by (name of site DOD mobile service provider)."

If site-managed iOS/iPadOS devices are not supervised, this is a finding.

Remediation:

Use one of the following methods to supervise iOS and iPadOS devices managed by the DOD mobile service provider.

Method 1:

- Register all current and new iOS and iPadOS devices in the DOD mobile service provider's Automated Device Management/Apple Business Manager (ABM) account.
- Enable supervision of managed iOS/iPadOS devices in the MDM.

Method 2:

- Configure each iOS/iPadOS device using the Apple Configurator tool for Supervision.
- This method is usually only appropriate when MDM management of the DOD Apple device is not appropriate or an older device cannot be registered in ABM.

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

1.56 AIOS-18-013300 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must disable "Allow USB drive access in Files app" if the authorizing official (AO) has not approved the use of DOD-approved USB storage drives with iOS/iPadOS devices.

```
GROUP ID: V-268056
RULE ID: SV-268056r1117267
```

Rationale:

Unauthorized use of USB storage drives could lead to the introduction of malware or unauthorized software into the DOD IT infrastructure and compromise of sensitive DOD information and systems.

```
SFRID: FMT_SMF.1.1 #47
```

Audit:

This requirement is not applicable if the AO has approved the use of USB drives to load files to Apple devices. The approval must be in writing and include which USB storage devices are approved for use.

If the AO has not approved the use of USB drives to load files to Apple devices, use the following procedures to verify compliance.

This a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding.

If the iPhone or iPad being reviewed is supervised by the MDM, review configuration settings to confirm "Allow USB drive access in Files app" is disabled.

This check procedure is performed on both the device management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS management tool, verify "Allow USB drive access in Files app" is unchecked.

On the iPhone and iPad device:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".

4. Tap the Configuration Profile from the iOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "USB drives not accessible in Files app" is listed.

If "Allow USB drive access in Files app" is not disabled in the management tool and "USB drives not accessible in Files app" is not listed in the Restrictions profile on the Apple device, this is a finding.

Remediation:

If the AO has not approved the use of USB drives to load files to Apple devices, install a configuration profile to disable "Allow USB drive access in Files app".

Additional Information:

CCI-001090

Prevent unauthorized and unintended information transfer via shared system resources.

- NIST SP 800-53::SC-4
- NIST SP 800-53A::SC-4.1
- NIST SP 800-53 Revision 4::SC-4
- NIST SP 800-53 Revision 5::SC-4

1.57 AIOS-18-013400 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Apple iOS must be configured to disable automatic transfer of diagnostic data to an external device other than an MDM service with which the device has enrolled.

```
GROUP ID: V-268057
RULE ID: SV-268057r1031237
```

Rationale:

Many software systems automatically send diagnostic data to the manufacturer or a third-party. This data enables the developers to understand real-world field behavior and improve the product based on that information. Unfortunately, it can also reveal information about what DOD users are doing with the systems and what causes them to fail. An adversary embedded within the software development team or elsewhere could use the information acquired to breach mobile operating system security. Disabling automatic transfer of such information mitigates this risk.

```
SFRID: FMT_SMF.1.1 #47a
```

Audit:

Review configuration settings to confirm "Allow sending diagnostic and usage data to Apple" is disabled.

This check procedure is performed on both the iOS management tool and the iOS device.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS management tool, verify "Allow sending diagnostic and usage data to Apple" is unchecked.

Alternatively, verify the text `<key>allowDiagnosticSubmission</key><false/>` appears in the configuration profile (`.mobileconfig` file).

On the Apple iOS device:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the management policy.

5. Tap "Restrictions".
6. Verify "Diagnostic submission not allowed".

Note: This setting also disables "Share With App Developers".

If "Allow sending diagnostic and usage data to Apple" is checked in the iOS management tool, `<key>allowDiagnosticSubmission</key><true/>` appears in the configuration profile, or the restrictions policy on the Apple iOS device from the Apple iOS management tool does not list "Diagnostic submission not allowed", this is a finding.

Remediation:

Install a configuration profile to disable sending diagnostic data to an organization other than DOD.

Additional Information:

CCI-001199

Protects the confidentiality and/or integrity of organization-defined information at rest.

- NIST SP 800-53::SC-28
- NIST SP 800-53A::SC-28.1
- NIST SP 800-53 Revision 4::SC-28
- NIST SP 800-53 Revision 5::SC-28

1.58 AIOS-18-013500 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS must implement the management setting: not allow a user to remove Apple iOS configuration profiles that enforce DOD security requirements.

```
GROUP ID: V-268058
RULE ID: SV-268058r1031238
```

Rationale:

Configuration profiles define security policies on Apple iOS devices. If a user is able to remove a configuration profile, the user can then change the configuration that had been enforced by that policy. Relaxing security policies may introduce vulnerabilities the profiles had mitigated. Configuring a profile to never be removed mitigates this risk.

```
SFRID: FMT_SMF.1.1 #47
```

Audit:

Review configuration settings to confirm configuration profiles are not removable.

This check procedure is performed on both the Apple iOS management tool and the Apple iOS device. The procedures below assume the site is not enrolled in Apple's Automatic Device Enrollment and are not applicable to devices under MDM management.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the Apple iOS management tool, verify "Security" is set to "Never" and "Automatically Remove Profile" is set to "Never".

On the Apple iOS device:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap each Configuration Profile from the Apple iOS management tool that contains the restrictions for the device.
5. Verify the "Remove Profile" button is not present.

If on the Apple iOS management tool or the iOS device the "Remove Profile" button is available on the configuration profile, this is a finding.

Remediation:

Configure the Apple iOS configuration profile so that it can never be removed.

The procedure for implementing this control will vary depending on the MDM/EMM used by the mobile service provider.

When using Apple Configurator, under "General Security", configure "Security" to "Never" and "Automatically Remove Profile" to "Never".

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

1.59 AIOS-18-014300 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must disable "Allow network drive access in Files access".

```
GROUP ID: V-268059
RULE ID: SV-268059r1031239
```

Rationale:

Allowing network drive access by the Files app could lead to the introduction of malware or unauthorized software into the DOD IT infrastructure and compromise of sensitive DOD information and systems.

```
SFRID: FMT_SMF.1.1 #47
```

Audit:

This a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding.

This check procedure is performed on both the device management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS management tool, verify "Allow network drive access in Files access" is unchecked.

On the iPhone and iPad device:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "Network drives not accessible in Files app" is listed.

If "Allow network drive access in Files access" is not disabled in the management tool and "Network drives not accessible in Files app" is not listed in Profile Restrictions on the Apple device, this is a finding.

Remediation:

Install a configuration profile to disable "Allow network drive access in Files access".

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

1.60 AIOS-18-014400 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must disable connections to Siri servers for the purpose of dictation.

```
GROUP ID: V-268060
RULE ID: SV-268060r1031240
```

Rationale:

If a user is able to configure the security setting, the user could inadvertently or maliciously set it to a value that poses unacceptable risk to DOD information systems. An adversary could exploit vulnerabilities created by the weaker configuration to compromise DOD sensitive information. Dictation information could contain sensitive DOD information; therefore, should not leave the DOD control.

```
SFRID: FMT_SMF.1.1 #47
```

Audit:

If the iPhone or iPad being reviewed is supervised by the MDM, review configuration settings to confirm "Disable connections to Siri servers for the purpose of dictation" is disabled.

This check procedure is performed on the device management tool.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS management tool, verify "Disable connections to Siri servers for the purpose of dictation" is checked.

If connections to Siri servers are not disabled for dictation, this is a finding.

Remediation:

Configure the Apple iOS configuration profile to disable connections to Siri servers for the purpose of dictation. This a supervised-only control.

The procedure for implementing this control will vary depending on the MDM/EMM used by the mobile service provider.

In the MDM console, select "disable connections to Siri servers for the purpose of dictation".

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

1.61 AIOS-18-014500 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must disable connections to Siri servers for the purpose of translation.

```
GROUP ID: V-268061
RULE ID: SV-268061r1031241
```

Rationale:

If a user is able to configure the security setting, the user could inadvertently or maliciously set it to a value that poses unacceptable risk to DOD information systems. An adversary could exploit vulnerabilities created by the weaker configuration to compromise DOD sensitive information. Translation information could contain sensitive DOD information and therefore should not leave the DOD control.

```
SFRID: FMT_SMF.1.1 #47
```

Audit:

This check procedure is performed on the device management tool.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS management tool, verify "Disable connections to Siri servers for the purpose of translation" is checked.

If connections to Siri servers are not disabled for translation, this is a finding.

Remediation:

Configure the Apple iOS configuration profile to disable connections to Siri servers for the purpose of translation.

The procedure for implementing this control will vary depending on the MDM/EMM used by the mobile service provider.

In the MDM console, select "disable connections to Siri servers for the purpose of translation".

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

1.62 AIOS-18-014600 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must disable copy/paste of data from managed to unmanaged applications.

```
GROUP ID: V-268062
RULE ID: SV-268062r1031242
```

Rationale:

If a user is able to configure the security setting, the user could inadvertently or maliciously set it to a value that poses unacceptable risk to DOD information systems. An adversary could exploit vulnerabilities created by the weaker configuration to compromise DOD sensitive information.

```
SFRID: FMT_SMF.1.1 #47
```

Audit:

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS management tool, verify "Require managed pasteboard" is set to "True".

If "Require managed pasteboard" is not set to "True", this is a finding.

Remediation:

Configure the Apple iOS configuration profile to disable copy/paste of data from managed to unmanaged applications.

The procedure for implementing this control will vary depending on the MDM/EMM used by the mobile service provider.

In the MDM console, set "Require managed pasteboard" to "True".

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

1.63 AIOS-18-014700 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must have DOD root and intermediate PKI certificates installed.

```
GROUP ID: V-268063
RULE ID: SV-268063r1031243
```

Rationale:

DOD root and intermediate PKI certificates are used to verify the authenticity of PKI certificates of users and web services. If the user is allowed to remove root and intermediate certificates, the user could allow an adversary to falsely sign a certificate in such a way that it could not be detected. Restricting the ability to remove DOD root and intermediate PKI certificates to the administrator mitigates this risk.

```
SFRID: FMT_MOF_EXT.1.2 #47
```

Audit:

Verify DOD intermediate and root certificates have been installed on Apple devices.

In the iOS management tool, verify the DOD intermediate and root certificates are installed on the Apple device.

On the iPhone and iPad device:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Tap "More Details".
7. Verify the DOD intermediate and root certificates are listed.

If DOD intermediate and root certificates are not installed on the Apple device, this is a finding.

Remediation:

Install DOD intermediate and root certificates on managed mobile devices using the MDM.

Additional Information:

CCI-000370

Manage configuration settings for organization-defined system components using organization-defined automated mechanisms.

- NIST SP 800-53::CM-6 (1)
- NIST SP 800-53A::CM-6 (1).1
- NIST SP 800-53 Revision 4::CM-6 (1)
- NIST SP 800-53 Revision 5::CM-6 (1)

1.64 AIOS-18-014800 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must be configured to disable "Auto Unlock" of the iPhone by an Apple Watch.

```
GROUP ID: V-268064
RULE ID: SV-268064r1031244
```

Rationale:

Auto Unlock allows an Apple Watch to automatically unlock an iPhone or Mac when in close proximity (not available for iPad). This feature allows the iPhone/Mac to be unlocked without the user entering the device passcode, which may lead to unauthorized users access to the iPhone/Mac and sensitive DOD data. This control is not applicable if the authorizing official (AO) has approved the use of Apple Watches.

```
SFRID: FMT_MOF_EXT.1.2 #47
```

Audit:

Determine if the site AO has approved the use of Apple Watch with DOD-owned iPhones. Look for a document showing approval. If not approved, review configuration settings to confirm "Allow Auto Unlock" is disabled. If approved, this requirement is not applicable.

This check procedure is performed on the device management tool.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS management tool, verify "Allow auto unlock" is not checked.

If Allow auto unlock is enabled, this is a finding.

This requirement will become "Supervised only" in a future iOS/iPadOS release.

Remediation:

If the AO has not approved the use of Apple Watch with DOD-owned iPhones, configure the Apple iOS configuration profile to disable "Allow auto unlock".

The procedure for implementing this control will vary depending on the MDM/EMM used by the mobile service provider.

In the MDM console, set "Allow auto unlock" to "False".

This requirement will become "Supervised only" in a future iOS/iPadOS release.

Additional Information:

CCI-000765

Implement multifactor authentication for access to privileged accounts.

- NIST SP 800-53::IA-2 (1)
- NIST SP 800-53A::IA-2 (1).1
- NIST SP 800-53 Revision 4::IA-2 (1)
- NIST SP 800-53 Revision 5::IA-2 (1)

CCI-002235

Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4::AC-6 (10)
- NIST SP 800-53 Revision 5::AC-6 (10)

1.65 AIOS-18-014900 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must disable the installation of alternative marketplace apps.

```
GROUP ID: V-268065
RULE ID: SV-268065r1031245
```

Rationale:

Forcing all applications to be installed from authorized application repositories can prevent unauthorized and malicious applications from being installed and executed on mobile devices. Allowing such installations and executions could cause a compromise of DOD data accessible by these unauthorized/malicious applications.

```
SFRID: FMT_MOF_EXT.1.2 #47
```

Audit:

This is a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding.

This check procedure is performed on both the device management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS management tool, verify "Allow marketplace app installation" is unchecked.

On the iPhone and iPad device:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "Marketplace app installation not allowed" is listed.

If "Marketplace app installation" is not disabled in the management tool, this is a finding.

Remediation:

Install a configuration profile to disable the installation of alternative marketplace apps. This a supervised-only control.

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

1.66 AIOS-18-015000 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must disable app installation from a website.

```
GROUP ID: V-268066
RULE ID: SV-268066r1031246
```

Rationale:

Forcing all applications to be installed from authorized application repositories can prevent unauthorized and malicious applications from being installed and executed on mobile devices. Allowing such installations and executions could cause a compromise of DOD data accessible by these unauthorized/malicious applications.

```
SFRID: FMT_MOF_EXT.1.2 #47
```

Audit:

This check procedure is performed on both the device management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS management tool, verify "Allow app installation from website" is unchecked.

On the iPhone and iPad device:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "Web app distribution not allowed" is not listed.

If "Allow app installation from website" is not disabled in the management tool, this is a finding.

Remediation:

Install a configuration profile to disable app installation from a website.

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

1.67 AIOS-18-015100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must delete eSIM content when the device is erased.

```
GROUP ID: V-268067
RULE ID: SV-268067r1031247
```

Rationale:

An eSIM may contain sensitive DOD data and must be wiped of data when the mobile device is wiped to protect sensitive data from exposure.

```
SFRID: FMT_MOF_EXT.1.2 #47
```

Audit:

This check procedure is performed on both the device management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS management tool, verify "Preserve eSIM content when device is erased" is unchecked.

On the iPhone and iPad device:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "Preserve eSIM content when device is erased" is not listed.

If "Preserve eSIM content when device is erased" is not disabled in the management tool, this is a finding.

Remediation:

Install a configuration profile to delete eSIM content when the device is erased.

Additional Information:

CCI-001033

Defines circumstances requiring sanitization of portable storage devices prior to connecting such devices to the system.

- NIST SP 800-53::MP-6 (3)
- NIST SP 800-53A::MP-6 (3).1 (i)
- NIST SP 800-53 Revision 4::MP-6 (3)
- NIST SP 800-53 Revision 5::MP-6 (3)

1.68 AIOS-18-015400 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must disable ChatGPT and other external AI app connections in Apple Intelligence.

```
GROUP ID: V-268068
RULE ID: SV-268068r1042535
```

Rationale:

The ChatGPT feature of Apple Intelligence allows DOD information to be downloaded from the DOD iPhone/iPad and processed by the ChatGPT application in the cloud. The ChatGPT feature of Apple Intelligence increases the risk of compromise of sensitive DOD information.

```
SFRID: FMT_MOF_EXT.1.2 #47
```

Audit:

This check procedure is performed on the device management tool and the device.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS management tool, verify the following controls are set to Disable (the text may vary, depending on the UEM/MDM product): -Allow External Intelligence Integrations -Allow External Intelligence Integrations Sign In

On the iPhone/iPad (Apple Intelligence capable device only):

1. Settings >> Apple Intelligence & Siri >> ChatGPT.
2. Verify “ChatGPT” is grayed out and disabled.

If ChatGPT and other external AI app connections are not disabled in the management tool or are not grayed out and disabled on the iPhone/iPad, this is a finding.

Remediation:

Install a configuration profile to disable ChatGPT and other external AI app connections for Apple Intelligence. -Set allowExternalIntelligenceIntegrations to False -Set allowExternalIntelligenceIntegrationsSignIn to False

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

1.69 AIOS-18-015500 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must disable the download of iOS/iPadOS beta updates.

```
GROUP ID: V-269568
RULE ID: SV-269568r1031249
```

Rationale:

Beta operating system updates may contain features that could lead to the compromise of sensitive DOD information or provide a vector for the attack on the DOD network. The current STIG will not normally provide controls to disable these unsecure features.

Audit:

This is a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding.

This check procedure is performed on both the device management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS management tool, verify "Allow installing configuration profiles (supervised only)" is unchecked.

On the iPhone and iPad device:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "Installing configuration profiles not allowed" is listed.

If "Allow installing configuration profiles" is not disabled in the management tool, this is a finding.

Remediation:

Install a configuration profile to disable the installation of new configuration profiles. This will block the download and installation of beta iOS and iPadOS updates. This is a supervised-only control.

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

1.70 AIOS-18-015600 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Apple iOS/iPadOS 18 must disable the ability to hide apps.

```
GROUP ID: V-272169
RULE ID: SV-272169r1067622
```

Rationale:

Hidden apps cannot be seen by enterprise management applications (e.g., MDM server), and therefore, unauthorized apps or apps with embedded malware could be installed and hidden from the MDM or mobile threat detection (MTD) apps. Hidden apps may lead to the compromise of sensitive DOD data or provide a vector to attacks on the DOD network.

```
FMT_MOF_EXT.1.2 #47
```

Audit:

This check procedure is performed on the device management tool and the iPhone and iPad.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS management tool, verify "Allow Apps to be hidden" is unchecked.

On the iPhone and iPad device:

1. Open the Settings app.
2. Tap "Apps".
3. At the bottom of the list of Apps, tap "Hidden Apps".
4. Verify there are no hidden apps listed.

If "Allow Apps to be hidden" is not disabled in the management tool or there are hidden apps installed on enterprise iPhones and iPads, this is a finding.

Remediation:

Install a configuration profile to disable hiding apps on iPhones and iPads.

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

1.71 AIOS-18-015700 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must disable recording cell phone calls on the iPhone.

```
GROUP ID: V-272170
RULE ID: SV-272170r1067624
```

Rationale:

Cell phone recordings are saved as unmanaged recordings in the Notes app, which may be accessible to unmanaged apps. There is a risk that sensitive DOD information can be recorded from a cell phone call, saved in Notes, and be accessible to an unmanaged App, which may expose sensitive DOD information.

```
SFRID: FMT_MOF_EXT.1.2 #47
```

Audit:

This check procedure is performed on the device management tool and the iPhone.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS management tool, verify "Allow call recording" is unchecked.

On the iPhone:

1. Open the Settings app.
2. Tap "Apps".
3. Tap "Call Recording".
4. Verify the "Call Recording" toggle is off and grayed out (cannot be set to "On").

If "Allow Call Recording" is not disabled in the management tool or "Call Recording" can be enabled on the iPhone, this is a finding.

Remediation:

Install a configuration profile to disable recording cell phone calls.

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

1.72 AIOS-18-015800 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must disable iPhone Mirroring on Mac.

```
GROUP ID: V-272171
RULE ID: SV-272171r1067626
```

Rationale:

iPhone Mirroring allows managed data on a DOD iPhone to be manipulated by an unmanaged Mac. In certain situations, this may lead to the exposure of sensitive DOD data like notifications, messages, photos, etc.

```
SFRID: FMT_MOF_EXT.1.2 #47
```

Audit:

This check procedure is performed on the device management tool and the iPhone.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS management tool, verify "Allow iPhone Mirroring (supervised only)" is unchecked.

On the iPhone:

1. Open the Settings app.
2. Tap "General".
3. Tap "Airplay and Continuity".
4. Tap "iPhone Mirroring".
5. Verify no Macs are listed, or the option is grayed out.

If "Allow iPhone Mirroring" is not disabled in the management tool or iPhone Mirroring is available for Macs on the iPhone, this is a finding.

Remediation:

Install a configuration profile to disable iPhone Mirroring on Mac. This is a supervised-only control.

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

1.73 AIOS-18-016000 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must disable the ability of the user to wipe the device.

```
GROUP ID: V-276199
RULE ID: SV-276199r1115666
```

Rationale:

This feature must be disabled to comply with DOD electronic records retention requirements for mobile devices. Otherwise, mobile device users could wipe the device, which would violate DOD policy.

```
SFR ID: FMT_MOF_EXT.1.2 #47
```

Audit:

Review configuration settings to confirm erasing of contents and settings is disabled.

This is a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding.

If the iPhone or iPad being reviewed is supervised by the MDM, follow these procedures:

This check procedure is performed on both the device management tool and the iPhone and iPad device.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS/iPadOS management tool, verify "Allow erase all content and settings" is unchecked.

On the iPhone/iPad device:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "Erase content and settings not allowed" is listed.

If "Allow erase all content and settings" is not disabled in the management tool and on the Apple device, this is a finding.

Remediation:

Install a configuration profile to disable "Allow Erase All Content and Settings". This is a supervised-only control.

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

1.74 AIOS-18-016100 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Apple iOS/iPadOS 18 must disable the use of voice assistant (Siri) unless required to meet Section 508 compliance requirements.

```
GROUP ID: V-276200
RULE ID: SV-276200r1115669
```

Rationale:

The use of voice assistants could expose sensitive DOD data to cloud-based servers during the processing of assistant requests.

```
SFR ID: FMT_MOF_EXT.1.2 #47
```

Audit:

Review configuration settings to confirm the use of Siri is disabled. Exception: Siri is allowed if used to meet Section 508 compliance requirements.

This check procedure is performed on both the device management tool and the iPhone and iPad device.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS/iPadOS management tool, verify "Allow Siri" is unchecked.

On the iPhone/iPad device:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "Siri not allowed" is listed.

If "Allow Siri" is not disabled in the management tool and on the Apple device, this is a finding.

Remediation:

Install a configuration profile to disable "Allow Siri" unless required to meet Section 508 compliance requirements.

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

1.75 AIOS-18-016200 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Apple iOS/iPadOS 18 must disable the use of voice assistant (Show user-generated content in Siri) unless required to meet Section 508 compliance requirements.

```
GROUP ID: V-276201
RULE ID: SV-276201r1115672
```

Rationale:

The use of voice assistants could expose sensitive DOD data to cloud-based servers during the processing of assistant requests.

```
SFR ID: FMT_MOF_EXT.1.2 #47
```

Audit:

Review configuration settings to confirm Siri is disabled. Exception: Siri is allowed if used to meet Section 508 compliance requirements.

Note: This control may not be configurable by some MDM products when "Allow Siri" is disabled.

This is a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding.

If the iPhone or iPad being reviewed is supervised by the MDM, follow these procedures:

This check procedure is performed on both the device management tool and the iPhone and iPad device.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS/iPadOS management tool, verify "Show user-generated content in Siri" or "Allow Siri" is unchecked.

On the iPhone/iPad device:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the restrictions policy.

5. Tap "Restrictions".
6. Verify "Show user-generated content in Siri not allowed" or "Siri not allowed" is listed.

If "Show user-generated content in Siri" is not disabled or Siri is not disabled in the management tool and on the Apple device, this is a finding.

Remediation:

Install a configuration profile to disable "Show user-generated content in Siri" unless required to meet Section 508 compliance requirements. This is a supervised-only control.

Note: This control may not be configurable by some MDM products when "Allow Siri" is disabled.

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

1.76 AIOS-18-016300 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Apple iOS/iPadOS 18 must disable the use of voice assistant (Siri suggestions) unless required to meet Section 508 compliance requirements.

```
GROUP ID: V-276202
RULE ID: SV-276202r1115675
```

Rationale:

The use of voice assistants could expose sensitive DOD data to cloud-based servers during the processing of assistant requests.

```
SFR ID: FMT_MOF_EXT.1.2 #47
```

Audit:

Review configuration settings to confirm Siri is disabled. Exception: Siri is allowed if used to meet Section 508 compliance requirements.

Note: This control may not be configurable by some MDM products when "Allow Siri" is disabled.

This is a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding.

If the iPhone or iPad being reviewed is supervised by the MDM, follow these procedures:

This check procedure is performed on both the device management tool and the iPhone and iPad device.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS/iPadOS management tool, verify "Allow Siri Suggestions" or "Allow Siri" is unchecked.

On the iPhone/iPad device:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the restrictions policy.

5. Tap "Restrictions".
6. Verify "Siri Suggestions not allowed" or "Siri not allowed" is listed.

If "Siri Suggestions" is not disabled or Siri is not disabled in the management tool and on the Apple device, this is a finding.

Remediation:

Install a configuration profile to disable "Allow Siri Suggestions" unless required to meet Section 508 compliance requirements. This is a supervised-only control.

Note: This control may not be configurable by some MDM products when "Allow Siri" is disabled.

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

1.77 AIOS-18-016400 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must disable automatic downloads of apps purchased on other Apple devices.

```
GROUP ID: V-276203
RULE ID: SV-276203r1115678
```

Rationale:

The automatic download of apps to a DOD mobile device could cause the exposure of sensitive DOD information when an unauthorized app is installed.

```
SFR ID: FMT_MOF_EXT.1.2 #47
```

Audit:

Review configuration settings to confirm automatic downloading of apps is disabled.

This is a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding.

If the iPhone or iPad being reviewed is supervised by the MDM, follow these procedures:

This check procedure is performed on both the device management tool and the iPhone and iPad device.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS/iPadOS management tool, verify "Allow automatic app downloads" is unchecked.

On the iPhone/iPad device:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "Automatic downloading apps not allowed" is listed.

If "Automatic downloading apps" is not disabled in the management tool and on the Apple device, this is a finding.

Remediation:

Install a configuration profile to disable "Allow automatic app downloads". This is a supervised-only control.

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

1.78 AIOS-18-016500 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must disable pairing with a host Mac or PC.

```
GROUP ID: V-276204
RULE ID: SV-276204r1115681
```

Rationale:

The connection of a DOD iPhone to a Mac or PC could cause the exposure of sensitive DOD information.

```
SFR ID: FMT_MOF_EXT.1.2 #47
```

Audit:

Review configuration settings to confirm host pairing is disabled.

This is a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding.

If the iPhone or iPad being reviewed is supervised by the MDM, follow these procedures:

This check procedure is performed on both the device management tool and the iPhone and iPad device.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS/iPadOS management tool, verify "Allow host pairing" is unchecked.

On the iPhone/iPad device:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "Pairing with iTunes not allowed" is listed.

If "Host pairing" is not disabled in the management tool and on the Apple device, this is a finding.

Remediation:

Install a configuration profile to disable "Allow host pairing". This is a supervised-only control.

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

1.79 AIOS-18-016600 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Apple iOS/iPadOS 18 must disable AirPrint.

```
GROUP ID: V-276205
RULE ID: SV-276205r1115684
```

Rationale:

AirPrint allows the printing of sensitive DOD documents to non-DOD controlled printers, which may lead to the exposure of sensitive DOD information.

```
SFR ID: FMT_MOF_EXT.1.2 #47
```

Audit:

Review configuration settings to confirm AirPrint is disabled.

This is a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding.

If the iPhone or iPad being reviewed is supervised by the MDM, follow these procedures:

This check procedure is performed on both the device management tool and the iPhone and iPad device.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS/iPadOS management tool, verify "Allow AirPrint" is unchecked.

On the iPhone/iPad device:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "AirPrint not allowed" is listed.

If AirPrint is not disabled in the management tool and on the Apple device, this is a finding.

Remediation:

Install a configuration profile to disable "Allow AirPrint". This is a supervised-only control.

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

1.80 AIOS-18-016800 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Apple iOS/iPadOS 18 must disable AirPrint: Allow storage of AirPrint credentials in Keychain.

```
GROUP ID: V-276207
RULE ID: SV-276207r1115690
```

Rationale:

AirPrint allows the printing of sensitive DOD documents to non-DOD controlled printers, which may lead to the exposure of sensitive DOD information.

```
SFR ID: FMT_MOF_EXT.1.2 #47
```

Audit:

Review configuration settings to confirm storage of AirPrint credentials in Keychain is disabled.

This is a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding.

Note: This control may not be configurable by some MDM products when "Allow AirPrint" is disabled.

If the iPhone or iPad being reviewed is supervised by the MDM, follow these procedures:

This check procedure is performed on both the device management tool and the iPhone and iPad device.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS/iPadOS management tool, verify "Allow storage of AirPrint credentials in Keychain" or "Allow AirPrint" is unchecked.

On the iPhone/iPad device:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the restrictions policy.

5. Tap "Restrictions".
6. Verify "Storage of AirPrint credentials in Keychain not allowed" or "AirPrint not allowed" is listed.

If "Storage of AirPrint credentials in Keychain" is not disabled or AirPrint is not disabled in the management tool and on the Apple device, this is a finding.

Remediation:

Install a configuration profile to disable "Allow storage of AirPrint credentials in Keychain". This is a supervised-only control.

Note: This control may not be configurable by some MDM products when "Allow AirPrint" is disabled.

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

1.81 AIOS-18-016700 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Apple iOS/iPadOS 18 must disable AirPrint: Allow discovery of AirPrint printers using iBeacons.

```
GROUP ID: V-276206
RULE ID: SV-276206r1115687
```

Rationale:

AirPrint allows the printing of sensitive DOD documents to non-DOD controlled printers, which may lead to the exposure of sensitive DOD information.

```
SFR ID: FMT_MOF_EXT.1.2 #47
```

Audit:

Review configuration settings to confirm discovery of AirPrint printers is disabled.

This is a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding.

Note: This control may not be configurable by some MDM products when "Allow AirPrint" is disabled.

If the iPhone or iPad being reviewed is supervised by the MDM, follow these procedures:

This check procedure is performed on both the device management tool and the iPhone and iPad device.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS/iPadOS management tool, verify "Allow discovery of AirPrint printers using iBeacons" or "Allow AirPrint" is unchecked.

On the iPhone/iPad device:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the restrictions policy.
5. Tap "Restrictions".

6. Verify "Discovery of AirPrint printers using iBeacons not allowed" or "AirPrint not allowed" is listed.

If "Discovery of AirPrint printers using iBeacons" is not disabled or AirPrint is not disabled in the management tool and on the Apple device, this is a finding.

Remediation:

Install a configuration profile to disable "Allow discovery of AirPrint printers using iBeacons". This is a supervised-only control.

Note: This control may not be configurable by some MDM products when "Allow AirPrint" is disabled.

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

1.82 AIOS-18-016900 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Apple iOS/iPadOS 18 must enable AirPrint feature: Disallow AirPrint to destinations with untrusted certificates.

```
GROUP ID: V-276208
RULE ID: SV-276208r1115693
```

Rationale:

AirPrint allows the printing of sensitive DOD documents to non-DOD controlled printers, which may lead to the exposure of sensitive DOD information.

```
SFR ID: FMT_MOF_EXT.1.2 #47
```

Audit:

Review configuration settings to confirm allowing AirPrint to destinations with untrusted certificates is disabled.

This is a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding.

Note: This control may not be configurable by some MDM products when "Allow AirPrint" is disabled.

If the iPhone or iPad being reviewed is supervised by the MDM, follow these procedures:

This check procedure is performed on both the device management tool and the iPhone and iPad device.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS/iPadOS management tool, verify "Disallow AirPrint to destinations with untrusted certificates" is checked or "Allow AirPrint" is unchecked.

On the iPhone/iPad device:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the restrictions policy.

5. Tap "Restrictions".
6. Verify "Allow AirPrint to destinations with untrusted certificates" or "AirPrint not allowed" is listed.

If "Disallow AirPrint to destinations with untrusted certificates" is disabled or AirPrint is not disabled in the management tool and on the Apple device, this is a finding.

Remediation:

Install a configuration profile to enable "Disallow AirPrint to destinations with untrusted certificates". This is a supervised-only control.

Note: This control may not be configurable by some MDM products when "Allow AirPrint" is disabled.

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

1.83 AIOS-18-017000 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Apple iOS/iPadOS 18 must disable Allowed Content Ratings (Movies).

```
GROUP ID: V-276209
RULE ID: SV-276209r1115696
```

Rationale:

There is no known mission need for this personal use feature.

```
SFR ID: FMT_MOF_EXT.1.2 #47
```

Audit:

Review configuration settings to confirm Allowed Content Ratings (Movies) is disabled.

This is a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding.

If the iPhone or iPad being reviewed is supervised by the MDM, follow these procedures:

This check procedure is performed on both the device management tool and the iPhone and iPad device.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS/iPadOS management tool, verify "Movie ratings" is set to "0" (disable all movies).

On the iPhone/iPad device:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "Movie ratings enforced" is listed.

If "Movie ratings" is not set to "0" in the management tool and "Movie ratings" are not enforced on the Apple device, this is a finding.

Remediation:

Install a configuration profile to disable "Allowed Content Ratings (Movies)" (ratingMovies key value = 0). This is a supervised-only control.

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

1.84 AIOS-18-017100 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Apple iOS/iPadOS 18 must disable Allowed Content Ratings (TV Shows).

```
GROUP ID: V-276210
RULE ID: SV-276210r1115699
```

Rationale:

There is no known mission need for this personal use feature.

```
SFR ID: FMT_MOF_EXT.1.2 #47
```

Audit:

Review configuration settings to confirm Allowed Content Ratings (TV Shows) is disabled.

This is a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding.

If the iPhone or iPad being reviewed is supervised by the MDM, follow these procedures:

This check procedure is performed on both the device management tool and the iPhone and iPad device.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS/iPadOS management tool, verify "TV Shows ratings" is set to "0" (disable all TV Shows).

On the iPhone/iPad device:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "TV show ratings enforced" is listed.

If "TV show ratings" is not set to "0" in the management tool and TV show ratings are not enforced on the Apple device, this is a finding.

Remediation:

Install a configuration profile to disable "Allowed Content Ratings (TV Shows)" (ratingTVShows key value = 0). This is a supervised-only control.

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

1.85 AIOS-18-017200 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Apple iOS/iPadOS 18 must disable the Apple Intelligence feature: Image Wand.

```
GROUP ID: V-276211
RULE ID: SV-276211r1115702
```

Rationale:

The security of the Apple Intelligence system has not been vetted by the DOD, and the risk to DOD sensitive information is not known at this time. Therefore, Apple intelligence features must be disabled until more information is available.

```
SFR ID: FMT_MOF_EXT.1.2 #47
```

Audit:

Review configuration settings to confirm Image Wand is disabled. Note: This control is only applicable to Apple Intelligence-capable iPhones and iPads.

This is a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding.

If the iPhone or iPad being reviewed is supervised by the MDM, follow these procedures:

This check procedure is performed on both the device management tool and the iPhone and iPad device.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS/iPadOS management tool, verify the Apple Intelligence feature: Image Wand is unchecked.

On the iPhone/iPad device:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "Image Wand not allowed" is listed.

If Image Wand is not disabled in the management tool and on the Apple device, this is a finding.

Remediation:

Install a configuration profile to disable the Apple Intelligence feature: Image Wand. This is a supervised-only control.

Note: This control is only applicable to Apple Intelligence-capable iPhones and iPads.

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

1.86 AIOS-18-017300 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Apple iOS/iPadOS 18 must disable the Apple Intelligence feature: Image Generation.

```
GROUP ID: V-276212
RULE ID: SV-276212r1115705
```

Rationale:

The security of the Apple Intelligence system has not been vetted by the DOD, and the risk to DOD sensitive information is not known at this time. Therefore, Apple intelligence features must be disabled until more information is available.

```
SFR ID: FMT_MOF_EXT.1.2 #47
```

Audit:

Review configuration settings to confirm Image Generation is disabled. Note: This control is only applicable to Apple Intelligence-capable iPhones and iPads.

This is a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding.

If the iPhone or iPad being reviewed is supervised by the MDM, follow these procedures:

This check procedure is performed on both the device management tool and the iPhone and iPad device.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS/iPadOS management tool, verify the Apple Intelligence feature: Image Generation is unchecked.

On the iPhone/iPad device:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "Image Playground not allowed" is listed.

If Image Generation is not disabled in the management tool and on the Apple device, this is a finding.

Remediation:

Install a configuration profile to disable the Apple Intelligence feature: Image Generation. This is a supervised-only control.

Note: This control is only applicable to Apple Intelligence-capable iPhones and iPads.

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

1.87 AIOS-18-017400 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Apple iOS/iPadOS 18 must disable the Apple Intelligence feature: generate new Genmoji.

```
GROUP ID: V-276213
RULE ID: SV-276213r1115708
```

Rationale:

The security of the Apple Intelligence system has not been vetted by the DOD, and the risk to DOD sensitive information is not known at this time. Therefore, Apple intelligence features must be disabled until more information is available.

```
SFR ID: FMT_MOF_EXT.1.2 #47
```

Audit:

Review configuration settings to confirm generate new Genmoji is disabled. Note: This control is only applicable to Apple Intelligence-capable iPhones and iPads.

This is a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding.

If the iPhone or iPad being reviewed is supervised by the MDM, follow these procedures:

This check procedure is performed on both the device management tool and the iPhone and iPad device.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS/iPadOS management tool, verify the Apple Intelligence feature: generate new Genmoji is unchecked.

On the iPhone/iPad device:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "Genmoji not allowed" is listed.

If generate new Genmoji is not disabled in the management tool and on the Apple device, this is a finding.

Remediation:

Install a configuration profile to disable the Apple Intelligence feature: generate new Genmoji. This is a supervised-only control.

Note: This control is only applicable to Apple Intelligence-capable iPhones and iPads.

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

1.88 AIOS-18-017700 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

DOD Apple iOS/iPadOS 18 devices must have a Mobile Threat Detection (MTD) app installed.

```
GROUP ID: V-276214
RULE ID: SV-276214r1115711
```

Rationale:

DOD mobile devices are at constant risk of cyber threats. MTD apps mitigate these risks by providing real-time threat detection, malware prevention, and vulnerability analysis.

```
SFR ID: FMT_MOF_EXT.1.2 #47
```

Audit:

Confirm an MTD app is installed on managed iPhones and iPads.

This check procedure is performed on both the device management tool and the iPhone and iPad device.

In the iOS/iPadOS management tool, verify an MTD app is listed as a managed app being deployed to site-managed devices.

On the iPhone/iPad device:

1. Open the Settings app.
2. Tap "Apps".
3. Verify that an MTD app is listed.

If an MTD app is not installed on the device, this is a finding.

Remediation:

Deploy a site-approved MTD app via the MDM server to managed iPhones and iPads.

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

1.89 AIOS-18-017800 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

DOD Apple iOS/iPadOS 18 devices must disable FaceTime.

```
GROUP ID: V-276196
RULE ID: SV-276196r1115625
```

Rationale:

FaceTime is considered a personal use feature.

Audit:

This a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding.

If the iPhone or iPad being reviewed is supervised by the MDM, follow these procedures:

This check procedure is performed on both the device management tool and the iPhone and iPad device.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS/iPadOS management tool, verify "Allow FaceTime" is unchecked.

On the iPhone/iPad device:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "FaceTime not allowed" is listed.

If "Allow FaceTime" is listed in the management tool or "FaceTime not allowed" is not listed on the Apple device, this is a finding.

Remediation:

Install a configuration profile to disable FaceTime. This a supervised-only control.

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

1.90 AIOS-18-017900 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

DOD Apple iOS/iPadOS 18 devices must disable eSIM transfers.

```
GROUP ID: V-276197
RULE ID: SV-276197r1115628
```

Rationale:

eSIM transfers could lead to the unauthorized use of DOD paid cellular service.

Audit:

Determine if the site authorizing official (AO) has approved the use of eSIM transfer. Look for documentation of AO approval. If eSIM transfer is not approved, review configuration settings to confirm it is disabled. If approved, this requirement is not applicable.

This a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding.

If the iPhone or iPad being reviewed is supervised by the MDM, follow these procedures:

This check procedure is performed on both the device management tool and the iPhone and iPad device.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS/iPadOS management tool, verify "Allow outgoing eSIM transfers" is unchecked.

On the iPhone/iPad device:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "Outgoing eSIM transfers not allowed" is listed.

If the AO has not approved eSIM transfers and "Allow eSIM outgoing transfers" is listed in the management tool or "Outgoing eSIM transfers not allowed" is not listed on the Apple device, this is a finding.

Remediation:

Install a configuration profile to disable the transfer of an eSIM from one DOD phone to another unless the service has been approved by the AO. This a supervised-only control.

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

1.91 AIOS-18-018000 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

DOD Apple iOS/iPadOS 18 devices must disable screenshots and screen recordings.

```
GROUP ID: V-276198
RULE ID: SV-276198r1115631
```

Rationale:

A screenshot or screen recording of sensitive DOD information could lead to the inadvertent exposure of that information.

Audit:

Review configuration settings to confirm screenshot and screen recording is disabled.

This check procedure is performed on both the device management tool and the iPhone and iPad device.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS/iPadOS management tool, verify "Allow screenshot and screen recording" is unchecked.

On the iPhone/iPad device:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the restrictions policy.
5. Tap "Restrictions".
6. Verify "Screen capture not allowed" is listed.

If "Allow screenshot and screen recording" is listed in the management tool or "Screen capture not allowed" is not listed on the Apple device, this is a finding.

Remediation:

Install a configuration profile to disable the screenshot and screen recording.

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

1.92 AIOS-18-018100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must implement the management setting: disable Camera.

```
GROUP ID: V-276224
RULE ID: SV-276224r1116200
```

Rationale:

Authorizing Official (AO) approval is required before the Apple device camera can be enabled for a specific user or group of users, based on a risk assessment of the operational environment. Camera use may lead to the exposure of sensitive DOD information in some operational environments.

```
SFR ID: FMT_MOF_EXT.1.2 #47
```

Audit:

Determine if the site AO has approved the use of Apple device cameras. Look for a document showing approval for a specific user or group of users. If not approved, review configuration settings to confirm "Allow Camera" is disabled. If approved, this requirement is not applicable.

This a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding (if the AO has not approved the use of the Apple device camera).

If the iPhone or iPad being reviewed is supervised by the MDM, follow these procedures:

This check procedure is performed on both the device management tool and the iPhone.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS management tool, verify "Allow Camera" is unchecked.

On the iPhone:

1. Open the Settings app.
2. Tap "General".
3. Tap "VPN & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the restrictions policy.

5. Tap "Restrictions".
6. Verify "Camera not allowed" is listed.

If the AO has not approved Apple device camera use, "Allow camera" is listed in the management tool, and "Camera not allowed" is not listed on the Apple device, this is a finding.

Remediation:

If the AO has not approved the use of Apple device cameras, install a configuration profile to disable camera use. This a supervised-only control.

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

1.93 AIOS-18-018200 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Apple iOS/iPadOS 18 must implement the management setting: disable the Bluetooth radio.

```
GROUP ID: V-278354
RULE ID: SV-278354r1130560
```

Rationale:

Authorizing official (AO) approval is required before the Apple device Bluetooth radio can be enabled. All AO approvals must be documented and based on critical mission need. Use of Bluetooth may lead to the exposure of sensitive DOD information in some operational environments.

```
SFR ID: FMT_MOF_EXT.1.2 #47
```

Audit:

Determine if the site AO has approved the use of Apple device Bluetooth radios. Look for a document showing AO approval. All AO approvals must be documented and based on critical mission need.

If not approved, review configuration settings on the MDM server to confirm Bluetooth modification has been disabled, and on the Apple iPhone or iPad, verify Bluetooth cannot be enabled. If approved, this requirement is not applicable.

This a supervised-only control. If the iPhone or iPad being reviewed is not supervised by the MDM, this control is automatically a finding (if the AO has not approved the use of the Apple device Bluetooth radio).

If the iPhone or iPad being reviewed is supervised by the MDM, follow these procedures:

This check procedure is performed on both the device management tool and managed iPhone or iPad.

Note: If an organization has multiple configuration profiles, the Check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

In the iOS management tool, verify the Bluetooth setting cannot be modified ("allowBluetoothModification" set to "false") in the configuration profile.

On the managed Apple iPhone or iPad, verify the Bluetooth radio is disabled and cannot be enabled: (Settings > Bluetooth)

If Bluetooth has not been disabled in the device's MDM configuration profile or if Bluetooth can be enabled on the Apple device, this is a finding.

Remediation:

If the AO has not approved the use of the Apple device Bluetooth radio, install a configuration profile to disable Bluetooth use. This a supervised-only control.

There are two steps to this procedure:

1. MDM sends device command to device to disable Bluetooth.
2. Include the key "allowBluetoothModification" set to "false" in the configuration profile installed on the device.

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	AIOS-18-001000 (Manual)	☐	☐
1.2	AIOS-18-003000 (Manual)	☐	☐
1.3	AIOS-18-003200 (Manual)	☐	☐
1.4	AIOS-18-003300 (Manual)	☐	☐
1.5	AIOS-18-003450 (Manual)	☐	☐
1.6	AIOS-18-003500 (Manual)	☐	☐
1.7	AIOS-18-003600 (Manual)	☐	☐
1.8	AIOS-18-003700 (Manual)	☐	☐
1.9	AIOS-18-006500 (Manual)	☐	☐
1.10	AIOS-18-006600 (Manual)	☐	☐
1.11	AIOS-18-006800 (Manual)	☐	☐
1.12	AIOS-18-006900 (Manual)	☐	☐
1.13	AIOS-18-006950 (Manual)	☐	☐
1.14	AIOS-18-007000 (Manual)	☐	☐
1.15	AIOS-18-007200 (Manual)	☐	☐
1.16	AIOS-18-007400 (Manual)	☐	☐
1.17	AIOS-18-007500 (Manual)	☐	☐
1.18	AIOS-18-007600 (Manual)	☐	☐
1.19	AIOS-18-008400 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	AIOS-18-009200 (Manual)	☐	☐
1.21	AIOS-18-009700 (Manual)	☐	☐
1.22	AIOS-18-009800 (Manual)	☐	☐
1.23	AIOS-18-009900 (Manual)	☐	☐
1.24	AIOS-18-010000 (Manual)	☐	☐
1.25	AIOS-18-010200 (Manual)	☐	☐
1.26	AIOS-18-010400 (Manual)	☐	☐
1.27	AIOS-18-010500 (Manual)	☐	☐
1.28	AIOS-18-010600 (Manual)	☐	☐
1.29	AIOS-18-010700 (Manual)	☐	☐
1.30	AIOS-18-010800 (Manual)	☐	☐
1.31	AIOS-18-010850 (Manual)	☐	☐
1.32	AIOS-18-010900 (Manual)	☐	☐
1.33	AIOS-18-010950 (Manual)	☐	☐
1.34	AIOS-18-011000 (Manual)	☐	☐
1.35	AIOS-18-011200 (Manual)	☐	☐
1.36	AIOS-18-011300 (Manual)	☐	☐
1.37	AIOS-18-011400 (Manual)	☐	☐
1.38	AIOS-18-011500 (Manual)	☐	☐
1.39	AIOS-18-011600 (Manual)	☐	☐
1.40	AIOS-18-011700 (Manual)	☐	☐
1.41	AIOS-18-011800 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.42	AIOS-18-011900 (Manual)	☐	☐
1.43	AIOS-18-012000 (Manual)	☐	☐
1.44	AIOS-18-012200 (Manual)	☐	☐
1.45	AIOS-18-012300 (Manual)	☐	☐
1.46	AIOS-18-012400 (Manual)	☐	☐
1.47	AIOS-18-012600 (Manual)	☐	☐
1.48	AIOS-18-012500 (Manual)	☐	☐
1.49	AIOS-18-012650 (Manual)	☐	☐
1.50	AIOS-18-012700 (Manual)	☐	☐
1.51	AIOS-18-012800 (Manual)	☐	☐
1.52	AIOS-18-012900 (Manual)	☐	☐
1.53	AIOS-18-013000 (Manual)	☐	☐
1.54	AIOS-18-013100 (Manual)	☐	☐
1.55	AIOS-18-013200 (Manual)	☐	☐
1.56	AIOS-18-013300 (Manual)	☐	☐
1.57	AIOS-18-013400 (Manual)	☐	☐
1.58	AIOS-18-013500 (Manual)	☐	☐
1.59	AIOS-18-014300 (Manual)	☐	☐
1.60	AIOS-18-014400 (Manual)	☐	☐
1.61	AIOS-18-014500 (Manual)	☐	☐
1.62	AIOS-18-014600 (Manual)	☐	☐
1.63	AIOS-18-014700 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.64	AIOS-18-014800 (Manual)	☐	☐
1.65	AIOS-18-014900 (Manual)	☐	☐
1.66	AIOS-18-015000 (Manual)	☐	☐
1.67	AIOS-18-015100 (Manual)	☐	☐
1.68	AIOS-18-015400 (Manual)	☐	☐
1.69	AIOS-18-015500 (Manual)	☐	☐
1.70	AIOS-18-015600 (Manual)	☐	☐
1.71	AIOS-18-015700 (Manual)	☐	☐
1.72	AIOS-18-015800 (Manual)	☐	☐
1.73	AIOS-18-016000 (Manual)	☐	☐
1.74	AIOS-18-016100 (Manual)	☐	☐
1.75	AIOS-18-016200 (Manual)	☐	☐
1.76	AIOS-18-016300 (Manual)	☐	☐
1.77	AIOS-18-016400 (Manual)	☐	☐
1.78	AIOS-18-016500 (Manual)	☐	☐
1.79	AIOS-18-016600 (Manual)	☐	☐
1.80	AIOS-18-016800 (Manual)	☐	☐
1.81	AIOS-18-016700 (Manual)	☐	☐
1.82	AIOS-18-016900 (Manual)	☐	☐
1.83	AIOS-18-017000 (Manual)	☐	☐
1.84	AIOS-18-017100 (Manual)	☐	☐
1.85	AIOS-18-017200 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.86	AIOS-18-017300 (Manual)	☐	☐
1.87	AIOS-18-017400 (Manual)	☐	☐
1.88	AIOS-18-017700 (Manual)	☐	☐
1.89	AIOS-18-017800 (Manual)	☐	☐
1.90	AIOS-18-017900 (Manual)	☐	☐
1.91	AIOS-18-018000 (Manual)	☐	☐
1.92	AIOS-18-018100 (Manual)	☐	☐
1.93	AIOS-18-018200 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Sep 12, 2025	1.0.0	Initial CIS Release