CIS Honeywell Android 13 COBO STIG Benchmark

v1.0.0 - 08-27-2025

Terms of Use

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

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

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

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

Table of Contents

Overview

Target Technology Details

Honeywell Android 13 COBO Secure Technical Implementation Guide (STIG)
Version: 1 Release: 1 Benchmark
Date: 22 Apr 2025

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Honeywell Android 13 COBO 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 Honeywell Android 13 COBO.

Recommendations

1 STIG RULES

Honeywell Android 13

Honeywell Android 13 COBO Secure Technical Implementation Guide (STIG)

Version: 1 Release: 1 Benchmark

Date: 22 Apr 2025

CLASSIFICATION unclassified

1.1 HONW-13-002800 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Honeywell Android 13 must be configured to enable audit logging.

```
GROUP ID: V-274317
RULE ID: SV-274317r1100404
```

Rationale:

Audit logs enable monitoring of security-relevant events and subsequent forensics when breaches occur. For audit logs to be useful, administrators must have the ability to view them.

SFR ID: FMT_SMF_EXT.1.1 #32

Audit:

Inspect the configuration on the managed Honeywell Android 13 device to enable audit logging.
This validation procedure is performed only on the EMM Administration Console.
On the EMM console:
COBO and COPE:

1. Open "Device owner management" section.
2. Verify that "Enable security logging" is toggled to "ON".

If the EMM console device policy is not set to enable audit logging, this is a finding.

Remediation:

Configure the Honeywell Android 13 device to enable audit logging.
On the EMM console:
COBO and COPE:

1. Open "Device owner management" section.
2. Toggle "Enable security logging" to "ON".

Additional Information:

CCI-000154 Provide the capability to centrally review and analyze audit records from multiple components within the system.

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

1.2 HONW-13-006000 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Honeywell Android 13 must be configured to enforce a minimum password length of six characters.

```
GROUP ID: V-274283
RULE ID: SV-274283r1100302
```

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.

SFR ID: FMT_SMF_EXT.1.1 #1a

Audit:

Review managed Honeywell Android 13 device configuration settings to determine if the mobile device is enforcing a minimum password length of six characters.
This validation procedure is performed on both the EMM Administration Console and the managed Honeywell Android 13 device.
On the EMM console:
COBO:

1. Open "Lock screen" settings.
2. Open "Password constraints".
3. Open "Minimum password quality".
4. Verify that Numeric Complex, Alphabetic, Alphanumeric, or Complex is selected.
5. Open "Minimum password length".
6. Verify that "6" is set for number of characters.

COPE:

1. Open "Lock screen" settings.
2. Open "Password constraints".
3. Select "Personal Profile".
4. Verify that "Minimum password quality" is set to Numeric Complex, Alphabetic, Alphanumeric, or Complex.
5. Open "Minimum password length".
6. Verify that the number of characters is set to "6" or higher.

On the managed Honeywell Android 13 device:
COBO and COPE:

1. Open Settings >> Security >> Screen lock.
2. Enter current password.
3. Tap "Pin or Password".
4. Verify that Password length required is at least "6".

If the device password length is not set to six characters or more on EMM console or on the managed Honeywell Android 13 device, this is a finding.

Remediation:

Configure the Honeywell Android 13 device to enforce a minimum password length of six characters.
On the EMM console:
COBO:

1. Open "Lock screen" settings.
2. Open "Password constraints".
3. Open "Minimum password quality".
4. Choose Numeric Complex, Alphabetic, Alphanumeric, or Complex.
5. Open "Minimum password length".
6. Enter in the number of characters as "6".

COPE:

1. Open "Lock screen" settings.
2. Open "Password constraints".
3. Select "Personal Profile".
4. Open "Minimum password quality".
5. Choose Numeric Complex, Alphabetic, Alphanumeric, or Complex.
6. Open "Minimum password length".
7. Enter in the number of characters as "6".

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)

1.3 HONW-13-006100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Honeywell Android 13 must be configured to not allow passwords that include more than four repeating or sequential characters.

```
GROUP ID: V-274284
RULE ID: SV-274284r1100305
```

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.

SFR ID: FMT_SMF_EXT.1.1 #1b

Audit:

Review managed Honeywell Android 13 device configuration settings to determine if the mobile device is prohibiting passwords with more than four repeating or sequential characters.
This validation procedure is performed on both the EMM Administration Console and the managed Honeywell Android 13 device.
On the EMM console:
COBO:

1. Open "Lock screen" settings.
2. Open "Password constraints".
3. Verify that quality is set to "Numeric (Complex)" or higher.

COPE:

1. Open "Lock screen" settings.
2. Open "Password constraints".
3. Select "Personal Profile".
4. Verify that quality is set to "Numeric (Complex)" or higher.

On the managed Honeywell Android 13 device:
COBO and COPE:

1. Open Settings >> Security >> Screen lock.
2. Enter current password.
3. Select "PIN".
4. Try to enter a new PIN with repeating numbers.
5. Verify that Password complexity requirements are listed: Ascending, descending, or repeated sequence of digits is not allowed.

If the EMM console device policy is set to a password with more than two repeating or sequential characters, or on the managed Honeywell Android 13 device, the device policy is set to a password with more than two repeating or sequential characters, this is a finding.
Note: "Alphabetic", "Alphanumeric", and "Complex" are also acceptable selections, but these selections will cause the user to select a complex password, which is not required by the STIG.

Remediation:

Configure the Honeywell Android 13 device to prevent passwords from containing more than four repeating or sequential characters.
On the EMM console:
COBO:

1. Open "Lock screen" settings.
2. Open "Password constraints".
3. Set password quality to "Numeric (Complex)".

COPE:

1. Open "Password constraints".
2. Select "Personal Profile".
3. Set password quality to "Numeric (Complex)".

Note: "Alphabetic", "Alphanumeric", and "Complex" are also acceptable selections, but these selections will cause the user to select a complex password, which is not required by the STIG.

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)

1.4 HONW-13-006300 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Honeywell Android 13 must be configured to lock the display after 15 minutes (or less) of inactivity.

```
GROUP ID: V-274285
RULE ID: SV-274285r1100308
```

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.

SFR ID: FMT_SMF_EXT.1.1 #2a, #2b

Audit:

Review managed Honeywell Android device configuration settings to determine if the mobile device is enforcing a screen-lock policy that will lock the display after a period of 15 minutes or less of inactivity.
Note: Honeywell Android 13 does not support the 15-minute increment. The available allowable selection is 10 minutes and then increases to 30 minutes. Therefore, the control must be set to 10 minutes.
This validation procedure is performed on both the EMM Administration Console and the Android 13 device.
On the EMM console:
COBO:

1. Open "Lock screen restrictions".
2. Verify that "Max time to screen lock" is set to "600".
   Note: The units are in seconds.

COPE:

1. Open "Lock screen restrictions".
2. Select "Personal Profile".
3. Verify that "Max time to screen lock" is set to "600".
   Note: The units are in seconds.

On the managed Honeywell Android 13 device:
COBO and COPE:

1. Open Settings >> Display.
2. Tap "Screen timeout".
3. Verify that the Screen timeout value is set to "600" seconds or less.

If the EMM console device policy is not set to enable a screen-lock policy that will lock the display after a period of inactivity of 600 seconds or less, this is a finding.

Remediation:

Configure the Honeywell Android 13 device to enable a screen-lock policy of 15 minutes for the max period of inactivity.
Note: Honeywell Android 13 does not support the 15-minute increment. The available allowable selection is 10 minutes and then increases to 30 minutes. Therefore, the control must be set to 10 minutes.
On the EMM console:
COBO:

1. Open "Lock screen restrictions".
2. Set "Max time to screen lock" to "600".
   Note: The units are in seconds.

COPE:

1. Open "Lock screen restrictions".
2. Select "Personal Profile".
3. Set "Max time to screen lock" to "600".
   Note: The units are in seconds.

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

1.5 HONW-13-006400 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Honeywell Android 13 must be configured to not allow more than 10 consecutive failed authentication attempts.

```
GROUP ID: V-274286
RULE ID: SV-274286r1100311
```

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 fewer 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.

SFR ID: FMT_SMF_EXT.1.1 #2c, FIA_AFL_EXT.1.5

Audit:

Review managed Honeywell Android 13 device configuration settings to determine if the mobile device has the maximum number of consecutive failed authentication attempts set at 10 or fewer.
This validation procedure is performed on both the EMM Administration Console and the managed Honeywell Android 13 device.
On the EMM console:
COBO:

1. Open "Lock screen" settings.
2. Open "Lock screen restrictions".
3. Verify that "Max password failures for local wipe" is set to a number between 1 and 10.

COPE:

1. Open "Lock screen" settings.
2. Open "Lock screen restrictions".
3. Select "Personal Profile".
4. Verify that "Max password failures for local wipe" is set to a number between 1 and 10.

On the managed Honeywell Android 13 device:
COBO and COPE:

1. Lock the device screen.
2. Attempt to unlock the screen and validate that the device autowipes after a specified number of invalid entries.
   Note: Perform this verification only with a test phone set up with a production profile.

If the EMM console device policy is not set to the maximum number of consecutive failed authentication attempts at 10 or fewer, or if on the managed Honeywell Android 13 device, the device policy is not set to the maximum number of consecutive failed authentication attempts at 10 or fewer, this is a finding.

Remediation:

Configure the Honeywell Android 13 device to allow only 10 or fewer consecutive failed authentication attempts.
On the EMM console:
COBO:

1. Open "Lock screen" settings.
2. Open "Lock screen restrictions".
3. Set "Max password failures for local wipe" to a number between 1 and 10.

COPE:

1. Open "Lock screen" settings.
2. Open "Lock screen restrictions".
3. Select "Personal Profile".
4. Set "Max password failures for local wipe" to a number between 1 and 10.

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

1.6 HONW-13-006500 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Honeywell Android 13 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-274287
RULE ID: SV-274287r1100314
```

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.

SFR ID: FMT_SMF_EXT.1.1 #8a

Audit:

Review managed Honeywell Android 13 device configuration settings to determine if the mobile device has only approved application repositories (DOD-approved commercial app repository, EMM server, and/or mobile application store).
This validation procedure is performed on both the EMM Administration Console and the managed Honeywell Android 13 device.
On the EMM console:
COBO and COPE:

1. Open "Set user restrictions".
2. Verify that "Disallow install unknown sources" is toggled to "ON".
3. Verify that "Disallow installs from unknown sources globally" is toggled to "ON".

On the Honeywell Android 13 device:
COBO and COPE:

1. Open Settings >> Apps >> Special app access.
2. Open "Install unknown apps".
3. Verify that the list of apps is blank or if an app is on the list, "Disabled by admin" is listed under the app name.

If the EMM console device policy is not set to allow connections to only approved application repositories, or on the managed Honeywell Android 13 device, the device policy is not set to allow connections to only approved application repositories, this is a finding.

Remediation:

Configure the Honeywell Android 13 device to disable unauthorized application repositories.
On the EMM console:
COBO and COPE:

1. Open "Set user restrictions".
2. Toggle "Disallow install unknown sources" to "ON".
3. Toggle "Disallow installs from unknown sources globally" to "ON".

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.7 HONW-13-006600 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Honeywell Android 13 must be configured to enforce an application installation policy by specifying an application allowlist that restricts applications by the following characteristics: [selection: list of digital signatures, cryptographic hash values, names, application version].

```
GROUP ID: V-274288
RULE ID: SV-274288r1100317
```

Rationale:

The application allowlist, 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 operating system (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.

Requiring all authorized applications to be in an application allowlist prevents the execution of any applications (e.g., unauthorized, malicious) that are not part of the allowlist. Failure to configure an application allowlist 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.

The application allowlist, in addition to controlling the installation of applications on the MD, must control user access/execution of all core applications (included in the OS by the OS vendor) and preinstalled applications (provided by the MD vendor and wireless carrier), or the MD must provide an alternate method of restricting user access/execution to core and preinstalled applications.

SFR ID: FMT_SMF_EXT.1.1 #8b

Audit:

Review managed Honeywell Android 13 device configuration settings to determine if the mobile device has an application allowlist configured. Verify that all applications listed on the allowlist have been approved by the authorizing official (AO).
On the EMM console:
COBO and COPE:

1. Go to the Android app catalog for managed Google Play.
2. Verify that all selected apps are AO approved.

On the managed Honeywell Android 13 device:
COBO and COPE:

1. Open the managed Google Play Store.
2. Verify that only the approved apps are visible.

Note: Managed Google Play is an allowed App Store.
If the EMM console list of selected managed Google Play apps includes nonapproved apps, this is a finding.
Note: The application allowlist will include approved core applications (included in the OS by the OS vendor) and preinstalled applications (provided by the MD vendor and wireless carrier), or the MD must provide an alternate method of restricting user access/execution to core and preinstalled applications. For Honeywell Android, there are no preinstalled applications.

Remediation:

Configure the Honeywell Android 13 device to use an application allowlist.
On the EMM console:
COBO and COPE:

1. Go to the Android app catalog for managed Google Play.
2. Select apps to be available (only approved apps).
3. Push updated policy to the device.

Note: Managed Google Play is an allowed App Store.

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4::CM-7 (2)
- NIST SP 800-53 Revision 5::CM-7 (2)

1.8 HONW-13-006700 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Honeywell Android 13 allowlist 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;
- Voice assistant application if available when MD is locked;
- Voice dialing application if available when MD is locked;
- Allows synchronization of data or applications between devices associated with user;
- Payment processing; and
- Allows unencrypted (or encrypted but not FIPS 140-3 validated) data sharing with other MDs, display screens (screen mirroring), or printers.

```
GROUP ID: V-274289
RULE ID: SV-274289r1100320
```

Rationale:

Requiring all authorized applications to be in an application allowlist prevents the execution of any applications (e.g., unauthorized, malicious) that are not part of the allowlist. Failure to configure an application allowlist 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 allowlist, 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 operating system (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.

SFR ID: FMT_SMF_EXT.1.1 #8b

Audit:

Review managed Honeywell Android 13 device configuration settings to determine if the mobile device has an application allowlist configured and that the application allowlist does 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;
- Voice assistant application if available when MD is locked;
- Voice dialing application if available when MD is locked;
- Allows synchronization of data or applications between devices associated with user;
- Payment processing; and
- Allows unencrypted (or encrypted but not FIPS 140-3 validated) data sharing with other MDs, display screens (screen mirroring), or printers.

This validation procedure is performed only on the EMM Administration Console.
On the EMM console:

1. Review the list of selected Managed Google Play apps.
2. Review the details and privacy policy of each selected app to verify that the app does not include prohibited characteristics.

If the EMM console device policy includes applications with unauthorized characteristics, this is a finding.

Remediation:

Configure the Honeywell Android 13 device application allowlist to exclude 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;
- Voice assistant application if available when MD is locked;
- Voice dialing application if available when MD is locked;
- Allows synchronization of data or applications between devices associated with user;
- Payment processing; and
- Allows unencrypted (or encrypted but not FIPS 140-3 validated) data sharing with other MDs, display screens (screen mirroring), or printers.

On the EMM console:

1. Go to the Android app catalog for managed Google Play.
2. Before selecting an app, review the app details and privacy policy to ensure the app does not include prohibited characteristics.

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

1.9 HONW-13-006800 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Honeywell Android 13 must be configured to not display the following (work profile) notifications when the device is locked: [selection:

a. email notifications b. calendar appointments c. contact associated with phone call notification d. text message notification e. other application-based notifications f. all notifications].

```
GROUP ID: V-274290
RULE ID: SV-274290r1100323
```

Rationale:

Many mobile devices display notifications on the lock screen so that 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 view 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.

SFR ID: FMT_SMF_EXT.1.1 #18

Audit:

Review managed Honeywell Android 13 device settings to determine if the Honeywell Android 13 device displays (work profile) notifications on the lock screen. Notifications of incoming phone calls are acceptable even when the device is locked.
This validation procedure is performed on both the EMM Administration Console and the managed Honeywell Android 13 device.
On the EMM console:
COBO:

1. Open "Lock screen" settings.
2. Open "Lock screen restrictions".
3. Verify that "Disable unredacted notifications" is toggled to "ON".

COPE:

1. Open "Lock screen" settings.
2. Open "Lock screen restrictions".
3. Select "Work Profile".
4. Verify that "Disable unredacted notifications" is toggled to "ON".

On the managed Honeywell Android 13 device:
COBO:

1. Go to Settings >> Display >> Lock screen.
2. Tap on "Privacy".
3. Verify that "Show sensitive content only when unlocked" is selected.

COPE:

1. Go to Settings >> Display >> Lock screen.
2. Tap on "When work profile is locked".
3. Verify that "Hide sensitive work content" is selected.

If the EMM console device policy allows work notifications on the lock screen, or the managed Honeywell Android 13 device allows work notifications on the lock screen, this is a finding.

Remediation:

Configure the Honeywell Android 13 device to not display (work profile) notifications when the device is locked.
On the EMM console:
COBO:

1. Open "Lock screen" settings.
2. Open "Lock screen restrictions".
3. Toggle "Disable unredacted notifications".

COPE:

1. Open "Lock screen" settings.
2. Open "Lock screen restrictions".
3. Select "Work Profile".
4. Toggle "Disable unredacted notifications".

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)

1.10 HONW-13-007200 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Honeywell Android 13 must be configured to disable trust agents.

```
GROUP ID: V-274294
RULE ID: SV-274294r1100335
```

Rationale:

Trust agents allow a user to unlock a mobile device without entering a passcode when the mobile device is, for example, connected to a user-selected Bluetooth device or in a user-selected location. This technology would allow unauthorized users to have access to DOD sensitive data if compromised. By not permitting the use of nonpassword authentication mechanisms, users are forced to use passcodes that meet DOD passcode requirements.

SFR ID: FMT_SMF_EXT.1.1 #22, FIA_UAU.5.1

Audit:

Review device configuration settings to confirm that trust agents are disabled. This procedure is performed on both the EMM Administration Console and the managed Honeywell Android 13 device.
On the EMM console:
COBO:

1. Open "Lock screen restrictions".
2. Verify that "Disable trust agents" is toggled to "ON".

COPE:

1. Open "Lock screen restrictions".
2. Select "Personal Profile".
3. Verify that "Disable trust agents" is toggled to "ON".
4. Select "Work Profile".
5. Verify that "Disable trust agents" is toggled to "ON".

On the managed Honeywell Android 13 device:
COBO and COPE:

1. Open Settings.
2. Tap "Security".
3. Tap "More security settings".
4. Tap "Trust agents".
5. Verify that all listed trust agents are disabled and cannot be enabled.

If on the EMM console, "disable trust agents" is not selected, or on the managed Honeywell Android 13 device a trust agent can be enabled, this is a finding.

Remediation:

Configure the Honeywell Android 13 device to disable trust agents.
On the EMM console:
COBO:

1. Open "Lock screen restrictions".
2. Toggle "Disable trust agents" to "ON".

COPE:

1. Open "Lock screen restrictions".
2. Select "Personal Profile".
3. Toggle "Disable trust agents" to "ON".
4. Select "Work Profile".
5. Toggle "Disable trust agents" to "ON".

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)

1.11 HONW-13-007400 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Honeywell Android 13 must be configured to disable developer modes.

```
GROUP ID: V-274296
RULE ID: SV-274296r1100341
```

Rationale:

Developer modes expose features of the mobile operating system that are not available during standard operation. An adversary may leverage a vulnerability inherent in a developer mode to compromise the confidentiality, integrity, and availability of DOD sensitive information. Disabling developer modes mitigates this risk.

SFR ID: FMT_SMF_EXT.1.1 #26

Audit:

Review managed Honeywell Android 13 device configuration settings to determine whether developer mode is enabled.
This validation procedure is performed on both the EMM Administration Console and the managed Honeywell Android 13 device.
On the EMM console:
COBO:

1. Open "Set user restrictions".
2. Verify that "Disallow debugging features" is toggled to "ON".

COPE:

1. Open "Set user restrictions".
2. Verify that "Disallow debugging features" is toggled to "ON".
3. Open "Set user restrictions on parent".
4. Verify that "Disallow debugging features" is toggled to "ON".

On the managed Honeywell Android 13 device:
COBO and COPE:

1. Go to Settings >> System.
2. Verify that "Developer Options" is not listed.
3. Go to Settings >> About Phone.
4. Tap on the Build Number to try to enable Developer Options and validate that action is blocked.

If the EMM console device policy is not set to disable developer mode, or on the managed Honeywell Android 13 device, the device policy is not set to disable developer mode, this is a finding.

Remediation:

Configure the Honeywell Android 13 device to disable developer modes.
On the EMM console:
COBO:

1. Open "Set user restrictions".
2. Toggle "Disallow debugging features" to "ON".

COPE:

1. Open "Set user restrictions".
2. Toggle "Disallow debugging features" to "ON".
3. Open "Set user restrictions on parent".
4. Toggle "Disallow debugging features" to "ON".

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

1.12 HONW-13-007700 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Honeywell Android 13 must be configured to display the DOD advisory warning message at startup or each time the user unlocks the device.

```
GROUP ID: V-274299
RULE ID: SV-274299r1100350
```

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.

SFR ID: FMT_SMF_EXT.1.1 #36

Audit:

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

1. By placing the DOD warning banner text in the user agreement signed by each managed Android 13 device user (preferred method).
2. By configuring the warning banner text on the EMM console and installing the banner on each managed Android 13 mobile device.

Determine which method is used at the Honeywell Android 13 device site and follow the appropriate validation procedure below.
Validation Procedure for Method #1:
Review the signed user agreements for several Honeywell Android 13 device users and verify that the agreement includes the required DOD warning banner text.
Validation Procedure for Method #2:
On the EMM console:
COBO:

1. Open "Lock screen restrictions".
2. Select "Lock screen message".
3. Verify the message.

COPE:

1. Open "Lock screen restrictions".
2. Select "Personal Profile".
3. Select "Lock screen message".
4. Verify the message.

If, for Method #1, the required warning banner text is not on all signed user agreements reviewed, this is a finding.
If, for Method #2, the EMM console device policy is not set to display a warning banner with the appropriate designated wording, or on the managed Honeywell Android 13 device, the device policy is not set to display a warning banner with the appropriate designated wording, this is a finding.

Remediation:

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

1. By placing the DOD warning banner text in the user agreement signed by each Honeywell Android 13 device user (preferred method).
2. By configuring the warning banner text on the EMM console and installing the banner on each Honeywell Android 13 mobile device.

On the EMM console:
COBO:

1. Open "Lock screen restrictions".
2. Select "Lock screen message".
3. Enter in message.

COPE:

1. Open "Lock screen restrictions".
2. Select "Personal Profile".
3. Select "Lock screen message".
4. Enter in message.

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

1.13 HONW-13-007800 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Honeywell Android 13 must be configured to generate audit records for the following auditable events: Detected integrity violations.

```
GROUP ID: V-274300
RULE ID: SV-274300r1100353
```

Rationale:

Audit logs enable monitoring of security-relevant events and subsequent forensics when breaches occur. They help identify attacks so that breaches can be prevented or limited in their scope. They facilitate analysis to improve performance and security. The Requirement statement lists key events for which the system must generate an audit record.

Note: This requirement applies only to integrity violation detections that can be logged by the audit logging component.

SFR ID: FMT_SMF_EXT.1.1 #37, FAU_GEN.1.1 #6 (FPT_TST_EXT.2/PREKERNAL)

Audit:

Review managed Honeywell Android 13 device configuration settings to determine if the mobile device is configured to generate audit records for the following auditable events: Detected integrity violations.
This validation procedure is performed only on the EMM Administration Console.
On the EMM console:
COBO and COPE:

1. Open the "Device owner management" section.
2. Verify that "Enable security logging" is toggled to "ON".

If the EMM console device policy is not set to enable security logging, this is a finding.

Remediation:

Configure the Honeywell Android 13 device to generate audit records for the following auditable events: Detected integrity violations.
On the EMM console:
COBO and COPE:

1. Open "Device owner management" section.
2. Toggle "Enable security logging" to "ON".

Additional Information:

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

1.14 HONW-13-008400 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Honeywell Android 13 must be configured to disable USB mass storage mode.

```
GROUP ID: V-274304
RULE ID: SV-274304r1100365
```

Rationale:

USB mass storage mode enables the transfer of data and software from one device to another. This software can include malware. When USB mass storage is enabled on a mobile device, it becomes a potential vector for malware and unauthorized data exfiltration. Prohibiting USB mass storage mode mitigates this risk.

SFR ID: FMT_SMF_EXT.1.1 #39

Audit:

Review managed Honeywell Android 13 device configuration settings to determine if the mobile device has a USB mass storage mode and whether it has been disabled.
This validation procedure is performed on both the EMM Administration Console and the managed Honeywell Android 13 device.
On the EMM console:
COBO:

1. Open "User restrictions".
2. Open "Set user restrictions".
3. Verify that "Disallow USB file transfer" is toggled to "ON".

COPE:

1. Open "User restrictions".
2. Open "Set user restrictions on parent".
3. Verify that "Disallow USB file transfer" is toggled to "ON".

On the managed Honeywell Android 13 device:

1. Plug a USB cable into the managed Honeywell Android 13 device and connect to a non-DOD network-managed PC.
2. Go to Settings >> Connected devices >> USB.
3. Verify that "No data transfer" is selected.

If the EMM console device policy is not set to disable USB mass storage mode, or on the managed Honeywell Android 13 device, the device policy is not set to disable USB mass storage mode, this is a finding.

Remediation:

Configure the Honeywell Android 13 device to disable USB mass storage mode.
On the EMM console:
COBO:

1. Open "User restrictions".
2. Open "Set user restrictions".
3. Toggle "Disallow USB file transfer" to "ON".

COPE:

1. Open "User restrictions".
2. Open "Set user restrictions on parent".
3. Toggle "Disallow USB file transfer" to "ON".

Additional Information:

CCI-002546 Physically or logically disable or remove organization-defined connection ports or input/output devices on organization-defined systems or system components.

- NIST SP 800-53 Revision 4::SC-41
- NIST SP 800-53 Revision 5::SC-41

1.15 HONW-13-008500 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Honeywell Android 13 must be configured to not allow backup of [all applications, configuration data] to locally connected systems.

```
GROUP ID: V-274305
RULE ID: SV-274305r1100368
```

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.

SFR ID: FMT_SMF_EXT.1.1 #40

Audit:

Review managed Honeywell Android 13 device configuration settings to determine if the capability to back up to a locally connected system has been disabled.
This validation procedure is performed on both the EMM Administration Console and the managed Honeywell Android 13 device.
On the EMM console:
COBO and COPE:

1. Open "Device owner management".
2. Verify that "Enable backup service" is toggled to "OFF".

On the managed Honeywell Android 13 device:
COBO:

1. Go to Settings >> System >> Backup.
2. Verify that Backup settings is "Not available".

COPE:

1. Go to Settings >> System >> Backup.
2. Select "Work".
3. Verify that Backup settings is "Not available".

If the EMM console device policy is not set to disable the capability to back up to a locally connected system, or on the managed Honeywell Android 13 device, the device policy is not set to disable the capability to back up to a locally connected system, and this is a finding.

Remediation:

Configure the Honeywell Android 13 device to disable backup to locally connected systems.
On the EMM console:
COBO and COPE:

1. Open "Device owner management".
2. Toggle "Enable backup service" to "OFF".

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

1.16 HONW-13-008600 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Honeywell Android 13 must be configured to not allow backup of [all applications, configuration data] to remote systems.

```
GROUP ID: V-274306
RULE ID: SV-274306r1100371
```

Rationale:

Backups to remote systems (including cloud backup) can leave data vulnerable to breach on the external systems, which often offer less protection than the mobile operating system. Where the remote backup involves a cloud-based solution, the backup capability is often used to synchronize data across multiple devices. In this case, DOD devices may synchronize DOD sensitive information to a user's personal device or other unauthorized computers that are vulnerable to breach. Disallowing remote backup mitigates this risk.

SFR ID: FMT_SMF_EXT.1.1 #40

Audit:

Review managed Honeywell Android 13 device configuration settings to determine if the capability to back up to a remote system has been disabled.
Note: Because personal accounts cannot be added to the work profile (HONW-13-009800), this control only impacts personal profile accounts. The site can allow backup based on local policy.
This validation procedure is performed on both the EMM Administration Console and the managed Honeywell Android 13 device.
On the EMM console:
COBO and COPE:

1. Open "Device owner management".
2. Verify that "Enable backup service" is toggled to "OFF".

On the managed Honeywell Android 13 device:
COBO:

1. Go to Settings >> System >> System >> Backup.
2. Verify that Backup settings is "Not available".

COPE:

1. Go to Settings >> System >> System >> Backup.
2. Select "Work".
3. Verify that Backup settings is "Not available".

If the EMM console device policy is not set to disable the capability to back up to a remote system, or on the managed Honeywell Android 13 device, the device policy is not set to disable the capability to back up to a remote system, this is a finding.

Remediation:

Configure the Honeywell Android 13 device to disable backup to remote systems (including commercial clouds).
On the EMM console:
COBO and COPE:

1. Open "Device owner management".
2. Toggle "Enable backup service" to "OFF".

Note: Because personal accounts cannot be added to the work profile (HONW-13-009800), this control only impacts personal profile accounts. The site can allow backup based on local policy.

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

1.17 HONW-13-008700 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Honeywell Android 13 must be configured to enable authentication of personal hotspot connections to the device using a preshared key.

```
GROUP ID: V-274307
RULE ID: SV-274307r1100374
```

Rationale:

If no authentication is required to establish personal hotspot connections, an adversary may be able to use that device to perform attacks on other devices or networks without detection. A sophisticated adversary may also be able to exploit unknown system vulnerabilities to access information and computing resources on the device. Requiring authentication to establish personal hotspot connections mitigates this risk.

Application note: If hotspot functionality is permitted, it must be authenticated via a preshared key. There is no requirement to enable hotspot functionality, and it is recommended this functionality be disabled by default.

SFR ID: FMT_SMF_EXT.1.1 #41

Audit:

This is a User-Based Enforcement (UBE) control.
Check a sample of Honeywell phones at the site and verify that the Wi-Fi hotspot preshared key (password) is set to "WPA2/WPA3-Personal" or "WPA3-Personal".

1. Go to Settings >> Network & Internet >> Hotspot & tethering.
2. Enable "Wi-Fi hotspot".
3. On the left of the slide, tap on "Wi-Fi Hotspot" to bring up the configuration options.
4. Click on the "Security" link and verify that either "WPA2/WPA3-Personal" or "WPA3-Personal" is selected.

If the Wi-Fi hotspot security is not set to "WPA2/WPA3-Personal" or "WPA3-Personal", this is a finding.

Remediation:

This is a UBE control.
Train users to not change the default Wi-Fi hotspot security setting: 15-character complex Wi-Fi hotspot preshared key (password) ("WPA2/WPA3-Personal" or WPA3-Personal"). (Refer to HONW-13-009800.)
If the required preshared key is not set up, train users to use the following procedure to set up the required setting:

1. Go to Settings >> Network & Internet >> Hotspot & tethering.
2. Enable "Wi-Fi hotspot".
3. On the left of the slide, tap on "Wi-Fi Hotspot" to bring up the configuration options.
4. Click on the "Security" link and select either "WPA2/WPA3-Personal" or "WPA3-Personal".

Additional Information:

CCI-001443 Protect wireless access to the system using authentication of users and/or devices.

- NIST SP 800-53::AC-18 (1)
- NIST SP 800-53A::AC-18 (1).1
- NIST SP 800-53 Revision 4::AC-18 (1)
- NIST SP 800-53 Revision 5::AC-18 (1)

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)

1.18 HONW-13-009000 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Honeywell Android 13 must be configured to disable multiuser modes.

```
GROUP ID: V-274309
RULE ID: SV-274309r1100447
```

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.

SFR ID: FMT_SMF_EXT.1.1 #47a

Audit:

Review documentation on the managed Honeywell Android 13 device and inspect the configuration on the Honeywell Android device to disable multiuser modes.
This validation procedure is performed on both the EMM Administration Console and the managed Honeywell Android 13 device.
On the EMM console:
COBO, COPE, and BYOAD:

1. Open "User restrictions".
2. Open "Set user restrictions".
3. Verify that "Disallow modify accounts" is toggled to "ON".

Note: This applies only to the work profile for BYOAD. A user can modify accounts in the personal profile.
On the managed Honeywell Android 13 device:
COBO and COPE:

1. Go to Settings >> Passwords & accounts >> Accounts for Owner.
2. Tap "Add account".
3. Verify that the action is not allowed.

BYOAD:

1. Go to Settings >> Passwords & accounts >> Work.
2. Tap "Add account".
3. Verify that the action is not allowed.

If the EMM console device policy is not set to disable multiuser modes or on the managed Honeywell Android 13 device, the device policy is not set to disable multiuser modes, this is a finding.

Remediation:

Configure the Honeywell Android 13 device to disable multiuser modes.
On the EMM console:
COBO, COPE, and BYOAD:

1. Open "User restrictions".
2. Open "Set user restrictions".
3. Toggle "Disallow modify accounts" to ON.

Note: This only applies to the work profile for BYOAD. A user can modify accounts in the personal profile.

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

1.19 HONW-13-009400 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Honeywell Android 13 must be configured to disable Bluetooth or configured via User-Based Enforcement (UBE) to allow Bluetooth for only Headset Profile (HSP), Hands-Free Profile (HFP), and Serial Port Profile (SPP).

```
GROUP ID: V-274313
RULE ID: SV-274313r1100392
```

Rationale:

Some Bluetooth profiles provide the capability for remote transfer of sensitive DOD data without encryption or otherwise do not meet DOD IT security policies and therefore must be disabled.

SFR ID: FMT_SMF_EXT.1.1/BLUETOOTH BT-8

Audit:

Determine if the authorizing official (AO) has approved the use of Bluetooth at the site. If the AO has not approved the use of Bluetooth, verify that Bluetooth has been disabled.
On the EMM console:
COBO:

1. Open "User restrictions" section.
2. Verify that "Disallow Bluetooth" is toggled to "ON".

COPE:

1. Open "User restrictions on parent" section.
2. Verify that "Disallow Bluetooth" is toggled to "ON".

On the managed Honeywell Android 13 device:
COBO and COPE:

1. Go to Settings >> Connected Devices >> Connection Preferences >> Bluetooth.
2. Verify that "Use Bluetooth" is set to "OFF" and cannot be toggled to "ON".

If the AO has approved the use of Bluetooth, on the managed Android 13 device:

1. Go to Settings >> Connected Devices.
2. Verify that only approved Bluetooth-connected devices using approved profiles are listed.

If the AO has not approved the use of Bluetooth, and Bluetooth use is not disabled via an EMM managed device policy, this is a finding.
If the AO has approved the use of Bluetooth, and Bluetooth devices using unauthorized Bluetooth profiles are listed on the device under "Connected devices", this is a finding.

Remediation:

Configure the Honeywell Android 13 device to disable Bluetooth, or if the AO has approved the use of Bluetooth (for example, for car hands-free use), train the user to connect to only authorized Bluetooth devices using only HSP, HFP, or SPP Bluetooth-capable devices (UBE).
To disable Bluetooth, use the following procedure:
On the EMM console:
COBO:

1. Open "User restrictions" section.
2. Toggle "Disallow Bluetooth" to "ON".

COPE:

1. Open "User restrictions on parent" section.
2. Toggle "Disallow Bluetooth" to "ON".

The user training requirement is satisfied in requirement HONW-13-009800.

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

CCI-001761 Defines the functions, ports, protocols, software, and services within the information system that are to be disabled or removed when deemed unnecessary and/or nonsecure.

- NIST SP 800-53 Revision 4::CM-7 (1) (b)
- NIST SP 800-53 Revision 5::CM-7 (1) (b)

1.20 HONW-13-009500 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Honeywell Android 13 must be configured to disable ad hoc wireless client-to-client connection capability.

```
GROUP ID: V-274314
RULE ID: SV-274314r1100448
```

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.

SFR ID: FMT_SMF_EXT.1.1/WLAN

Audit:

Review the configuration to determine if the Honeywell Android devices are disallowing Wi-Fi Direct.
This validation procedure is performed on both the management tool and the Honeywell Android 13 device.
On the management tool, in the user restrictions, verify that "Wi-Fi Direct" has been set to "Disallow".
On the Honeywell Android device:

1. Open Settings >> Connections >> Wi-Fi.
2. From the hamburger menu, select Wi-Fi Direct.
3. Verify that Wi-Fi Direct cannot be selected.

If on the management tool "Wi-Fi Direct" is not set to "Disallow", or on the Honeywell Android device a Wi-Fi direct device is listed that can be connected to, this is a finding.

Remediation:

Configure the Honeywell Android devices to disallow Wi-Fi Direct.
On the management tool, in the user restrictions, set "Wi-Fi Direct" to "Disallow".
Wi-Fi Direct connections and pairing between devices will become unavailable.

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

1.21 HONW-13-009600 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

All mobile Honeywell cryptography must be configured to be in FIPS 140-3 validated mode.

```
GROUP ID: V-274315
RULE ID: SV-274315r1100449
```

Rationale:

Unapproved cryptographic algorithms cannot be relied on to provide confidentiality or integrity, and DOD data could be compromised as a result. The most common vulnerabilities with cryptographic modules are those associated with poor implementation. FIPS 140-3 validation provides assurance that the relevant cryptography has been implemented correctly. FIPS 140-3 validation is also a strict requirement for use of cryptography in the federal government for protecting unclassified data.

SFR ID: FCS

Audit:

Review the configuration to determine if the Honeywell Android devices are in FIPS mode.
On the MDM console (for SDM660 only):

1. In the MDM console, load the active DeviceConfig.xml for the managed device.
2. Verify that item DeviceConfig >> HoneywellSetting >> EnforceOSFipsMode has a value of "1" for "Enable OS FIPS Mode".

On the Honeywell Android 13 device (SDM660 only):

1. Open Settings >> Honeywell Settings >> FIPS Enforce Mode.
2. Verify that "FIPS Enforce Mode" is enabled.

If "FIPS Enforce Mode" is not enabled, this is a finding.

Remediation:

On the MDM console (for SDM660 only):

1. Ask the MDM administrator to edit the following item in DeviceConfig.xml:
   Modify item: DeviceConfig >> HoneywellSetting >> EnforceOSFipsMode.
   Value sample: 1: Enable OS FIPS mode; 0: Disable OS FIPS mode.
2. In the MDM console, the MDM administrator will package this DeviceConfig.xml and push this package to the CN80G device.

On the Honeywell Android 13 device (SDM660 only):

1. Open Settings >> Honeywell Settings >> FIPS Enforce Mode.
2. Enable "FIPS Enforce Mode".

Additional Information:

CCI-002450 Implement organization-defined types of cryptography for each specified cryptography use.

- NIST SP 800-53 Revision 4::SC-13
- NIST SP 800-53 Revision 5::SC-13 b

1.22 HONW-13-009800 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Honeywell Android 13 users must complete required training.

```
GROUP ID: V-274318
RULE ID: SV-274318r1100455
```

Rationale:

The security posture of Honeywell 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 the use of an unmanaged personal space, the user 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 Honeywell mobile device may become compromised, and DOD sensitive data may become compromised.

SFR ID: NA

Audit:

Review a sample of site User Agreements for Honeywell Android 13 device users or similar training records and training course content.
Verify that the Honeywell Android 13 device users have completed the required training. The intent is that required training is renewed on a periodic basis in a time period determined by the AO.
If any Honeywell Android 13 device user has not completed the required training, this is a finding.

Remediation:

All Honeywell Android 13 device users must complete training on the following training topics (users must acknowledge that they have reviewed training via a signed User Agreement or similar written record):

- Operational security concerns introduced by unmanaged applications/unmanaged personal space, including applications using global positioning system (GPS) tracking.
- Need to ensure no DOD data is saved to the personal space 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 that a factory data reset is performed prior to device hand-off. Follow mobility service provider decommissioning procedures as applicable.
- How to configure the following UBE controls (users must configure the control) on the Honeywell device:
  **Secure use of Calendar Alarm.
  **Local screen mirroring and mirroring procedures (authorized/not authorized for use).
  **Do not upload DOD contacts via smart call and caller ID services.
  **Do not configure a DOD network (work) VPN profile on any third-party VPN client installed in the personal space.
  **If Bluetooth connections are approved for mobile device, types of allowed connections (for example, car hands-free, but not Bluetooth wireless keyboard).
  **How to perform a full device wipe.
  **Use default Wi-Fi hotspot password: 15-character complex Wi-Fi hotspot preshared password enabled ("WPA2/WPA3-personal").
- AO guidance on acceptable use and restrictions, if any, on downloading and installing personal apps and data (music, photos, etc.) in the Honeywell device personal space.

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

1.23 HONW-13-009900 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Honeywell Android 13 must be configured to enforce that Wi-Fi Sharing is disabled.

```
GROUP ID: V-274319
RULE ID: SV-274319r1100410
```

Rationale:

Wi-Fi Sharing is an optional configuration of Wi-Fi Tethering/Mobile Hotspot, which allows the device to share its Wi-Fi connection with other wirelessly connected devices instead of its mobile (cellular) connection.

Wi-Fi Sharing grants the "other" device access to a corporate Wi-Fi network and may possibly bypass the network access control mechanisms. This risk can be partially mitigated by requiring the use of a preshared key for personal hotspots.

SFR ID: FMT_SMF_EXT.1.1 #47

Audit:

Review device configuration settings to confirm Wi-Fi Sharing is disabled.
Mobile Hotspot must be enabled to enable Wi-Fi Sharing. If the authorizing official (AO) has not approved Mobile Hotspot, and it has been verified as disabled on the EMM console, no further action is needed.
If Mobile Hotspot is being used, use the following procedure to verify that Wi-Fi Sharing is disabled:
On the EMM console:
COBO:

1. Open "Set user restrictions".
2. Verify that "Disallow sharing admin configured Wi-Fi" is set to "ON".

COPE:

1. Open "Set user restrictions on parent".
2. Verify that "Disallow sharing admin configured Wi-Fi" is set to "ON".

If on the EMM console, "Disallow sharing admin configured Wi-Fi" is not enabled, this is a finding.

Remediation:

Configure the Honeywell Android 13 device to disable Wi-Fi Sharing.
Mobile Hotspot must be enabled to enable Wi-Fi Sharing. If the AO has not approved Mobile Hotspot, and it has been disabled on the EMM console, no further action is needed.
If Mobile Hotspot is being used, use the following procedure to disable Wi-Fi Sharing:
On the EMM console:
COBO:

1. Open "Set user restrictions".
2. Toggle "Disallow sharing admin configured Wi-Fi" to "ON".

COPE:

1. Open "Set user restrictions on parent".
2. Toggle "Disallow sharing admin configured Wi-Fi" to "ON".

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

1.24 HONW-13-010000 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Honeywell Android 13 must have the DOD root and intermediate PKI certificates installed.

```
GROUP ID: V-274320
RULE ID: SV-274320r1100413
```

Rationale:

DOD root and intermediate PKI certificates are used to verify the authenticity of PKI certificates of users and web services. If the root and intermediate certificates are not available, an adversary could falsely sign a certificate in such a way that it could not be detected. Providing access to the DOD root and intermediate PKI certificates greatly diminishes the risk of this attack.

SFR ID: FMT_SMF_EXT.1.1 #47

Audit:

Review device configuration settings to confirm that the DOD root and intermediate PKI certificates are installed.
This procedure is performed on both the EMM Administration Console and the managed Honeywell Android 13 device.
The current DOD root and intermediate PKI certificates may be obtained in self-extracting zip files at https://cyber.mil/pki-pke (for NIPRNet).
On the EMM console, verify that the DOD root and intermediate certificates are part of a device and/or work profile that is being pushed down to the devices.
On the managed Honeywell Android 13 device:

1. Open Settings.
2. Tap "Security".
3. Tap "More security settings".
4. Tap "Encryption & credentials".
5. Tap "Trusted credentials".
6. Verify that DOD root and intermediate PKI certificates are listed under the User tab in the Work section.

If on the EMM console the DOD root and intermediate certificates are not listed in a profile, or the managed Android 13 device does not list the DOD root and intermediate certificates under the user tab, this is a finding.

Remediation:

Configure the Honeywell Android 13 device to install DOD root and intermediate certificates.
On the EMM console, upload DOD root and intermediate certificates as part of a device and/or work profile.
The current DOD root and intermediate PKI certificates may be obtained in self-extracting zip files at https://cyber.mil/pki-pke (for NIPRNet).

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

1.25 HONW-13-010100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Honeywell Android 13 work profile must be configured to prevent users from adding personal email accounts to the work email app.

```
GROUP ID: V-274321
RULE ID: SV-274321r1100416
```

Rationale:

If the user is able to add a personal email account (POP3, IMAP, EAS) to the work email app, it could be used to forward sensitive DOD data to unauthorized recipients. Restricting email account addition to the administrator or restricting email account addition to allowlisted accounts mitigates this vulnerability.

SFR ID: FMT_SMF_EXT.1.1 #47

Audit:

Review the managed Honeywell Android 13 work profile configuration settings to confirm that users are prevented from adding personal email accounts to the work email app.
This procedure is performed on both the EMM Administrator console and the managed Honeywell Android 13 device.
COPE:
On the EMM console:

1. Open "Set user restrictions".
2. Verify that "Disallow modify accounts" is toggled to "ON".

On the managed Honeywell Android 13 device:

1. Open Settings.
2. Tap "Passwords & accounts".
3. Select "Work".
4. Tap "Add account".
5. Verify that a message is displayed to the user stating, "Action not allowed".

If on the EMM console the restriction to "Disallow modify accounts" is not set, or on the managed Honeywell Android 13 device the user is able to add an account in the Work section, this is a finding.

Remediation:

Configure the Honeywell Android 13 device to prevent users from adding personal email accounts to the work email app.
On the EMM console:
COPE:

1. Open "Set user restrictions".
2. Toggle "Disallow modify accounts" to "ON".

Refer to the EMM documentation to determine how to provision users' work email accounts for the work email app.

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

1.26 HONW-13-010200 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Honeywell Android 13 work profile must be configured to enforce the system application disable list.

```
GROUP ID: V-274322
RULE ID: SV-274322r1100419
```

Rationale:

The system application disable list controls user access to/execution of all core and preinstalled applications.

Core application: Any application integrated into Honeywell Android 13 by Honeywell.

Preinstalled application: Additional noncore applications included in the Honeywell Android 13 build by Honeywell or the wireless carrier.

Some system applications can compromise DOD data or upload users' information to non-DOD-approved servers. A user must be blocked from using such applications that exhibit behavior that can result in compromise of DOD data or DOD user information.

The site administrator must analyze all preinstalled applications on the device and disable all applications not approved for DOD use by configuring the system application disable list.

SFR ID: FMT_SMF_EXT.1.1 #47

Audit:

Review the managed Honeywell Android 13 work profile configuration settings to confirm the system application disable list is enforced. This setting is enforced by default. Verify that only approved system apps have been placed on the core allowlist. This procedure is performed on the EMM Administrator console.
Review the system app allowlist and verify that only approved apps are on the list.
COBO:

1. Open "Apps management" section.
2. Select "Hide apps".
3. Verify that package names of apps are listed.

COPE:

1. Open "Apps management" section.
2. Select "Hide apps on parent".
3. Verify that package names of apps are listed.

If on the EMM console the system app allowlist contains unapproved core apps, this is a finding.

Remediation:

Configure the Honeywell Android 13 device to enforce the system application disable list.
The required configuration is the default configuration when the device is enrolled. If the device configuration is changed, use the following procedure to bring the device back into compliance:
On the EMM console:
COBO:

1. Open "Apps management" section.
2. Select "Hide apps".
3. Enter package names of apps to hide.

COPE:

1. Open "Apps management" section.
2. Select "Hide apps on parent".
3. Enter package names of apps to hide.

Configure a list of approved Honeywell core and preinstalled apps in the core app allowlist.

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

1.27 HONW-13-010600 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Honeywell Android 13 must be configured to disallow configuration of date and time.

```
GROUP ID: V-274323
RULE ID: SV-274323r1100422
```

Rationale:

Determining the correct time a particular application event occurred on a system is critical when conducting forensic analysis and investigating system events.

Periodically synchronizing internal clocks with an authoritative time source is necessary to correctly correlate the timing of events that occur across the enterprise. The three authoritative time sources for Honeywell Android 13 are an authoritative time server that is synchronized with redundant United States Naval Observatory (USNO) time servers as designated for the appropriate DOD network (NIPRNet or SIPRNet), or the Global Positioning System (GPS), or the wireless carrier.

Time stamps generated by the audit system in Honeywell Android 13 must include both date and time. The time may be expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC.

SFR ID: FMT_SMF_EXT.1.1 #47

Audit:

Review the managed Honeywell Android 13 device configuration settings to confirm that autofill services are disabled.
This procedure is performed on both the EMM Administration Console and the managed Honeywell Android 13 device.
On the EMM console:
COBO:

1. Open "Set user restrictions".
2. Verify that "Disallow config date time" is toggled to "ON".

COPE:

1. Open "Set user restrictions on parent".
2. Verify that "Disallow config date time" is toggled to "ON".

On the managed Honeywell Android 13 device:
COBO and COPE:

1. Open Settings.
2. Tap "System".
3. Tap "Date & times".
4. Verify that "Set time automatically" is grayed out and is "Enabled by admin".

If on the EMM console "Disallow config date time" is not set to "On", or on the managed Android 13 device "User network-provided time" is not grayed out, this is a finding.

Remediation:

Configure the Honeywell Android 13 device to set auto network time.
On the EMM console:
COBO:

1. Open "Set user restrictions".
2. Toggle "Disallow config date time" to "ON".

COPE:

1. Open "Set user restrictions on parent".
2. Toggle "Disallow config date time" to "ON".

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

1.28 HONW-13-010800 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Android 13 devices must have the latest available Honeywell Android 13 operating system installed.

```
GROUP ID: V-274325
RULE ID: SV-274325r1100428
```

Rationale:

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

SFR ID: FMT_SMF_EXT.1.1 #47

Audit:

Review device configuration settings to confirm the Honeywell Android device has the most recently released version of managed Honeywell Android 13 installed.
This procedure is performed on both the EMM console and the managed Honeywell Android 13 device.
In the EMM management console, review the version of Honeywell Android 13 installed on a sample of managed devices. This procedure will vary depending on the EMM product.
On the managed Honeywell Android 13 device, to determine the installed operating system version:
COBO and COPE:

1. Open Settings.
2. Tap "About phone".
3. Verify "Build number".

If the installed version of the Honeywell Android 13 operating system on any reviewed devices is not the latest released by Honeywell, this is a finding.

Remediation:

Install the latest released version of the Honeywell Android 13 operating system on all managed Honeywell devices.
Note: Honeywell Android device operating system updates are released directly by Honeywell or can be distributed via the EMM. Check each device manufacturer and/or carriers for current updates.

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

1.29 HONW-13-010900 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Android 13 devices must be configured to disable the use of third-party keyboards.

```
GROUP ID: V-274326
RULE ID: SV-274326r1100431
```

Rationale:

Many third-party keyboard applications are known to contain malware.

SFR ID: FMT_SMF_EXT.1.1 #47

Audit:

Review the managed Honeywell Android 13 configuration settings to confirm that no third-party keyboards are enabled.
This procedure is performed on the EMM console.
On the EMM console:
COBO and COPE:

1. Open "Input methods".
2. Tap "Set input methods".
3. Verify that only the approved keyboards are selected.

If third-party keyboards are allowed, this is a finding.

Remediation:

Configure the Honeywell Android 13 device to disallow the use of third-party keyboards.
On the EMM console:
COBO and COPE:

1. Open "Input methods".
2. Tap "Set input methods".
3. Select only the approved keyboard.

Additionally, administrators can configure application allowlists for Honeywell Play that do not have any third-party keyboards for user installation.

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

1.30 HONW-13-011000 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Android 13 devices must be configured to enable Common Criteria (CC) mode.

```
GROUP ID: V-274327
RULE ID: SV-274327r1100446
```

Rationale:

The CC mode feature is a superset of other features and behavioral changes that are mandatory MDFPP requirements. If CC mode is not implemented, the device will not be operating in the NIAP-certified compliant CC mode of operation.

CC mode implements the following behavioral/functional changes: How the Bluetooth and Wi-Fi keys are stored using different types of encryption.

SFR ID: FMT_SMF_EXT.1.1 #47

Audit:

Review the managed Honeywell Android 13 configuration settings to confirm CC mode is enabled.
This procedure is performed on the EMM console.
COBO and COPE:

1. Open "Device owner management".
2. Verify that "Enable Common Criteria mode" is toggled to "ON".

If CC mode is not enabled, this is a finding.

Remediation:

Configure the Honeywell Android 13 device to implement CC mode.
On the EMM console:
COBO and COPE:

1. Open "Device owner management".
2. Toggle "Enable Common Criteria mode" to "ON".

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

1.31 HONW-13-012200 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Honeywell Android 13 must be configured to disable all data signaling over [assignment: list of externally accessible hardware ports (for example, USB)].

```
GROUP ID: V-274328
RULE ID: SV-274328r1100437
```

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.

SFR ID: FMT_MOF_EXT.1.2 #24

Audit:

Review the device configuration to confirm that the USB port is disabled except for charging the device.
On the EMM console:

1. Open "Set user restrictions".
2. Verify that "Enable USB" is toggled to "OFF".

If on the EMM console the USB port is not disabled, this is a finding.

Remediation:

Configure the Honeywell Android 13 device to disable the USB port (except for charging the device).
COPE and COBO:
On the EMM console:

1. Open "Set user restrictions".
2. Toggle "Enable USB" to "OFF".

Additional Information:

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)

1.32 HONW-13-012300 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Honeywell Android 13 must allow only the administrator (EMM) to install/remove DOD root and intermediate PKI certificates.

```
GROUP ID: V-274316
RULE ID: SV-274316r1100401
```

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.

SFR ID: FMT_MOF_EXT.1.2 #47

Audit:

Review the device configuration to confirm that the user is unable to remove DOD root and intermediate PKI certificates.
On the EMM console:

1. Open "Set user restrictions".
2. Verify that "Disallow config credentials" is toggled to "ON".

On the Honeywell Android 13 device:

1. Open Settings.
2. Tap "Security".
3. Tap "Advanced".
4. Tap "Encryption & credentials".
5. Tap "Trusted credentials".
6. Verify that the user is unable to untrust or remove any work certificates.

If on the Honeywell Android 13 device the user is able to remove certificates, this is a finding.

Remediation:

Configure the Honeywell Android 13 device to prevent a user from removing DOD root and intermediate PKI certificates.
On the EMM console:

1. Open "Set user restrictions".
2. Toggle "Disallow config credentials" to "ON".

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)

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	HONW-13-002800 (Manual)	☐	☐
1.2	HONW-13-006000 (Manual)	☐	☐
1.3	HONW-13-006100 (Manual)	☐	☐
1.4	HONW-13-006300 (Manual)	☐	☐
1.5	HONW-13-006400 (Manual)	☐	☐
1.6	HONW-13-006500 (Manual)	☐	☐
1.7	HONW-13-006600 (Manual)	☐	☐
1.8	HONW-13-006700 (Manual)	☐	☐
1.9	HONW-13-006800 (Manual)	☐	☐
1.10	HONW-13-007200 (Manual)	☐	☐
1.11	HONW-13-007400 (Manual)	☐	☐
1.12	HONW-13-007700 (Manual)	☐	☐
1.13	HONW-13-007800 (Manual)	☐	☐
1.14	HONW-13-008400 (Manual)	☐	☐
1.15	HONW-13-008500 (Manual)	☐	☐
1.16	HONW-13-008600 (Manual)	☐	☐
1.17	HONW-13-008700 (Manual)	☐	☐
1.18	HONW-13-009000 (Manual)	☐	☐
1.19	HONW-13-009400 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	HONW-13-009500 (Manual)	☐	☐
1.21	HONW-13-009600 (Manual)	☐	☐
1.22	HONW-13-009800 (Manual)	☐	☐
1.23	HONW-13-009900 (Manual)	☐	☐
1.24	HONW-13-010000 (Manual)	☐	☐
1.25	HONW-13-010100 (Manual)	☐	☐
1.26	HONW-13-010200 (Manual)	☐	☐
1.27	HONW-13-010600 (Manual)	☐	☐
1.28	HONW-13-010800 (Manual)	☐	☐
1.29	HONW-13-010900 (Manual)	☐	☐
1.30	HONW-13-011000 (Manual)	☐	☐
1.31	HONW-13-012200 (Manual)	☐	☐
1.32	HONW-13-012300 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Aug 27, 2025	1.0.0	Initial CIS Release