CTIA Cybersecurity Certification Test Plan for IoT Devices

Version 1.0

August 2018

CTIA Certification Program

1400 16th Street, NW

Suite 600

Washington, DC 20036

certification@ctiacertfication.org

1.202.785.0081

www.ctia.org/certification

Table of Contents

Section 1 Introduction

1.1 Purpose

The purpose of this document is to define the CTIA Certification Program testing requirements for CTIA Cybersecurity Certification of managed Internet of Things (IoT) devices. For the purpose of this document, an IoT device contains an IoT application layer that provides identity and authentication functionality and at least one communications module supporting either LTE or Wi-Fi®.

1.2 Scope

This test plan defines the cybersecurity tests that will be conducted in CTIA Authorized Test Labs (CATLs) on devices submitted for CTIA Cybersecurity Certification. An IoT device connects to at least one network to exchange data with other devices, vehicles, home appliances, infrastructure elements, etc. The device might include hardware, software, sensors, actuators and network connectivity. Tests are defined such that accurate, repeatable testing may be conducted among all CATLs. Detailed step-by-step test procedures and specific test equipment configurations are left to the CATL and will be presented to CTIA as part of the CATL authorization process as defined in the *Policies and Procedures for CTIA Authorized Testing Laboratories* document [1].

CTIA Cybersecurity Certification is defined in three categories. The first category identifies core IoT device security features; and the second and third categories identify security elements of increasing device complexity, sophistication and manageability.

Testing assumes that the device provides an execution environment for IoT applications that makes use of the LTE communications module and/or the Wi-Fi communications module. If the IoT application is not associated with the LTE communications module, the Wi-Fi communications module, or both, then the device architecture is out of scope of this test plan. If the IoT application supports both communications modules, then tests that involve network communications shall be tested with LTE and Wi-Fi to ensure the same security features are available for both network environments.

Many different mechanisms may be used to achieve the security goals. The IoT device vendor may select the mechanisms that are deemed most relevant for the intended market. One of the goals of this test plan is to make sure the widest adopted standards are used to ensure compatibility across cybersecurity systems. The test plan mandates a number of standards: AES key size standards, end-to-end encryption standards, syslog standards, etc. These are intended to allow for a baseline of security standards that are compatible with the most systems.

This test plan assumes minimum support for encryption based on AES with a 128-bit key. Support for this algorithm and key size by all devices provides an interoperable cryptographic capability; however, devices may also support other algorithms and key sizes that provide the same or more cryptographic security.

1.2.1 Category 1 IoT Cybersecurity Tests

The Category 1 IoT security features are:

Terms of Service and Privacy Policies – Device Terms of Service and privacy policy are readily available. The Terms of Service cover “end of life” for the device.

Password Management – Device supports local password management.

Authentication – Device supports user authentication.

Access Controls – Device enforces role-based access control.

Patch Management – Device supports automatic and manual installation of patches from an authorized source.

Software Upgrades – Device supports manual installation software upgrades from an authorized source.

1.2.2 Category 2 IoT Cybersecurity Tests

The Category 2 IoT security features expand on the Category 1 IoT security features and add:

Audit Log – Device supports the gathering audit log events and reporting them to an EMS using IPsec, SSH, TLS, or DTLS for encryption and integrity protection.

Encryption of Data in Transit – Device supports encrypted communications using IPsec, SSH, TLS or DTLS.

Multi-Factor Authentication – Device supports multiple authentication factors.

Remote Deactivation – Device can be remotely deactivated by the EMS.

Secure Boot – Device supports a secure boot process to protect its hardware (e.g., UEFI).

Threat Monitoring – Device supports logging of anomalous or malicious activity based on configured polices and rules.

IoT Device Identity – Device provides an IoT Device Type and a globally unique IoT Device Identity.

1.2.3 Category 3 IoT Cybersecurity Tests

The Category 3 IoT security features expand on the Category 1 and Category 2 IoT security features and add:

Encryption of Data at Rest– Device supports an effective mechanism for encrypting data stored on the device.

Digital Signature Generation and Validation – Device supports generation and validation of digital signatures.

Tamper Evidence – Device has the ability to alert a monitoring system when it is physically opened.

Design-In Features – Device includes features to fail secure, provide boundary security, and ensure function isolation.

1.3 Applicable Documents

The following documents are referenced in this test plan. Unless otherwise specified, the latest released version shall be used:

[1] Policies and Procedures for CTIA Authorized Testing Laboratories, CTIA

[2] RFC 5652

[3] RFC 5751

[4] NIST SP 800-53 Rev 4

[5] NIST SP 800-63B Authentication and Lifecycle Management

[6] Council on CyberSecurity (CCS) Critical Security Controls (CSC)

[7] NIST SP 800-40 Rev 3

[8] CTIA Consumer Code for Wireless Service

[9] ISO/IEC 27001:2013

[10] ANSI/ISA 62443-2-1:2009

[11] NIST SP 800-92

[12] RFC 5424

[13] RFC 5425

[14] RFC 6012

[15] NIST Cybersecurity Framework v1.1

[16] NIST SP 800-113

[17] FIPS PUB 197

[18] RFC 5246

[19] NIST SP 800-147

[20] NIST SP 800-63-3

[21] NIST SP 800-25

[22] NIST SP 800-49

[23] NIST SP 800-89

[24] FIPS PUB 186-4

[25] RFC 5280

[26] NIST SP 800-160

[27] GSM AA.39

[28] NIST Cybersecurity for IoT Program

[29] NIST SP 800-41 Rev 1

[30] NIST SP 800-111

[31] SP800-90A

[32] RFC 4301 -- Security Architecture for the Internet Protocol

[33] RFC 4303 -- IP Encapsulating Security Payload (ESP)

[34] RFC 4306 -- Internet Key Exchange (IKEv2) Protocol

[35] RFC 5282 -- Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol

[36] RFC 4251 -- The Secure Shell (SSH) Protocol Architecture

[37] RFC 4252 -- The Secure Shell (SSH) Authentication Protocol

[38] RFC 4253 -- The Secure Shell (SSH) Transport Layer Protocol

[39] RFC 4254 -- The Secure Shell (SSH) Connection

[40] RFC 8308 -- Extension Negotiation in the Secure Shell (SSH) Protocol

1.4 Definitions

Term	Definition
Adequate Privilege	Adequate Privilege is any account that has the ability to upgrade the device software (Section 3.6)
Device Deactivation	A deactivated device is unable to communicate with any network using any port or protocol.
Digital Signature	A digital signature is a cryptographic mechanism for checking authenticity. This test plan makes use of RSA and ECDSA digital signatures, which are based on different cryptographic primitives. This test plan accommodates one variant of the RSA digital signature: RSASSA-PKCS1-v1_5. This test plan accommodates one variant of the ECDSA digital signature: ECDSA with curve P-256. Both variants depend upon the SHA-256 hash function.
Enterprise Management System (EMS)	A large-scale application software package that supports business processes, account management, device audit log monitoring, and data analytics in complex organizations. The EMS may be a collection of unique services (such as active directory) that may be diversified with a service provider (such as a cloud based service) feeding information to a corporate EMS.
Fresh Character String	To attempt to modify the password with an acceptable set of characters where the system correctly accepts the new password. Section 3.2.

Term	Definition
IoT Device	An IoT device connects to at least one network to exchange data with other devices, vehicles, home appliances, infrastructure elements, etc. An IoT device might include hardware, software, sensors, actuators and network connectivity.
IoT Device ID	The IoT Device ID is the unique identifier for a single device. This identifier is permanently set by the manufacturer and is not changeable.
IoT Device Type	A permanently assigned identifier for a group of devices that share common characteristics, functions or behaviors.
Normal Operation	This means to allow the device to be turned on, performing all the device's startup routines to completion. At this point the device is in normal operation mode, it may or may not have connectivity to an LTE or Wi-Fi network and be awaiting further commands. When device is under normal operation the first time, the device may have some additional setup activities, such as setting the password, connecting to the network for the first time, performing patching / updates, that may be unique during the first time setup.
P7S Format	The file format of a digital signature using the Cryptographic Message Syntax (CMS), which is also known as PKCS#7. The most recent version of CMS can be found in RFC 5652 [2]. In addition, RFC 5751 [3] defines the application/pkcs7-signature media type for digitally signed content using this same format.
Remote Deactivation	Disable the IoT device from the EMS. A deactivated device cannot generate network traffic. A manual reset may be needed to reactivate the device or configure it to work on another network.
Severity Based Deadline	Within the EMS, a policy can be established so that the audit log entries will be sent to the EMS upon the severity level specified in the configuration. Rather than waiting on a time based reporting threshold (every 5 minutes) or a size based reporting threshold (log reaches 100k), SysLog provides a severity level capability, which allows more severe events to be reported to the EMS more promptly than routine ones.
Software Patch	A software patch is safely installed in an automated manner while the device is operating. A patch does not make major changes to the device configuration or add new features that change the security posture of the device.
Software Upgrade	A software upgrade is installed in a manual manner. A software upgrade may change the IoT device configuration or features in a security relevant way. Upgrades are expected to be installed when the device is operational in a stable environment.

Section 2 Prerequisites

The prerequisites in this section must be met for the IoT device to obtain CTIA Cybersecurity Certification. As stated in Section 1.2, if the device does not include a LTE communications module, a Wi-Fi communications module, or both, then the device architecture is out of scope of this test plan.

2.1 PTCRB or GCF Certification

If the device has an LTE communications module, then the device shall obtain PTCRB (www.ptcrb.com) or GCF (www.globalcertificationforum.org) certification before CTIA Cybersecurity Certification is granted. These certification programs ensure the device meets industry-agreed requirements for operating on an LTE network.

2.2 Wi-Fi Certification

If the device has a Wi-Fi communications module, then the device shall obtain the Wi-Fi Alliance® (www.wi-fi.org) certification for WPA2™ Enterprise and certification for each IEEE 802.11 PHY type that the device supports before CTIA Cybersecurity Certification is granted. These certification programs ensure interoperability with other Wi-Fi CERTIFIED™ devices.

The device shall be certified for:

- Interoperable connectivity in 5 GHz and 2.4 GHz bands
- WPA2 security mechanisms for both personal and enterprise environments

The device shall be certified for each of the IEEE 802.11 PHY types that it supports:

- Wi-Fi CERTIFIED b/g in 2.4 GHz
- Wi-Fi CERTIFIED n in 2.4 GHz
- Wi-Fi CERTIFIED a in 5 GHz
- Wi-Fi CERTIFIED n in 5 GHz
- Wi-Fi CERTIFIED ac
- Wi-Fi CERTIFIED Wi-Gig™ in 60 GHz

Section 3 Category 1 IoT Cybersecurity Tests

This section describes the first category of CTIA Cybersecurity Certification tests for IoT devices on a managed network. To achieve a Category 1 CTIA Cybersecurity Certification, the device must pass all of the tests in Section 2 and this section.

There shall be no interruption of power or battery while the device is being tested.

3.1 Terms of Service and Privacy Policies Test

Reference: *CTIA Consumer Code for Wireless Service*, NIST SP 800-53 Rev 4 [4]

Purpose: Confirm that Terms of Service and privacy policy for the device are available. This test ensures the manufacturer provides the lifetime of the product as well as make the customer aware of their privacy policy and where data might be stored outside of the device.

Procedural Overview:

- Confirm that Terms of Service document, privacy policy document, and list the cloud services that the device requires access to for normal operation are available.

Testing Prerequisites:

- Verify existence and availability of the Terms of Service and the privacy policy of the device.
- The Terms of Service and the privacy policy must be applicable to the device and model submitted for certification, but may be broad enough to cover several similar models of devices.

Test Cases:

3.1.1 Try to obtain the Terms of Service or Use for the device (e.g., included in the box or download from the device maker's web page). If the Terms of Service or Use for the device is obtained, then this test passes; otherwise it fails.

3.1.2 Within the Terms of Service or Terms & Conditions for the device, locate the portion of the document that covers "end of life" or "end of your term" for the device. If the Terms of Service covers "end of life" or "end of your term" of the device, then this test passes; otherwise it fails.

3.1.3 Try to obtain the privacy policy for the device (e.g., included in the box or download from the device maker's web page). If the privacy policy for the device is obtained, then this test passes; otherwise it fails.

3.1.4 Try to obtain the list of cloud services that the device requires access to for normal operation device (e.g., included in the box or download from the device maker's web page). If the documentation says there are no dependencies on cloud services or the documentation provides a list of cloud service dependencies or it covers "Back Up and Cloud Services" for the device, then this test passes; otherwise it fails.

3.2 Password Management Test

Reference: NIST SP 800-53 Rev. 4 [4], NIST SP 800-63B [5]

Purpose: Confirm that the device can locally manage user passwords with the intent to make passwords unique to each device; to change the default password on first use; to remove the ability of the user to set it to a commonly used / easily guessable, bad password.

Procedural Overview:

- Confirm that default passwords are specific to the device, not generic.
- Confirm that default passwords are rejected during normal operation.
- Confirm that the device can change locally managed passwords, and the password contains at least 8 characters, but the password does not contain several repetitive or sequential characters.
- Confirm that the password for one user cannot be accessed by any other user.

Testing Prerequisites:

- Ensure that default passwords are in place at the start of this test**.**
- Determine the procedure to restore factory settings from the device documentation.

Test Cases:

3.2.1 Try to login with the default password. If the default password is the same for many devices (e.g., a password of "admin"), then this test fails; if the default password is specific to the device (e.g., based on the serial number or MAC address of the device), then this test passes.

NOTE: Confirm with Device Maker that the password is unique to the device if only one DUT is provided.

3.2.2 Try starting normal operation before changing any passwords. If the device refuses to begin normal operation or forces the user to change the default passwords, then this test passes; otherwise it fails.

3.2.3 Try setting a password to a fresh character string, and then perform the procedure to restore the device to factory settings. If the device refuses to begin normal operation or forces the user to change the default passwords, then this test passes; otherwise it fails.

3.2.4 Try setting a password to a fresh character string less than 8 characters. If the device refuses to set the password to the provided string or device gives a notification message by asking to input at least 8 characters, then this test passes; otherwise it fails.

3.2.5 Try setting a password back to the default value. If the device refuses to set the password to the provided string, then this test passes; otherwise it fails.

3.2.6 If the device supports more than one user password, login as the most privileged user and try to obtain the passwords of other users. If the device discloses the password of another user, then this test fails; otherwise it passes.

NOTE: The most privileged user might be able to set the passwords for other users, but doing so should not allow them to learn the current password for other users.

3.3 Authentication Tests

Reference: CCS CSC [6], NIST SP 800-53 Rev 4 [4]

Purpose: Confirm that the device supports user authentication to be able to make changes to the device configuration with the goal to require authentication before changes are made, reducing risk to the device that anyone can walk up and make anonymous changes to the device.

Procedural Overview:

- Confirm that the device requires user login to perform any privileged action.

Testing Prerequisites:

- Obtain device documentation on the login roles and their privileges
- Ensure all passwords have been changed from their defaults.
- Obtain a method to unlock the device if multiple failed login attempts cause the device to lock.

Test Cases:

3.3.1 Try to login with the default password. If the login to the device is unsuccessful, then this test passes; otherwise it fails.

3.3.2 Try to login with an incorrect password. If the login to the device is unsuccessful, then this test passes; otherwise it fails.

3.3.3 Try to login with the correct password. If the login to the device is successful, then this test passes; otherwise it fails.

3.3.4 If the device supports more than one authenticated role, try to login to each role with an incorrect password. If the login to the device is unsuccessful in each case, then this test passes; otherwise it fails.

3.3.5 If the device supports more than one authenticated role, try to login to each role with the correct password. If the login to the device is successful in each case, then this test passes; otherwise it fails.

3.4 Access Controls

Reference: CCS CSC [6], NIST SP 800-53 Rev 4 [4]

Purpose: Confirm that the device enforces role-based access control. The intent of this test is to make sure user or low level accounts cannot perform privileged actions; that roles are clearly separated and enforced.

Test Applicability: If a device has no privileged accounts and only one user accounts, it passes

Procedural Overview:

- Confirm that login to an administrative role is required to perform any action at a privilege level.

Testing Prerequisites:

- Obtain device documentation on the roles and their privileges.
- Ensure all passwords have been changed from their defaults.

Test Cases:

3.4.1 Prior to login, try to perform a privileged action described in the device documentation. If the privileged action is performed, then this test fails; otherwise it passes.

3.4.2 After login as a user with adequate privilege, try to perform a privileged action. If the privileged action is performed by the device, then this test passes; otherwise it fails.

3.4.3 If the device supports more than one authenticated role, test that the user must provide a valid password associated with the proper role in order to perform each privileged action. If the privileged action is performed by the device only after login to the proper role, then this test passes; otherwise it fails.

NOTE: Simple devices will have a single administrative role, but more complex devices may have many different roles with different, potentially overlapping, sets of privileges.

3.5 Patch Management

Reference: CCS CSC [6], NIST SP 800-53 Rev 4 [4], NIST SP 800-40 Rev 3 [7]

Purpose: Confirm that the device supports automatic and manual installation of unmodified software patches from an authorized source in order to correct software problems and fix vulnerabilities. These patches are expected to not reset the existing configuration.

NOTE: Support for download of software patches from a remote location is not required in Category 1; however, such a capability may be the most feasible approach to patch management for all of the categories.

Test Applicability: If a device vendor states their device is not patchable but is upgradable, then skip the tests in this section.

Procedural Overview:

- Confirm that the device supports automatic installation of unmodified software patches from an authorized source without causing the device configuration to be reset.
- Confirm that the device supports manual installation of unmodified software patches from an authorized source without causing the device configuration to be reset.

Testing Prerequisites:

- Determine the current device software version and patch level, then locate a patch that is suitable for installation.
- Determine when it is safe and appropriate to manually install a software patch from the device documentation.
- Determine the current device configuration.

Test Cases:

3.5.1 Without any user login, test that the device will observe that a software patch is available, download it, check that the patch is unmodified from an authorized source, and then at an appropriate time installs the software patch. If the software patch is installed, then this test passes; otherwise it fails.

3.5.2 After login as a user with adequate privilege, try to install an unmodified software patch from an authorized source. If the device installs the software patch, then this test passes; otherwise it fails.

3.5.3 After login as a user with adequate privilege, try to install a software patch from an authorized source that has been modified. If the device refuses to install the software patch, then this test passes; otherwise it fails.

3.5.4 After successfully installing a software patch, determine whether the installation processing has reset the device configuration. If the device configuration has not been reset, then this test passes; otherwise it fails.

NOTE: This test case ensures that installation of the patch does not reset custom settings to their default values. The device is expected to retain its custom settings if a patch is applied. New settings that exist only after the patch is applied, may be initially set at default values.

3.5.5 After login as a user with adequate privilege, try to install a software patch from an unauthorized source. If the device refuses to install the software patch, then this test passes; otherwise it fails.

3.6 Software Upgrades

Reference: CCS CSC [6], NIST SP 800-53 Rev 4 [4]

Purpose: Confirm that the device supports manual installation of unmodified software upgrades from an authorized source in order to migrate to a newer version, which may contain additional features.

Procedural Overview:

- Confirm that the device supports manual installation of unmodified software upgrades from an authorized source without causing the device configuration to be reset.

Testing Prerequisites:

- Determine the current device software version and patch level, then locate a software upgrade that is suitable for installation.
- Determine the current device configuration.

Test Cases:

3.6.1 After login as a user with adequate privilege, try to install an unmodified software upgrade from an authorized source. If the device installs the software upgrade, then this test passes; otherwise it fails.

3.6.2 After login as a user with adequate privilege, try to install a software upgrade from an authorized source that has been modified. If the device refuses to install the software upgrade, then this test passes; otherwise it fails.

3.6.3 After login as a user with adequate privilege, try to install a software upgrade from an unauthorized source. If the device refuses to install the software upgrade, then this test passes; otherwise it fails.

3.6.4 After successfully installing a software upgrade, determine whether the installation changed the device configuration. If the device configuration has not changed, then this test passes; otherwise it fails.

NOTE: The intent of this test case is to not have all the custom settings reset to default settings when an upgrade has been performed. New configuration setting associated with new features in the software update will, of course, have default settings, but old configuration settings should not be changed.

Section 4 Category 2 IoT Cybersecurity Tests

This section describes the second category of CTIA Cybersecurity Certification tests for IoT devices on a managed network. To achieve a Category 2 CTIA Cybersecurity Certification, the device must pass all of the tests in Section 3, and this section.

There shall be no interruption of power or battery while the device is being tested.

4.1 Terms of Service and Privacy Policies Test

Reference: *CTIA Consumer Code for Wireless Service* [8], NIST SP 800-53 Rev 4 [4]

Purpose: Confirm that Terms of Service and privacy policy for the device are available.

Procedure:

- Confirm that there is a process to update Terms of Service and privacy policy documents.

Testing Prerequisites:

- Conduct the tests in Section 3.1.

Test Cases

4.1.1 Try to obtain the document that describes the process for updating the Terms of Service for the device. If the document is obtained, then this test passes; otherwise it fails.

4.1.2 Try to obtain the document that describes the Terms of Service for the device. If the document states the expected life of the product (i.e., number of years) in which the device will be supported, then this test passes; otherwise it fails.

4.1.3 Try to obtain the document that describes the process for updating the privacy policy for the device. If the document is obtained, then this test passes; otherwise it fails.

4.2 Password Management Test

Reference: ISO/IEC 27001:2013 [9], NIST SP 800-63B [5]

Purpose: Confirm that the device can be integrated with an EMS.

Procedure:

- After the device has been integrated with an EMS, confirm that the device will not allow passwords to be set to a string that is prohibited by the EMS.
- After a period of inactivity, confirm that the user must provide their password to continue.

Testing Prerequisites:

- Conduct the tests in Section 3.2.
- Integrated the device with a functioning EMS.
- Specify a configuration set for the EMS for testing
- Determine the time interval of inactivity for the device to automatically end the session and require the user to enter their password to continue.

Test Cases:

4.2.1 Try setting the password to a string that is prohibited by the EMS. If the device forces the user to change the password, to a string that is acceptable to the EMS, then this test passes; otherwise it fails.

4.2.2 Login, remain inactive for a time that exceeds the documented idle login time interval, and then try to perform some action. If the device requires reentry of the password to perform the action, then this test passes; otherwise it fails.

4.3 Authentication Tests

Reference: CCS CSC [6], ISO/IEC 27001:2013 [9], NIST SP 800-53 Rev 4 [4]

Purpose: Confirm that the device supports user authentication.

Procedure:

Confirm that the device honors the disabling of a user role in the EMS.

Testing Prerequisites:

- Conduct the tests in Section 3.3.
- Integrate the device with an EMS, and ensure that a privileged role has been disabled.
- Ensure there is no interruption of power or battery while the device is being tested.

Test Cases:

4.3.1 Try to login with a privileged role that has been disabled in the EMS. If the login to the device is unsuccessful, then this test passes; otherwise it fails.

4.4 Access Controls

No additional requirements for Category 2.

4.5 Patch Management

Reference: CCS CSC [6], NIST SP 800-53 Rev 4 [4], NIST SP 800-40 Rev 3 [7]

Purpose: Confirm that the device supports the download of software patches from a remote location in order to correct software problems and fix vulnerabilities.

Test Applicability: If a device manufacturer states their device is not patchable, but is upgradable, then skip “Patch Management’ and move on to upgrades. This test is not applicable.

Procedure:

Confirm that the device supports download of software patches from a remote location.

Testing Prerequisites:

- Conduct the tests in Section 3.5.
- Determine the current device software version and patch level, and then locate a patch that is suitable for installation.
- Determine when it is safe and appropriate to manually install a software patch from the device documentation.
- Determine the current device configuration.

Test Cases:

4.5.1 Without any user login, test that the device will observe that a software patch is available, download the patch from a remote location, check that the patch is unmodified from an authorized source, and then at a time when it is safe and appropriate installs the software patch. If the software patch is installed, then this test passes; otherwise it fails.

4.5.2 After login as a user with adequate privilege, download an unmodified software patch from a remote location that was produced by an authorized source, and then try to install it. If the device installs the software patch, then this test passes; otherwise it fails.

4.5.3 After login as a user with adequate privilege, download a modified software patch from a remote location, and then try to install it. If the device refuses to install the software patch, then this test passes; otherwise it fails.

4.5.4 After login as a user with adequate privilege, download a software patch from a remote location that was produced by an unauthorized source, and then try to install it. If the device refuses to install the software patch, then this test passes; otherwise it fails.

4.6 Software Upgrades

Reference: CCS CSC [6], NIST SP 800-53 Rev 4 [4]

Purpose: Confirm that the device supports download of software upgrades from a remote location and installation of software upgrades from an authorized source in order to migrate to a newer version, which may contain additional features.

Procedure:

- Confirm that the device supports download from a remote location and installation of software upgrades from an authorized source.

Testing Prerequisites:

- Conduct the tests in Section 3.6.
- Determine the current device software version and patch level, and then locate a software upgrade that is suitable for installation.

Test Cases:

4.6.1 After login as a user with adequate privilege, download from a remote location an unmodified software upgrade from an authorized source, and then try to install it. If the device installs the software upgrade, then this test passes; otherwise it fails.

4.6.2 After login as a user with adequate privilege, download from a remote location a modified software upgrade, and then try to install it. If the device refuses to install the software upgrade, then this test passes; otherwise it fails.

4.6.3 After login as a user with adequate privilege, download from a remote location a software upgrade from an unauthorized source, and then try to install it. If the device refuses to install the software upgrade, then this test passes; otherwise it fails.

4.7 Audit Log

Reference: CCS CSC [6], ISA 62443-2-1:2009 [10], ISO/IEC 27001:2013 [9], NIST SP 800-53 Rev 4 [4], NIST SP 800-92 [11], RFC 5424 [12], RFC5425 [13], RFC 6012 [14]

Purpose: Confirm that the device supports the gathering and reporting of audit log events to an EMS.

Procedure:

- Confirm that the EMS audit log gathers at least emergency, alert, critical, and error events, and that these events are transferred to the EMS at an interval selected by the EMS in the Syslog format over a session protected with SSH, IPsec, TLS, or DTLS.
- Confirm that audit log older entries can be trimmed or reset only by a privileged role.
- Confirm that the most privileged role cannot make changes to individual log entries.

Testing Prerequisites:

- Obtain device documentation on the roles and their privileges. Make a list of the roles that can view audit log entries. Make a list of the roles that can delete audit log entries.
- Obtain device documentation on the actions that will cause audit log entries to be generated.
- Integrate the device with an EMS, and ensure that an audit event reporting threshold (e.g., 0 for an emergency, and 7 for debug) has been configured.
- Configure a network traffic monitor to capture network traffic between the device and the EMS.

Test Cases:

4.7.1 Perform actions that will create emergency, alert, critical, and error audit log entries. View the EMS audit log. If the expected audit log entries are present in the audit log, then this test passes; otherwise it fails.

4.7.2 Observe the network traffic between the device and the EMS. If SSH, IPsec, TLS, or DTLS is use to protect the session is used to transfer the audit log entries that exceed the established audit event reporting threshold are transferred in SysLog format within the configured time interval, then this test passes; otherwise it fails.

4.7.3 Try to delete local audit log entries using a non-privileged role that is not authorized to perform these privileged actions. If these privileged actions can be performed by a role other than the ones described in the device documentation, then this test fails; otherwise it passes.

4.7.4 Login as the most privileged user and try to change an audit log entry. If the device allows an audit entry to be changed, then this test fails; otherwise it passes.

NOTE: The most privileged user might be able to delete entries from the audit log, but the user should not be able to change the content of an audit log entry. The oldest audit log entries may be automatically purged when a configured size limit is reached.

4.8 Encryption of Data in Transit

Reference: CCS CSC [6], NIST CSF v1.1 [15], NIST SP 800-53 Rev 4 [4], NIST SP 800-113 [16], FIPS PUB 197 [17], RFC 5246 [18], RFC 6012 [14]

Purpose: Confirm that the device supports encrypted communications using SSH, IPsec, TLS or DTLS. For compatibility and interoperability, the devices must support 128-bit AES.

Test Applicability: If the device does not use cloud services, then the tests in this section are not applicable and they are skipped.

Procedure:

- Confirm that the device supports encryption of data communications using SSH, IPsec, TLS, or DTLS with 128-bit AES.

Testing Prerequisites:

- Configure the device to use SSH, IPsec, TLS, or DTLS to encrypt network traffic with 128-bit AES.
- Configure a network traffic monitor to capture network traffic to and from the device.
- Determine the cloud services that the device depends upon, if any.

  NOTE: This list was obtained as part of the tests in Section 3.1.

Test Cases:

4.8.1 Perform actions that will generate network traffic to the EMS. View the network traffic monitor. If the traffic is protected with SSH, IPsec, TLS, or DTLS using 128-bit AES, then this test passes; otherwise it fails.

NOTE: If the device is set at a level beyond AES-128, set the device to AES-128 for compatibility purposes of testing the device with the EMS.

4.8.2 Perform actions (e.g., such as Logging, Authentication, Authorization, or an OTA (over the air) update) that will generate network traffic to the cloud services that the device depends upon. If the traffic is protected with SSH, IPsec, TLS, or DTLS using 128-bit AES, then this test passes; otherwise it fails.

4.9 Multi-Factor Authentication

Reference: CCS CSC [6] , NIST SP 800-53 Rev 4 [4], NIST SP 800-63B [5]

Purpose: Confirm that the device can be configured to require two different authentication factors for login.

NOTE: One factor will most likely be a password (i.e., something you know). The other factor could be biometric (i.e., something you are) or possession of a physical object (i.e., something you have).

Procedure:

- Configure the device to require at least two different authentication factors for login, and then confirm that all of the factors are successfully checked at login.

Testing Prerequisites:

- Obtain device documentation on multi-factor authentication. Enable multi-factor authentication for the most privileged role.
- Obtain one factor for multi-factor authentication

Test Cases:

4.9.1 Try to login with the most privileged role supported by the device with the correct password and the incorrect additional factor. If the role logs in to the device unsuccessfully, then this test passes; otherwise it fails.

4.9.2 Try to login with the most privileged role supported by the device with an incorrect password and the correct additional factor. If the role logs in to the device unsuccessfully, then this test passes; otherwise it fails.

4.9.3 Try to login with the most privileged roles supported by the device with the correct password and the correct additional factor. If the role logs in to the device successfully, then this test passes; otherwise it fails.

4.10 Remote Deactivation

Reference: CCS CSC [6], NIST CSF v1.1 [15], ISO/IEC 27001:2013 [9], NIST SP 800-53 Rev 4 [4]

Purpose: Confirm that the unique device can be remotely deactivated by the EMS.

Procedure:

- Confirm that the device can be remotely deactivated by an authenticated command from EMS.

Testing Prerequisites:

- Integrate the device with an EMS, and configure the remote deactivation capability.
- Configure a network traffic monitor to capture network traffic between the device and the EMS.

Test Cases:

4.10.1 Try issuing the deactivation command at the EMS. Observe the authenticated command being sent from the EMS to the device. If the device deactivates, then this test passes; otherwise it fails.

4.10.2 Try issuing the deactivation command at the EMS, capture the command at the traffic monitor, modify the checksum, and send the modified command to the device. If the device deactivates, then this test fails; otherwise it passes.

4.10.3 Confirm that the device can be uniquely identified by the EMS. If the device can **be** identified uniquely by the EMS, then this test passes, otherwise it fails.

4.11 Secure Boot

Reference: CCS CSC [6], NIST SP 800-53 Rev 4 [4], NIST SP 800-147 [19]

Purpose: Confirm that the device protects the integrity of the boot process.

Procedure:

- Confirm that the device includes a mechanism to protect the boot process against unintended or malicious modification.

Testing Prerequisites:

- Confirm that the device in the out-of-the-box configuration will securely boot and begin normal operation.
- If the device offers more than one boot configuration, place the device in the secure configuration.
- Verify the existence of documentation that describes the secure boot process.

Test Cases:

4.11.1 If the device offers more than one boot configuration, try to start the device when placed in a secure boot configuration. If the device begins normal operation, then this test passes; otherwise it fails.

4.11.2 Obtain documentation of the secure boot process. If the documentation describing the secure boot process is obtained, then this test passes; otherwise it fails.

4.12 Threat Monitoring

Reference: ISO/IEC 27001:2013 [9], NIST SP 800-53 Rev 4 [4]

Purpose: Confirm that the device supports logging of anomalous or malicious activity based on configured polices and rules.

Procedure:

- Confirm that the EMS audit log gathers events based on anomalous or malicious activity based on configured polices and rules.

Testing Prerequisites:

- Obtain device documentation on the policies and rules that can be configured to detect anomalous or malicious activity, and then configure the policies and rules to detect activities that the tester can trigger.

- Integrate the device with an EMS, and ensure that an audit reporting has been configured.

Test Cases:

4.12.1 Take actions that will trigger the configured policies and rules. View the EMS audit log. If the expected audit log entries are present in the audit log, then this test passes; otherwise it fails**.**

NOTE: These actions might include brute force password attempts, elevation of privileges, creation of new accounts, removal of accounts, system updates, CPU activity spikes, event log activity spikes, change of clock time setting, loss of communication, loss of GPS signal, network ports opened, network ports closed peripheral connection, and so on.

4.13 IoT Device Identity

Reference: NIST SP 800-63B [5], NIST SP 800 63-3 [20]

Purpose: Confirm that the device can identify itself with an IoT Device Type and a globally unique IoT Device Identity.

NOTE: There are many ways that a vendor can assign an IoT Device Type and a globally unique IoT Device Identity; this test plan does not require the use of a particular approach.

Procedure:

- Confirm that the device can provide an IoT Device Type that can be used to determine the capabilities of the device.

- Confirm that the device can provide a globally unique IoT Device Identity.
- Confirm the device records the IoT Device Type and globally unique IoT Device Identity in the EMS audit log.

Testing Prerequisites:

- Obtain the IoT Device Type and the globally unique IoT Device Identity for the device.
- Obtain device documentation on the actions that will cause audit log entries to be generated.

Test Cases:

4.13.1 Perform an action that will create audit log entries. View the EMS audit log. If the expected audit log entries contain the IoT Device Type and globally unique IoT Device Identity present in the audit log, then this test passes; otherwise it fails.

Section 5 Category 3 IoT Cybersecurity Tests

This section describes the third category of CTIA Cybersecurity Certification tests for IoT devices on a managed network. Category 3 offers the most comprehensive level of testing for cybersecurity threats. To achieve a Category 3 CTIA Cybersecurity Certification, the device must pass all of the tests in Section 2, Section 3, Section 4 and this section.

There shall be no interruption of power or battery while the device is being tested.

5.1 Terms of Service and Privacy Policies Test

No additional requirements for Category 3.

5.2 Password Management Test

Reference: ISO/IEC 27001:2013 [9], NIST SP 800-63B [5]

Purpose: Confirm that the device can be integrated with an EMS and that the device includes a mechanism to limit the rate of unsuccessful authentication attempts to greatly increase the time needed to guess a password.

Procedure:

- After the device has been integrated with an EMS, confirm that the device implements a rate-limiting or blocking mechanism that limits the number of unsuccessful authentication attempts.

Testing Prerequisites:

- Conduct the tests in Section 3.2 and Section 4.2.
- Integrate the device with an EMS.
- Obtain the documentation of rate-limiting or blocking mechanism from manufacturer.

Test Cases:

5.2.1 Try to login with the incorrect password several times in a row**.** If the rate-limiting or blocking mechanism performs according to the manufacturer specifications, then the test passes; otherwise it fails.

5.3 Authentication Tests

No additional requirements for Category 3.

5.4 Access Controls

No additional requirements for Category 3.

5.5 Patch Management

Reference: CCS CSC [6], ISO/IEC 27001:2013 [9], NIST SP 800-53 Rev 4 [4], NIST SP 800-40 Rev 3 [7]

Purpose: Confirm that the device supports automatic installation of digitally signed software patches from an authorized source in order to correct software problems and fix vulnerabilities at a time that is coordinated with an EMS.

Test Applicability: If a device manufacturer states their device is not patchable, but is upgradable, then skip "Patch Management' and move on to upgrades. This test is not applicable.

Procedure:

Confirm that the device supports automatic installation of software patches from an authorized source at a time that is coordinated with an EMS.

Confirm that the device validates the digital signature on the software patch immediately prior to installation.

NOTE: Digital signature validation depends on the functionality in Section 5.14.

Testing Prerequisites:

- Conduct the tests in Section 3.5 and Section 4.5.
- Integrate the device with an EMS.
- Determine the current device software version and patch level, then locate a patch that is suitable for installation.
- Modify a copy of the patch by altering the digital signature, creating an invalid patch.

Test Cases:

5.5.1 Try to install the invalid patch with the modified digital signature. If the software patch is successfully installed, then this test fails; otherwise it passes.

5.5.2 Without any user login, test that the device will observe that a software patch is available, download it, check that the patch is unmodified from an authorized source, and then at a time coordinated with the EMS installs the software patch. If the software patch is installed at the coordinated time, then this test passes; otherwise it fails.

5.6 Software Upgrades

Reference: CCS CSC [6], ISO/IEC 27001:2013 [9], NIST SP 800-53 Rev 4 [4]

Purpose: Confirm that the device supports automatic installation of digitally signed software upgrades from an authorized source in order to migrate to a newer version at a time that is coordinated with an EMS.

Procedure:

- Confirm that the device supports automatic installation of software upgrades from an authorized source at a time that is coordinated with an EMS.

- Confirm that the device validates the digital signature on the software upgrade immediately prior to installation.

  NOTE: Digital signature validation depends on the functionality in Section 4.13.

Testing Prerequisites:

- Conduct the tests in Section 3.6 and Section 4.6.
- Integrate the device with an EMS.
- Determine the current device software version and patch level, then locate a software upgrade that is suitable for installation.
- Modify a copy of the software upgrade by altering the digital signature, creating an invalid software upgrade.

Test Cases:

5.6.1 Try to install the invalid software upgrade with the modified digital signature. If the software upgrade is successfully installed, then this test fails; otherwise it passes.

5.6.2 Without any user login, test that the device will observe that a software upgrade is available, download it, check that the software upgrade is unmodified from an authorized source, and then at a time coordinated with the EMS installs the software upgrade. If the software upgrade is installed at the coordinated time, then this test passes; otherwise it fails.

5.7 Audit Log

Reference: CCS CSC [6], ISA 62443-2-1:2009 [10], ISO/IEC 27001:2013 [9], NIST SP 800-53 Rev 4 [4], NIST SP 800-92 [11], RFC 5424 [12], RFC 6012 [14]

Purpose: Confirm that the device supports the gathering of audit log events and reporting them to an EMS within a severity-based deadline.

Procedure:

- Confirm that emergency, alert, critical, and error events are transferred to the EMS event within a severity-based deadline.

Testing Prerequisites:

- Conduct the tests in Section 4.7.
- Configure a network traffic monitor to capture network traffic between the device and the EMS.
- Configure delivery deadlines for emergency, alert, critical, and error events.

Test Cases:

5.7.1 Perform some actions that will create emergency, alert, critical, and error audit log entries. Observe the network traffic between the device and the EMS. If a SSH, IPsec, TLS, or DTLS is used to protect the session that is used to transfer the audit log entries before the configured deadlines are transferred in SysLog format, then this test passes; otherwise it fails.

5.8 Encryption of Data in Transit

No additional requirements for Category 3.

5.9 Multi-Factor Authentication

No additional requirements for Category 3.

5.10 Remote Deactivation

No additional requirements for Category 3.

5.11 Secure Boot

No additional requirements for Category 3.

5.12 Threat Monitoring

No additional requirements for Category 3.

5.13 IoT Device Identity

No additional requirements for Category 3.

5.14 Digital Signature Generation and Validation

Reference: NIST SP 800-25 [21] , NIST SP 800-49 [22], NIST SP 800-53 Rev 4 [4], NIST SP 800-89 [23], FIPS PUB 186-4 [24], RFC 5280 [25], RFC 5652 [2], RFC 5751 [3]

Purpose: Confirm that the device can generate an RSA or ECDSA digital signature, and it can validate RSA and ECDSA digital signatures using a set of trust anchors.

Procedure:

- Confirm that the device can generate an RSA or ECDSA digital signature in the P7S format, and it can validate RSA and ECDSA digital signatures in the P7S format.

Testing Prerequisites:

- Generate or install a digital signature private key for use with either the RSA or ECDSA algorithm.
- Obtain an X.509 certificate that includes the public key that corresponds to the digital signature private key.
- Configure at least one trust anchor that can be used to validate an RSA digital signature.

- Configure at least one trust anchor that can be used to validate an ECDSA digital signature.

Test Cases:

5.14.1 Try to generate a digital signature using either the RSA or ECDSA algorithm in the P7S format and includes the X.509 certificate of the device. If the device produces a valid digital signature, then this test passes; otherwise it fails.

5.14.2 Try to validate a correct RSA digital signature in the P7S format that is associated with a configured trust anchor. If the device validates the signature, then this test passes; otherwise it fails.

5.14.3 Try to validate a correct ECDSA digital signature in the P7S format that is associated with a configured trust anchor. If the device validates the signature, then this test passes; otherwise it fails.

5.14.4 Try to validate a correct RSA digital signature in the P7S format that is not associated with a configured trust anchor. If the device validates the signature, then this test fails; otherwise it passes.

5.14.5 Try to validate a correct ECDSA digital signature in the P7S format that is not associated with a configured trust anchor. If the device validates the signature, then this test fails; otherwise it passes.

5.15 Encryption of Data at Rest

Reference: ISO/IEC 27001:2013 [9], NIST SP 800-53 Rev 4 [4], NIST SP 800-113 [16], FIPS PUB 197 [17]

Purpose: Confirm that the device includes an effective mechanism for encrypting data stored in the device.

Procedure:

- Confirm that the device implements either an encrypting file system or a file encryption mechanism that uses 128-bit AES.

Testing Prerequisites:

- Obtain device documentation on encryption of data stored in the device.

Test Cases:

5.15.1 Obtain the documentation on encryption of data stored in the device. If multiple encryption algorithms are supported, configure the device to use AES with a 128-bit key. If the device supports encryption of files with AES with a 128-bit key, then this test passes; otherwise it fails.

5.15.2 Login as a user with sufficient privilege and then configure the device to use the encrypting file system or a file encryption mechanism to protect files with AES with a 128-bit key. If the device continues to operate normally, then this test passes; otherwise it fails.

5.16 Tamper Evidence

Reference: NIST SP 800-53 [4]

Purpose: Confirm that the device has the ability to alert an EMS when it is physically opened.

Procedure:

- Confirm that the device alerts an EMS and records in the audit log when it is physically opened.

Testing Prerequisites:

- Integrate the device with the EMS.
- Configure a network traffic monitor to capture network traffic between the device and EMS.

Test Cases:

5.16.1 While the device is disconnected from any external power source, try to open the device case, close the case, and restore external power. If the device sends an alert to the EMS, then this test passes; otherwise it fails.

5.17 Design-In Features

Reference: NIST SP 800-53 [4], NIST SP 800-160 [26]

Purpose: Confirm that the security design of the device includes features to fail secure, provide boundary security, and ensure function isolation.

Procedure:

- Confirm that the device was designed to fail secure.

  NOTE: When failure is detected, the device goes to a secure state.

- Confirm that the device was designed to deny all inbound and outbound network communications, except for those that are essential for the device to operate properly.

  NOTE: The Threat monitoring functionality may play a significant role in the enforcement of a policy to “deny-all, permit-by-exception” network communications.

- Confirm that the device was designed to isolate critical functions from less critical functions with separation and segmentation mechanisms.

  NOTE: If malicious software gets into the device, these mechanisms deter the propagation to other parts of the device and other devices while critical functions continue to operate properly. For example, boundary controls within a device could be used to allow only whitelisted activities.

Testing Prerequisites:

- Verify existence and availability of design documentation for the security mechanisms of the device.

Test Cases:

5.17.1 Try to obtain a declaration from the device manufacturer that the device was designed to fail secure. If a declaration is obtained, then this test passes; otherwise it fails.

5.17.2 Try to obtain the design documentation for the network communications security mechanisms of the device. If the device was designed to deny all inbound and outbound network communications, except for those that are essential for the device to operate properly, then this test passes; otherwise it fails.

5.17.3 Try to obtain a declaration from the device manufacturer that the device was designed to isolate critical functions from less critical functions. If a declaration is obtained, then this test passes; otherwise it fails.

5.17.4 Try to connect to the device from an external host using each TCP port, UDP port, and any other device-supported protocols. If the device confirms the port is open on any port or protocol that is not described in the design documentation, then this test fails; otherwise it passes.

Appendix A— Revision History

Date	Version	Description
August 2018	1.0	Initial release