IoT Cybersecurity Certification FAQ

1. ## Is my IoT Device eligible for the certification?

   If your device has been built with the following features/elements, it is eligible for the certification. Please discuss with a CTIA Certification Authorized Test Lab (ATL).

Terms of Service & Privacy Policies	Authentication	Access Controls
Patch Management and Software Upgrade	IoT Device Identity	Encryption of Data at Rest
Encryption of Data in Transit	Use of Subscription Related Information	Design in Features
Tamper Protection and Evidence	Constrain IoT Devices	Audit Log
Remote Deactivation	Secure Boot	Threat Monitoring
Secure Backup		

   Note: For the definitions of test elements listed above, please reference CTIA Cybersecurity Certification Test Plan for IoT Devices on https://ctiacertification.org/test-plans/

2. ## Where can I submit the certification request for IoT Cybersecurity Certification?

   Certification requests can be submitted online at https://certify.ctiacertification.org/

3. ## Where can I download the IoT Cybersecurity Certification Program Document?

   The document is available at https://ctiacertification.org/

4. ## I have devices that are similar by design, do they all have to undergo IoT Cybersecurity Certification testing?

   A device that is uniquely defined must go through its own cybersecurity testing. Leveraging of "parent" device testing is not accepted. "Uniquely defined" means a specific combination of hardware, software and firmware release versions. A new release of the software for a device will require a manufacturer to assess whether a retest is needed (see Question 5).

5. ## What is the process for updating test reports if the software, hardware, or firmware version of the device changes? Is full regression required for every minor software change or patch?

   If a device's hardware, software, or firmware update includes a "security-relevant change" where the device changes its behavior in areas covered by the testing that was conducted for the current certification, it needs to be retested. The Original Equipment Manufacturer (OEM) and an authorized test lab determine the scope of retesting. The OEM submits an Engineering Change Order (ECO) certification request in the certification database.

6. ## What is considered an "authorized source" for receiving patches or software upgrades?

   An authorized source is the source or location authorized by the OEM that hosts the patches and software upgrades.

7. ## Is there any restriction on the version of Transport Layer Security (TLS) that is used by the device?

   TLS 1.2 is the current minimum requirement.

8. ## Is a CAT-M1 or NB-IoT device eligible for Cybersecurity Certification?

   Yes.

9. ## If the device supports 4G LTE, 5G NR, or Wi-Fi connectivity, will the full scope of tests be required for each technology?

   Yes.

10. ## Can a sensor or hub with no local interface or connection that communicates only through cloud servers be eligible for certification?

    Yes. Please see Question 1.

11. ## If a device doesn't have a user interface, is it exempt from cybersecurity testing?

    No. All test cases for the levels must be passed in order to obtain certification.

12. ## If there is no user login capability on the device, would it still be eligible for testing and certification?

    Yes. All test cases for the levels must be passed in order to obtain certification unless otherwise stated in the applicability section of each test. Please see Question 1.

13. ## How many samples should be provided for testing?

    A minimum of three units of the device must be provided for testing.

14. ## Some tests may require proprietary information (e.g., login and password information needed to place a modified patch in a desired remote location). Can the device still obtain cybersecurity certification without disclosing this information?

    All tests required for a level must be successfully passed to obtain certification. Authorized test labs and vendors may execute non-disclosure or confidentiality agreements to protect proprietary information such as login information.

15. ## How does the CTIA Cybersecurity Certification Test Plan classify an IoT device?

As per the Cybersecurity Certification Test Plan, an IoT device contains an IoT application layer that provides identity and authentication functionality and at least one communications mode supporting either 4G LTE, 5G NR, or Wi-Fi connectivity. An IoT device connects to at least one network to exchange data with other devices, vehicles, home appliances, infrastructure elements, etc.

16. ## What certification levels are available?

Level 1: Consumer and enterprise devices.
Level 2: Enterprise devices (including infrastructure managed devices).
In the previous test plan versions, there were three certification levels. Core security elements in Level 1 were for consumer-grade devices. Enhanced security elements (Level 2) and advance security elements (Level 3) were mainly for enterprise managed or infrastructure managed devices. Starting with Test Plan Version 2.1, the certification levels have been consolidated into two levels.

17. ## How is the device certification level decided?

The level of device certification is decided by the manufacturer. The OEM will declare the level of certification during the certification submission process.

18. ## Why is the Cybersecurity Certification Test Plan divided into two levels of testing?

Each level is associated with increasing device complexity and enhanced security elements. Level 1 represents the minimum baseline IoT security features that all devices shall provide.

19. ## If the vendor wants Level 2 certification, do they need to test the device for the Level 1 test plans as well?

Yes, Level 2 testing includes Level 1 testing. Each progressive level of certification includes the test cases from the lower levels.

20. ## Are there prerequisites to qualify a device for IoT Cybersecurity testing?

No. A vendor does not need to obtain any other certification as a prerequisite for IoT Cybersecurity Certification.

21. ## Do I need to obtain other certifications (e.g., PTCRB, IoT Network Certified, GCF) prior to IoT Cybersecurity testing?

No. A vendor does not need to obtain other certifications in order to receive IoT Cybersecurity Certification.

22. If an IoT device integrates a wireless module, does the module need to be certified?

The certification is only applicable to IoT end-devices regardless of wireless architecture (e. g. module or chipset based).

23. What does a vendor need to provide to start testing?

In addition to three samples of the device, a vendor needs to provide the completed Vendor Questionnaire in the IoT Cybersecurity Program document to an Authorized Test Lab and any additional equipment and documentation to properly access and power the device under testing.

24. What is the purpose of the IoT Cybersecurity Certification Program?

The IoT Cybersecurity Certification Program is designed to help improve security for connected devices and thus help to grow the IoT Marketplace. The program helps protect consumers and wireless infrastructure while creating a more secure foundation for smart cities, connected cars, mHealth and other IoT applications. The creation of an IoT security baseline also addresses a growing global concern over potential cybersecurity issues and policy implications related to IoT.

25. Is CTIA IoT Cybersecurity Certification sufficient for approval to deploy a device on an operator's network?

While CTIA IoT Cybersecurity Certification covers a wide range of requirements, operators may require compliance with additional specifications and tests to satisfy their unique security requirements. It is highly recommended to understand the target operator's security requirements prior to seeking certification.

26. Is my general-purpose computing device (e.g., smartphone, tablet, laptop) eligible for IoT Cybersecurity Certification?

Yes, if the device is able to meet the criteria defined in Question 1 ("Is my IoT Device eligible for the certification?") then it is eligible for the certification process. However, please note that IoT Cybersecurity Certification is designed for IoT devices (as defined in Section 1.4 of the CTIA Cybersecurity Certification Test Plan for IoT Devices) and that general purpose computing devices such as smartphones, tablets, etc. typically encompass a wider range of functionality tested for in IoT Cybersecurity Certification.

27. My IoT Device has several limitations including the inability to perform software updates. Is my IoT Device eligible for the certification?

If the IoT device is a “constrained IoT device” (fully defined both “CTIA Certification Cybersecurity Test Plan” and “CTIA Cybersecurity Certification Program for IoT Devices” but briefly an IoT device that has limitations in the ability to process, communicate, or store data), then it can only be tested and certified to Level 1 and nothing beyond (such that a Level 2 device cannot be a “constrained IoT device”).