IoT Cybersecurity Certification FAQ

1. Is my IoT Device eligible for the certification?

Before requesting certification, you must be able to answer yes to the following questions. If you answer no to just one of the questions, please discuss this with an authorized test lab.

- **Terms of Service and Privacy Policy**. Does your device have a Terms of Service and a Privacy Policy? You need to state online how long you plan to support your IoT device. This doesn't mean that you can't extend that support period after the product is launched through a ToS update.
- **Passwords**. Do each of your devices have unique passwords, whether they are accessed by the user or the cloud service provider? The IoT device is connecting via LTE and/or Wi-Fi and you're expecting some remote connectivity, which means there is likely some authentication action happening remotely to your device; is this authentication based on passwords?
- **Login Roles**. If your device supports more than one role (privilege level), does your device enforce separation between the supported roles (e.g., a user account and an admin account)?
- **Providing updates**. Does your company provide software patches and/or software/firmware updates for your device? Does your device validate the patch or update?

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. Original Equipment Manufacturer (OEM) and authorized test labs determine the scope of retesting. 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 both LTE & 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 the device is just a black box and the user is not expected to login to the device does that mean that the device is not eligible for the certification?

    No. 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 module supporting either LTE 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: Core security elements recommended for consumer-grade devices.
    Level 2: Enhanced security elements well-suited for business and enterprise managed devices.
    Level 3: Advance security elements designed to protect infrastructure-managed devices.

17. ## How is the device certification level (1/2/3) 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. ## If the vendor wants Level 3 certification, do they need to test the device for the Level 1 and Level 2 test plans as well?

    Yes, Level 3 testing includes Level 1 and 2 testing. Each progressive level of certification includes the test cases from the lower levels.

19. ## Why is the Cybersecurity Certification Test Plan divided into different 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 should provide.

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, 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 devices. Since the test plan is not applicable to cellphones or modules, the IoT device itself must obtain the certification.

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.