Cybersecurity Labeling for Consumer IoT Products

U.S. CYBER TRUST MARK

The views expressed in this presentation are those of the authors and may not necessarily represent the views of the Federal Communications Commission.

Cybersecurity Labeling for IoT
(PS Docket No. 23-239)

- On March 15, 2024, the FCC adopted a Report and Order and Further Notice of Proposed Rulemaking.
- The R&O establishes a voluntary cybersecurity labeling program for wireless consumer Internet of Things (IoT) products.
- As program owner, the FCC will establish requirements for IoT Products to qualify for the FCC IoT Label.
- The FCC IoT Label will let consumers know that an IoT Product bearing the Label has met minimum cybersecurity standards.

- The program is supported by a Lead Administrator, Cybersecurity Labeling Administrators (CLAs), and CyberLABs.
  - Lead Administrator collaborates with stakeholders to make recommendations to the FCC on cybersecurity standards and testing procedures and label design etc.; and is responsible for developing a consumer education campaign.
  - Cybersecurity Label Administrators (CLAs) are responsible for day-to-day management of the program (e.g., accepting and reviewing applications and test reports and approving/denying use of the FCC IoT Label).
  - CyberLABs are responsible for testing products to demonstrate compliance to the IoT Cybersecurity Label requirements; may be a CLA-run testing lab, an independent testing lab, or a testing lab internal to the applicant, but it must be accredited and recognized by the Lead Administrator.

Lead Administrator

Cybersecurity Label Administrators (CLAs)

CyberLABs

International Standard Accreditation (ISO/IEC)

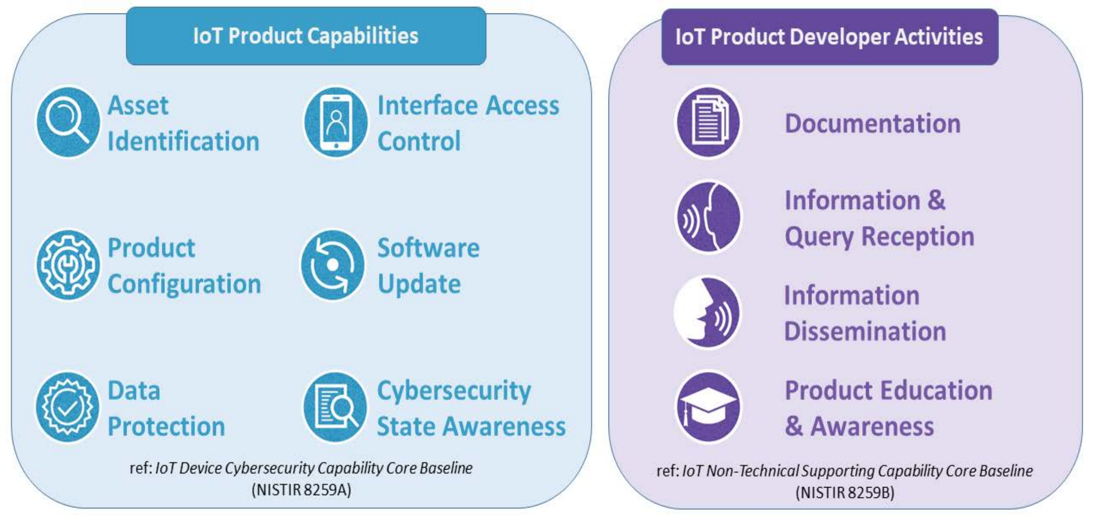
ISO
International Organization for Standardization
IEC
INTERNATIONAL ELECTROTECHNICAL COMMISSION

- The Lead Administrator and CLAs must be accredited to ISO/IEC 17065 (Conformity assessment requirements for bodies certifying products, processes, and services) and the FCC’s program scope.
- CyberLABs must be accredited to ISO/IEC 17025 (General requirements for the competence of testing and calibration laboratories) and the FCC's program scope and recognized by the Lead Administrator.
- Organizations accrediting prospective CLAs and CyberLABs must be accredited to ISO/IEC 17011 (Conformity assessment requirements for accreditation bodies).

NIST IoT Core Baseline for Consumer IoT Products (NISTIR 8425)

- **NIST's Core Baseline** (8425) serves as the basis of the FCC's IoT Labeling Program
- NISTIR 8259 Series of reports, Foundational Activities for IoT Device Manufacturers, provides guidance for designing securable IoT products with core device capabilities and non-technical activities that support common cybersecurity goals
- NIST’s Core Baseline and the FCC Labeling program both apply to the **IoT Product** rather than just the IoT Device to cover the full IoT product system used by consumers.

NISTIR 8259 Guidance for Product Development


IoT Product Capabilities
Asset Identification
Interface Access Control
Product Configuration
Software Update
Data Protection
Cybersecurity State Awareness
IoT Product Developer Activities
Documentation
Information & Query Reception
Information Dissemination
Product Education & Awareness

ref: *IoT Device Cybersecurity Capability Core Baseline* (NISTIR 8259A)

ref: *IoT Non-Technical Supporting Capability Core Baseline* (NISTIR 8259B)

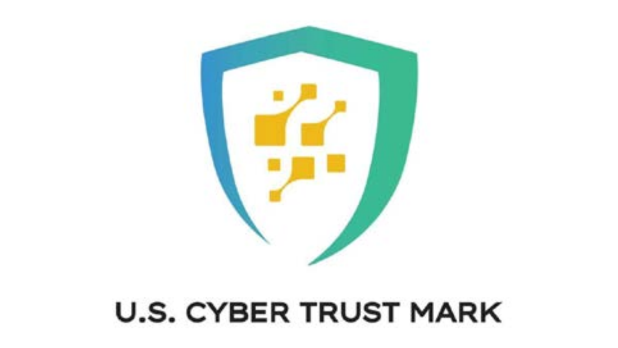
What Are IoT Products and IoT Devices?

- IoT Product
  - Includes the device and additional product components that are necessary to use the IoT device beyond basic operational features (e.g., mobile app, gateway, backend); and
  - Includes data communications links to external components.
  - Does **not** include external components or any external third-party components that are outside the manufacturer's control.
- IoT Device
  - FCC adopted the following modified version of the NIST definition of an IoT device, which adds the requirement that the device be "Internet connected" and "capable of intentionally emitting RF energy"

    An Internet-connected device capable of intentionally emitting radiofrequency energy that has at least 1 transducer for interacting directly with the physical world (e.g., a sensor or actuator) and at least one network interface for interfacing with the digital world (e.g., Ethernet, Wi-Fi, Bluetooth).

- Examples of IoT Products Smart thermostats, smart lights, smart locks, smart appliances, smart cameras, fitness trackers, and smart watches.

Label Overview



- The FCC IoT Label is **binary**: Products either qualify, or do not qualify, to bear the label.
- The IoT Label includes the **U.S. Cyber Trust Mark and a QR code**.
  - The QR code is linked to a decentralized, publicly available registry with consumer-friendly information about the security of the product.
  - Registry information is presented/made available by manufacturers authorized to use the FCC IoT Label through a common Application Programming Interface (API), which provides a consistent way for the public to access the information.
- The location of the FCC IoT Label and specific label design (e.g., white spaces and size) will be part of multi-stakeholder process coordinated by Lead Administrator.

Registry

- Registry displays consumer friendly security-related information:
  - Instructions on how to change the default password.
  - Additional information on how to configure the device securely.
  - Information on whether software updates and patches are automatic and how to access security updates/patches if they are not automatic.
  - The end date of the minimum support period, or a statement that the device is unsupported and that the purchaser should not rely on the manufacturer to release security updates.
  - Whether the manufacturer maintains a hardware bill of materials (HBOM) and/or software bill of materials (SBOM).

U.S. CYBER TRUST MARK

Process for FCC Label Approval

1. **Applicant (e.g., manufacturer) has its eligible product tested by a CyberLAB.**

2. **Applicant submits an application with supporting documents (including CyberLAB test report) to a CLA requesting approval to use the FCC IoT Label.**

3. **CLA reviews the application, test report, and other supporting documentation and determines whether the IoT product meets the program requirements.**

4. **CLA approves or denies the application.**

Excluded from the Program

Medical devices (FDA)

Motor vehicles and motor vehicle equipment (NHTSA)

Equipment on the FCC’s Covered List

IoT products produced by an entity on the Covered List as producing “covered equipment”

IoT products from a company named on other lists addressing national security

IoT products produced by entities banned from Federal procurement

International Reciprocal Recognition

- International harmonization of cybersecurity standards will bring immense value to manufacturers.
- The U.S. and the EU have committed to work together on achieving mutual recognition for our government-backed cybersecurity labeling programs and regulations for Internet-of-things devices via a Joint Cybersafe Products Action Plan.
- Japan has committed to work with the U.S. to “ensure interoperability” of its IoT labeling scheme currently under development.
- The FCC Public Safety and Homeland Security Bureau and the Office of International Affairs will work with other federal agencies to develop international recognition of the Commission’s IoT Label and mutual recognition of international labels.
- Products meeting a common baseline standard will elevate the overall global cybersecurity baseline for IoT and promote security-by-design approaches to smart products.

Questions?