Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products

National Institute of Standards and Technology

February 4, 2022

This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.02042022-2

National Institute of Standards and Technology
U.S. Department of Commerce

Abstract

Executive Order (EO) 14028, "Improving the Nation's Cybersecurity," tasks the National Institute of Standards and Technology (NIST), in coordination with the Federal Trade Commission (FTC) and other agencies, to initiate pilot programs for cybersecurity labeling. NIST is, among other actions, directed "… to identify IoT cybersecurity criteria for a consumer labeling program…" This document seeks to fulfill this directive by recommending consumer IoT product label criteria, label design and consumer education considerations, and conformity assessment considerations for use by a scheme owner to inform a consumer Internet of Things (IoT) product labeling program.

Keywords

Consumer IoT; criteria; cybersecurity; executive order; label.

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST, nor does it imply that the products mentioned are necessarily the best available for the purpose.

Additional Information

For additional information on NIST's Cybersecurity programs, projects and publications, visit the Computer Security Resource Center. Information on other efforts at NIST and in the Information Technology Laboratory (ITL) is also available.

Submit comments on this publication to: labeling-eo@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Table of Contents

List of Appendices

1 Introduction

1.1 Background

This document provides recommended criteria for a cybersecurity labeling effort for consumer internet of things (IoT) products. Executive Order (EO) 14028, "Improving the Nation's Cybersecurity," [EO14028] issued on May 12, 2021, directed the National Institute of Standards and Technology (NIST) to develop these criteria for use in a pilot program.

NIST was directed to "identify IoT cybersecurity criteria for a consumer labeling program, and shall consider whether such a consumer labeling program may be operated in conjunction with or modeled after any similar existing government programs consistent with applicable law. The criteria shall reflect increasingly comprehensive levels of testing and assessment that a product may have undergone, and shall use or be compatible with existing labeling schemes that manufacturers use to inform consumers about the security of their products."

NIST was also directed to "examine all relevant information, labeling, and incentive programs and employ best practices. This review shall focus on ease of use for consumers and a determination of what measures can be taken to maximize manufacturer participation."[1]

NIST began developing the proposed product criteria by building on its existing work in IoT cybersecurity – including the NISTIR 8259 family of documents [IR8259] [IR8259A] [IR8259B] defining baseline cybersecurity capabilities for IoT devices from an analysis of international standards and guidance – and by leveraging available standards and guidance, reviewing vulnerabilities that enabled recent compromises of IoT products, and seeking feedback from the community through workshops and comments on draft versions of the criteria. Reviews of available international standards and guidance addressing consumer IoT product cybersecurity and recent public news stories about compromised IoT products and their vulnerabilities contributed to the profiling of the NISTIR 8259A [IR8259A] and NISTIR 8259B [IR8259B] core baseline for the consumer IoT sector. Draft versions of the criteria released on August 31 and December 3, 2021, were available for community feedback at workshops on September 14 and December 9, 2021, and in writing.

1.2 Scheme and Scheme Owner

NIST is identifying key elements of a potential labeling scheme that could be established by another organization or program. The criteria that NIST is recommending are stated in terms of minimum requirements and desirable attributes; NIST is not establishing its own scheme or program, nor is NIST designing or proposing a design of a consumer IoT product label. The key elements of the recommendations criteria include a proposed baseline product criteria as well as labeling and conformity assessment considerations. The product criteria in this document specify desired outcomes, allowing providers and customers to choose the best approaches for their devices and environments. One size will not fit all, and multiple solutions might be offered by label providers.

[1] For more information, see sections 4(s) and 4(t) of EO 14028.

Implementation of the consumer IoT product labeling program as guided by these recommendations and considerations requires a scheme owner. The role of a consumer labeling scheme owner, which could be a public or private sector organization, is critical. **The scheme owner is the entity that manages the labeling scheme and determines its structure and management and performs oversight to ensure that the scheme is functioning consistently in keeping with overall objectives. The scheme owner is responsible for tailoring the product criteria, defining conformity assessment requirements, developing the label and associated information, and conducting related consumer outreach and education.** A scheme could be defined at a sector level, or an overall scheme owner could be responsible for multiple categories. There can be flexibility in establishing how the baseline IoT criteria apply to specific ranges of IoT products and which conformity assessment activities are appropriate, but multiple variations of labels or labeling approaches would likely cause confusion among consumers and limit the effectiveness of the efforts.

1.3 Document Scope and Goals

This document discusses considerations and recommendations for the development of a consumer IoT product labeling program. The following key recommendations are addressed:

- Baseline product criteria for consumer IoT products are expressed as outcomes rather than as specific statements as to how they would be achieved.
- No single conformity assessment approach is appropriate given the variety of ways those baseline criteria could apply to a wide range of products.
- A single binary label (a "seal of approval" type of label indicating a product has met a baseline standard) is likely most appropriate, coupled with a layered approach that leads interested consumers to additional detail online.

The goal of this document is to provide recommendations, additional information, and context related to these responsibilities for use by a scheme owner creating the consumer IoT product labeling program.

1.4 Document Structure

The remainder of this document is organized as follows:

- Section 2 - provides the IoT product criteria, the technical foundations of those criteria, and considerations related to the product criteria.
- Section 3 - discusses considerations around the label.
- Section 4 - discusses considerations around the conformity assessment mechanism used.

2 Baseline Product Criteria

The recommended baseline product criteria for a consumer IoT product cybersecurity labeling program reflect the intent to develop **product-focused outcomes that enable consumers to make informed decisions about purchasing and maintaining these products.** This section describes the scope and approach of the recommended baseline product criteria and states each criterion.

2.1 Scope of an IoT Product

Consumer[2] IoT products often constitute a set of system components that work together to deliver functionality realized at the end point or 'device' component of the product. NIST describes an IoT device as computing equipment with at least one transducer (i.e., sensor or actuator) and at least one network interface [IR8259].[3] All IoT products contain at least one IoT device and may contain only this product component.[4] In many cases, the IoT product may be purchased as one piece of equipment (i.e., the IoT device) but still requires other components to operate, such as a backend (i.e., cloud server) or companion user application on a personal computer or smartphone. Complex IoT products may contain multiple physical IoT devices, contain other kinds of equipment, or connect to multiple backends or companion applications as components. Though there are possibly a large number of component combinations that may create an IoT product, it is helpful to think of three specific kinds of IoT product components (other than the IoT device itself, which is always present in an IoT product):

- Specialty networking/gateway hardware (e.g., a hub within the system where the IoT device is used).
- Companion application software (e.g., a mobile app for communicating with the IoT device).
- Backends (e.g., a cloud service, or multiple services, that may store and/or process data from the IoT device).

These product components have access to the IoT device and the data it creates and uses – making these components potential attack vectors that could impact the IoT device, customer, and others (e.g., via attacks on systems, local networks, or the Internet at large). Since these additional components can introduce new or unique risks to the IoT product, the entire IoT product, including auxiliary components, must be securable.

In the context of these labeling recommendations, an IoT product is defined as an IoT device and any additional product components that are necessary to use the IoT device

[2] Consumer IoT products are those intended for personal, family, or household use.

[3] This description excludes common general purpose computing equipment (e.g., personal computers, smartphones) as well as general internet and networking infrastructure (e.g., internet routers and switches).

[4] Product components are akin to system components and do not include general purpose sub-device components such as processors and other chipsets, network cards, etc.

beyond basic operational features.[5] For example, an unconnected smart lightbulb may still illuminate in one color, but its smart features, such as color changes, cannot be used without other product components.

2.2 Recommended Baseline Product Criteria

Within the scope of a consumer IoT product, the following baseline product criteria are recommended by NIST to define the cybersecurity outcomes expected of IoT products and IoT product developers as part of a consumer IoT product labeling program. Most criteria concern the IoT product directly and are expected to be satisfied by software and/or hardware means implemented in the IoT product. Some criteria apply to the IoT product developer rather than to the IoT product directly. These criteria are expected to be satisfied through actions and supported by assertions and evidence from the developer rather than from the IoT product itself.

Product criteria are recommended to apply to the IoT product overall, as well as to each individual IoT product component (e.g., IoT device, backend, companion app), as appropriate.[6] A scheme owner has flexibility in adapting the product criteria and determining appropriate supporting evidence. Though NIST recommends that all criteria apply to every IoT product, some components may not be able or need to support all criteria. That might be the case due to product risk considerations, product development (e.g., cybersecurity tasks delegated via contracts and supply chain), nature of the components to form the product (e.g., backends may be highly distributed), or limitations of IoT components (e.g., devices may be constrained, companion software apps may have limited access and functionality).

Note: for some sub-criteria, additional detail to the outcome (i.e., normative text) is listed following **bolded** text, while additional explanation and examples (i.e., informative text) are listed following *italicized* text.

Asset Identification: The IoT product is uniquely identifiable and inventories all of the IoT product's components.

1. The IoT product can be uniquely identified by the customer and other authorized entities (e.g., the IoT product developer).
2. The IoT product uniquely identifies each IoT product component and maintains an up-to-date inventory of connected product components.

[5] NISTIRs 8259 [IR8259], 8259A [IR8259A], and 8259B [IR8259B] discuss cybersecurity related to IoT *devices*, but this work discusses IoT *products* even though these criteria are developed based on NISTIRs 8259A and 8259B. This expansion in scope is based on the large number of consumer IoT products that have some additional component beyond the IoT device itself needed to function (e.g., cloud backend, smartphone app). Since these components can have privileged and tightly coupled relationships with IoT devices, their cybersecurity will be closely related to the cybersecurity of the IoT device and, thus, the IoT product.

[6] Given the nature of consumer IoT product, it is expected that all IoT products should satisfy all technical product criteria since they will, in most cases, be finished products intended for direct plug-and-play use. Individual IoT product components, though, may be more likely to not require certain criteria (e.g., based on lack of applicability).

Cybersecurity utility: The ability to identify IoT products and their components is necessary to support asset management for updates, data protection, and digital forensics capabilities for incident response.

Product Configuration: The configuration of the IoT product is changeable, there is the ability to restore a secure default setting, and any and all changes can only be performed by authorized individuals, services, and other IoT product components.

1. The customer can change the configuration settings of the IoT product via one or more IoT product components.
2. The IoT product applies configuration settings to applicable IoT components.

Cybersecurity utility: The ability to change aspects of how the IoT product functions can help customers tailor the IoT product's functionality to their needs and goals. Customers can configure their IoT products to avoid specific threats and risk they know about based on their risk appetite.

Data Protection: The IoT product and its components protect data stored (across all IoT product components) and transmitted (both between IoT product components and outside the IoT product) from unauthorized access, disclosure, and modification.

1. Each IoT product component protects data it stores via secure means, including the ability to delete or render inaccessible data stored that is either collected from or about the customer, home, family, etc.
2. When data is sent between IoT product components or outside the product, protections are used for the data transmission.[7]

Cybersecurity utility: Maintaining confidentiality, integrity, and availability of data is foundational to cybersecurity for IoT products. Customers will expect that data is protected and that protection of data helps to ensure safe and intended functionality of the IoT product.

Interface Access Control: The IoT product and its components restrict logical access to local and network interfaces – and to protocols and services used by those interfaces – to only authorized individuals, services, and IoT product components.

1. Each IoT product component controls access (to and from) all interfaces (e.g., local interfaces, network interfaces, protocols, and services) in order to limit access to only authorized entities. **At a minimum, the IoT product and its components shall:**
    a. Use and have access only to interfaces necessary for the IoT product's operation. All other channels and access to channels are removed or secured.

[7] This may include the ability to communicate with product components that cannot fully implement the Product Component Data Protection sub-capability (e.g., cannot support adequate cryptography) in a way that reduces the subsequent risk (e.g., data transmitted with sub-par or limited protection), such as short-range and/or local network transmission protocol (e.g., Zigbee, Bluetooth) to communicate with some product components in limited, but necessary circumstances.

   b. For all interfaces necessary for the IoT product's use, access control measures are in place (e.g., unique password-based multifactor authentication).
   c. For all interfaces, access and modification privileges are limited.
2. The IoT product executes means via some, but not necessarily all, components to protect and maintain interface access control. **At a minimum, the IoT product shall:**
   a. Validate that data sent to other product components matches specified definitions of format and content.
   b. Prevent unauthorized transmissions or access to other product components.
   c. Maintain appropriate access control during initial connection (i.e., on-boarding) and when reestablishing connectivity after disconnection or outage.

Cybersecurity utility: Inventorying and controlling access to all internal and external interfaces to the IoT product will help preserve the confidentiality, integrity, and availability of the IoT product, its components, and data by helping prevent unauthorized access and modification.

Software Update: The software[8] of all IoT product components can be updated by authorized individuals, services, and other IoT product components only by using a secure and configurable mechanism, as appropriate for each IoT product component.

1. Each IoT product component can receive, verify, and apply verified software updates.
2. The IoT product implements measures to keep software on IoT product components up to date (i.e., automatic application of updates or consistent customer notification of available updates via the IoT product).

Cybersecurity utility: Software may have vulnerabilities discovered after the IoT product has been deployed; software update capabilities can ensure secure delivery of security patches.

Cybersecurity State Awareness: The IoT product supports detection of cybersecurity incidents affecting or affected by IoT product components and the data they store and transmit.

1. The IoT product captures and records information about the state of IoT components that can be used to detect cybersecurity incidents affecting or affected by IoT product components and the data they store and transmit.

Cybersecurity utility: Protection of data and ensuring proper functionality can be supported by the ability to alert the customer when the device starts operating in unexpected ways, which could mean that unauthorized access is being attempted, malware has been loaded, botnets have been created, device software errors have happened, or other types of actions have occurred that was not initiated by the IoT product user or intended by the developer.

[8] This includes executable code, as well as software libraries, support packs, and other non-executable software data.

Documentation: The IoT product developer creates, gathers, and stores[9] information relevant to cybersecurity of the IoT product and its product components prior to customer purchase, and throughout the development of a product and its subsequent lifecycle.

1. Throughout the development lifecycle, the IoT product developer creates or gathers and stores information relevant to the cybersecurity of the IoT product and its product components, **including**:
    a. Assumptions made during the development process and other expectations related to the IoT product, **including**:
        i. Expected customers and use cases.
        ii. Physical use, including security of the location of the IoT product and its product components (e.g., a camera for use inside the home that has an off switch on the device vs. a security camera for use outside the home that does not have an off switch on the device), and characteristics.
        iii. Network access and requirements (e.g., bandwidth requirements).
        iv. Data created and handled by the IoT product.
        v. Any expected data inputs and outputs (including error codes, frequency, type/form, range of acceptable values, etc.).
        vi. The IoT product developer's assumed cybersecurity requirements for the IoT product.
        vii. Any laws and regulations with which the IoT product and related support activities comply.
        viii. Expected lifespan and anticipated cybersecurity costs related to the IoT product (e.g., price of maintenance), and length and terms of support.
    b. All IoT components, including but not limited to the IoT device, that are part of the IoT product.
    c. How the baseline product criteria are met by the IoT product across its product components, including which baseline product criteria are not met by IoT product components and why (e.g., the capability is not needed based on risk assessment).
    d. Product design and support considerations related to the IoT product, *for example*:
        i. All hardware and software components, from all sources (e.g., open source, propriety third-party, internally developed) used to create the IoT product (i.e., used to create each product component).
        ii. IoT platform used in the development and operation of the IoT product, its product components, including related documentation.
        iii. Protection of software and hardware elements implemented to create the IoT product and its product components (e.g., secure boot, hardware root of trust, and secure enclave).

[9] The documentation discussed in this criterion is maintained and controlled by the IoT product developer. Sharing of this information may be appropriate and can be limited to authorized technicians and cybersecurity experts seeking more information about the IoT product (e.g., in assessing the IoT product for labeling, investigating a breach), but the documented information is not intended, in all cases, to be shared directly with consumers.

iv. Consideration of the known risks related to the IoT product and known potential misuses.
v. Secure software development and supply chain practices used.
vi. Accreditation, certification, and/or evaluation results for cybersecurity-related practices.
vii. The ease of installation and maintenance of the IoT product by a customer (i.e., the usability of the product [ISO9241]).

e. Maintenance requirements for the IoT product, *for example*:
   i. Cybersecurity maintenance expectations and associated instructions or procedures (e.g., vulnerability/patch management plan).
   ii. How the IoT product developer identifies authorized supporting parties who can perform maintenance activities (e.g., authorized repair centers).
   iii. Cybersecurity considerations of the maintenance process (e.g., how customer data unrelated to the maintenance process remains confidential even from maintainers).
f. The secure system lifecycle policies and processes associated with the IoT product, **including**:
   i. Steps taken during development to ensure the IoT product and its product components are free of any known, exploitable vulnerabilities.
   ii. The process of working with component suppliers and third-party vendors to ensure the security of the IoT product and its product components is maintained for the duration of its supported lifecycle.
   iii. Any post end-of-support considerations, such as the discovery of a vulnerability which would significantly impact the security, privacy, or safety of customers who continue to use the IoT product and its product components.
g. The vulnerability management policies and processes associated with the IoT product, **including**:
   i. Methods of receiving reports of vulnerabilities (see Information and Query Reception below).
   ii. Processes for recording reported vulnerabilities.
   iii. Policy for responding to reported vulnerabilities, including the process of coordinating vulnerability response activities among component suppliers and third-party vendors.
   iv. Policy for disclosing reported vulnerabilities.
   v. Processes for receiving notification from component suppliers and third-party vendors about any change in the status of their supplied components, such as end of production, end of support, deprecated status (e.g., the product is no longer recommended for use), or known insecurities.

Cybersecurity utility: Generating, capturing, and storing important information about the IoT product and its development (e.g., assessment of the IoT product and development practices used to create and maintain it) can help inform the IoT product developer regarding the product's actual cybersecurity posture.

Information and Query Reception: The ability of the IoT product developer to receive information relevant to cybersecurity and respond to queries from the customer and others about information relevant to cybersecurity.

1. The IoT product developer can receive information related to the cybersecurity of the IoT product and its product components and can respond to queries related to cybersecurity of the IoT product and its product components from customers and others, **including**:
    a. The ability of the IoT product developer to identify a point of contact to receive maintenance and vulnerability information (e.g., bug reporting capabilities and bug bounty programs) from customers and others in the IoT product ecosystem (e.g., repair technician acting on behalf of the customer).
    b. The ability of the IoT product developer to receive queries from and respond to customers and others in the IoT product ecosystem about the cybersecurity of the IoT product and its components.

    Cybersecurity utility: As IoT products are used by customers, those customers may have questions or reports of issues that can help improve the cybersecurity of the IoT product over time.

Information Dissemination: The IoT product developer broadcasts (e.g., to the public) and distributes (e.g., to the customer or others in the IoT product ecosystem) information relevant to cybersecurity.

1. The IoT product developer can broadcast to many/all entities via a channel (e.g., a post on a public channel) to alert the public and customers of the IoT product about cybersecurity relevant information and events throughout the support lifecycle. **At a minimum, this information shall include**:
    a. Updated terms of support (e.g., frequency of updates and mechanism(s) of application) and notice of availability and/or application of software updates.
    b. End of term of support or functionality for the IoT product.
    c. Needed maintenance operations.
    d. New IoT device vulnerabilities, associated details, and mitigation actions needed from the customer.
    e. Breach discovery related to an IoT product and its product components used by the customers, associated details, and mitigation actions needed from the customer (if any).
2. The IoT product developer can distribute information relevant to cybersecurity of the IoT product and its product components to alert appropriate ecosystem entities (e.g., common vulnerability tracking authorities, accreditors and certifiers, third-party support and maintenance organizations) about cybersecurity relevant information, *for example*:
    a. Applicable documentation captured during the design and development of the IoT product and its product components.
    b. Cybersecurity and vulnerability alerts and information about resolution of any vulnerability.

c. An overview of the information security practices and safeguards used by the IoT product developer.
d. Accreditation, certification, and/or evaluation results for the IoT product developer's cybersecurity-related practices.
e. A risk assessment report or summary for the IoT product developer's business environment risk posture.

Cybersecurity utility: As the IoT product, its components, threats, and mitigations change, customers will need to be informed about how to securely use the IoT product.

Product Education and Awareness: The IoT product developer creates awareness of and educates customers and others in the IoT product ecosystem about cybersecurity-related information (e.g., considerations, features) related to the IoT product and its product components.

1. The IoT product developer creates awareness and provides education targeted at customers about information relevant to cybersecurity of the IoT product and its product components, **including**:
    a. The presence and use of IoT product cybersecurity capabilities, **including at a minimum**:
        i. How to change configuration settings and the cybersecurity implications of changing settings, if any.
        ii. How to configure and use access control functionality (e.g., set and change passwords).
        iii. How software updates are applied and any instructions necessary for the customer on how to use software update functionality.
        iv. How to manage device data including creation, update, and deletion of data on the IoT product.
    b. How to maintain the IoT product and its product components during its lifetime, including after the period of security support (e.g., delivery of software updates and patches) from the IoT product developer.
    c. How an IoT product and its product components can be securely re-provisioned or disposed of.
    d. Vulnerability management options (e.g., configuration and patch management and anti-malware) available for the IoT product or its product components that could be used by customers.
    e. Additional information customers can use to make informed purchasing decisions about the security of the IoT product (e.g., the duration and scope of product support via software upgrades and patches).

    Cybersecurity utility: Customers will need to be informed about how to securely use the device to lead to the best cybersecurity outcomes for the customers and the consumer IoT product marketplace.

2.3 IoT Product Vulnerabilities Related to Recommended Criteria

Since IoT product vulnerabilities have led to breaches and enabled a variety of malicious activities, one goal of these criteria is to address IoT product vulnerabilities. Understanding already exploited vulnerabilities in IoT products and ensuring the consumer IoT product labeling program considers these incidents in its criteria can help to improve the cybersecurity of the IoT ecosystem.

Table 1 illustrates some real-life examples of IoT product attacks and the associated vulnerability exploits that contributed to allowing the associated security incidents to occur. In many cases when breaches occur, it is not possible to determine with certainty all the specific tactics and techniques used by the hackers to exploit vulnerabilities. Multiple techniques can be used to exploit a single vulnerability. The examples provided are not exhaustive; they aim to help in understanding the relationships between various vulnerabilities, attacks, and security criteria to prevent similar attacks.

The first column lists vulnerability factors and example actions that could have occurred through security vulnerabilities. The second column provides examples of the associated MITRE ATT&CK [ATT&CK] tactics and techniques that possibly were used to exploit the vulnerabilities. The third column lists IoT product security criteria proposed in this report that, if met, may have prevented the vulnerabilities or prevented vulnerabilities from being exploited.

Table 1: Real-world IoT product vulnerabilities and related proposed baseline criteria

Vulnerability Factors	Example Relevant Tactics: Techniques from ATT&CK	Related Baseline Criteria
Example 1: Unauthorized Access to Baby Monitors Unauthorized individuals exploited weak authentication to access data, video cameras, and microphones in baby monitors of multiple brands. In some cases, product developers failed to respond to vulnerability reports.		
Direct access to the internet combined with weak or compromised authentication credentials leave the monitor vulnerable to unauthorized access.	• Privilege Escalation: Access Token Manipulation • Credential Access: Credentials from Password Stores • Collection: Data from Configuration Repository	Product Configuration Interface Access Control Product Education and Awareness Cybersecurity State Awareness
Internet-accessible configuration details leave the monitor and local connections (i.e., home networks) easily discoverable by adversaries.	• Collection: Data from Configuration Repository	Product Configuration Product Education and Awareness
Unencrypted sensitive data is available through the baby monitor, leaving the data vulnerable to access, modification, exfiltration, and misuse.	• Collection: Data from Information Repositories • Collection: Data from Local System	Data Protection Product Education and Awareness
Example 2: Mirai Malware Variants Attacks Use of weak authentication enabled the loading of malware onto the device and use of that device in Distributed Denial of Service and other attacks.		
Not using authentication, and using weak authentication credentials, leaves the IoT	• Initial Access: Valid Accounts	Asset Identification Interface Access Control

Vulnerability Factors	Example Relevant Tactics: Techniques from ATT&CK	Related Baseline Criteria
devices vulnerable to unauthorized access through internet and other network connections.	• Execution: Command and Scripting Interpreter • Privilege Escalation: Boot or Logon Initialization Scripts	Information Dissemination Product Education and Awareness
Without intrusion detection and additional security controls for performing admin commands, the IoT device is vulnerable to having adversaries launch discovery code through the device, identify network databases, and exfiltrate the data.	• Execution: Command and Scripting Interpreter • Lateral Movement: Remote Services	Software Update Cybersecurity State Awareness Product Education and Awareness
IoT products without internal configuration and admin controls leave the products and attached networks vulnerable to having adversaries execute commands, scripts, or binaries, creating the possibility to launch malicious code or commands using the IoT product.	• Execution: Command and Scripting Interpreter • Command and Control: Data Obfuscation	Interface Access Control Documentation
Example 3: Unauthorized Access to and Publication of Fitness Tracker Data Fitness tracker location data for military personnel was publicly posted even when the product was configured for privacy.		
Web application vulnerabilities created by faulty software coding or an insufficiently secured web server leave sensitive data vulnerable to viewing, copying, exfiltrating, modifying or deleting by unauthorized entities through the internet.	• Initial Access: Exploit Public-Facing Application • Lateral Movement: Lateral Tool Transfer • Command and Control: Application Layer Protocol	Product Configuration Cybersecurity State Awareness Documentation Information Dissemination
Unsecured data stored in mobile applications (e.g., without secure file permissions or in insecure locations such as external storage directories) enable vulnerabilities allowing unauthorized access to data.	• Initial Access: Deliver Malicious App via Authorized App Store • Persistence: Code Injection • Collection: Data from Local System	Product Configuration Cybersecurity State Awareness Documentation Information Dissemination
Using weak de-identification methods leaves data vulnerable to being re-identified allowing unauthorized access to sensitive data.	• Privilege Escalation: Abuse Elevation Control Mechanism • Discovery: File and Directory Discovery	Product Configuration Data Protection Documentation
Example 4: Unauthorized Access to Home Security Camera Data and Controls Unauthorized access to data and views of the inside and outside of buildings occurred with multiple brands of security cameras.		
Having weak or no authentication methods leaves home security product configuration controls and data vulnerable to access by unauthorized entities.	• Initial Access: External Remote Services • Initial Access: Valid Accounts	Interface Access Control

Vulnerability Factors	Example Relevant Tactics: Techniques from ATT&CK	Related Baseline Criteria
Weak data protection in storage and transit creates vulnerabilities within home security cameras allowing adversaries to exfiltrate data.	• Discovery: File and Directory Discovery • Persistence: Boot or Logon Autostart	Data Protection Documentation Information Dissemination
Manufacturers and their support entities without procedures for consumers to ask questions about secure device use, report security complaints, etc., leave consumers and products vulnerable.	• Impact: Data Manipulation	Information and Query Reception
Lack of monitoring capabilities within home security camera products, and lack of supporting procedures for reacting to home safety event triggers, leave consumers vulnerable when quick response is needed to events.	• Command and Control: Data Obfuscation • Command and Control: Proxy • Behavior Prevention on Endpoint: Windows Management Instrumentation	Asset Identification Product Configuration Documentation
Lack of access control to data recording/collection leaves critical home security camera data vulnerable to unauthorized deletion, exfiltration, viewing, and modification.	• Command and Control: Data Obfuscation • Collection: Video Capture	Asset Identification Product Configuration Documentation Information Dissemination Product Education and Awareness
Example 5: Access to Data and Networks Through Used IoT Devices Still accessible data on secondhand IoT devices putting previous owners at risk		
When data has not been removed from devices, and/or devices have not been reset to factory settings, the devices are vulnerable to having the data and device settings (which may include account credentials, sensitive images, network connection data, etc.) accessed by subsequent device owners.	• Credential Access: Credentials from Password Stores • Collection: Data from Configuration Repository Privilege Escalation: Access Token Manipulation	Product Configuration Interface Access Control Product Education and Awareness Cybersecurity State Awareness
Devices with network configuration settings and other details enable subsequent IoT product users to gain access to associated networks.	• Collection: Data from Configuration Repository	Product Configuration Product Education and Awareness
Sensitive data in storage within used IoT products are vulnerable to access, use and misuse by subsequent users of the IoT product.	• Collection: Data from Information Repositories • Collection: Data from Local System	Data Protection Product Education and Awareness
Example 6: Unauthorized Access to Data and Networks Through a Smart Fish Tank Thermometer Unauthorized access to the fish tank thermometer enabled hackers to reach sensitive databases and exfiltrate data		
Lack of access controls from the smart thermometer to the attached network devices left servers, databases, and other digital assets vulnerable through the	• Lateral Movement: Exploitation of Remote Services	Interface Access Control Documentation

Vulnerability Factors	Example Relevant Tactics: Techniques from ATT&CK	Related Baseline Criteria
smart thermometer.	• Initial Access: External Remote Services	
Remote access from the internet to the smart thermometer made the device and network to which the thermometer was attached vulnerable to unauthorized remote commands.	• Execution: Exploitation for Client Execution • Execution: Command and Scripting Interpreter	Product Configuration Product Education and Awareness
Lack of alarms or other indicators from the device of unusual activities made the smart thermometer preclude notice by network administrators of the compromised state of the device.	• Lateral Movement: Exploitation of Remote Services • Impact: Endpoint Denial of Service • Discovery: System Information Discovery	Cybersecurity State Awareness

2.4 Risk, Tailoring, and Tiering Considerations

Considering the heterogeneity of consumer IoT products, components, use cases, risks, and mitigations, the criteria outlined in Section 2.2 are not prescriptive with respect to how they would be achieved. Rather, they are stated in such a way that resources such as standards or conformity assessment approaches can be used to build a program that demonstrates support for the recommended outcomes. This approach offers multiple benefits:

- Flexibility in meeting the criteria to support different IoT product (e.g., component combinations) cybersecurity (e.g., ways to satisfy the criteria) approaches, which allows for a robust cybersecurity marketplace and ecosystem that can meet disparate needs and contexts.
- Easy adaptability as technologies and risks change over time. Outcome oriented criteria enable those changes rather than specifying current solutions. This allows cybersecurity solutions and mitigations to be upgraded and changed over time without significant changes in the product criteria for labeling.
- Outcomes speak directly to the risks they are intended to mitigate, which can help guide a developer or conformity assessor in determining the applicability of criteria to a specific IoT product or its components.

While the outcome-based approach allows for the flexibility required by a diverse marketplace of IoT products, the role of the scheme owner is critical to ensure that supporting evidence demonstrates that the product meets the expected outcomes. A scheme owner should consider aspects of risk and intended use of IoT products as they consider how a consumer IoT labeling program will be deployed and operate. These and other aspects of a consumer IoT labeling program design may lead scheme owners to tailor the outcomes and/or supporting evidence for different consumer IoT products, possibly including establishing adequate and appropriate tiers for the consumer IoT labeling program. A scheme owner should consider:

- Risks to the IoT product (including its data).

- Risks to each IoT product component.
- Risks to the customer (via the IoT product or its components).
- Risks to the community (e.g., society, the Internet).
- Mitigations appropriate to those risks.
- Implementation across product components of those mitigations.

The scheme owner will synthesize these with other considerations related to the consumer IoT labeling program (e.g., conformity, labeling) to determine how to best apply the baseline criteria related to all IoT product components given the heterogeneity of IoT product implementations. The scheme owner must also consider how to best apply the baseline criteria to all IoT products, where risks and appropriate mitigations may vary. In their connection to networks, IoT products have a common need for the baseline cybersecurity described in Section 2.2. After this common baseline, there is no single criterion to drive the definition of higher tiers. While IoT product developers have expected use cases for products, innovative new types and uses for IoT products with new risks will continue to emerge. A scheme owner may determine that some use cases and/or risks may warrant criteria beyond the baseline identified in Section 2.2.

Tiers are best determined and designed into the consumer IoT product labeling program by the scheme owner. As a scheme owner applies the baseline criteria to all IoT products, a path for tiers to be built into a labeling program that is not readily apparent at this stage may be realized. While some existing IoT cybersecurity labeling approaches use differentiated tiers, there is no single approach to defining cybersecurity tiers. Opportunities to create tiers are also not limited to technical criteria; they also can be built from increasingly rigorous conformity testing. Some existing and proposed approaches include defining higher cybersecurity tiers above an initial baseline with the following characteristics:

- Additional product criteria defined by the perceived inherent risk of the device type (e.g., stove, baby monitor).
- Additional product criteria defined by the perceived inherent risk of the expected use case (e.g., camera will be used in a security system).
- Additional requirements and testing tools (e.g., penetration testing) were used to gather evidence of conformity with the criteria.

Ultimately, the scheme owner must consider all aspects of the consumer IoT landscape and devise the best approach to apply the baseline criteria to all consumer IoT products, including any tiers. Scheme owners may also have to build out requirements that can directly inform a conformity assessment (e.g., a test plan) to ensure sufficient evidence of conformity to the criteria is captured to justify the IoT product being labeled.

2.5 Utilizing Existing Standards, Programs, and Schemes

An understanding of any tailoring and/or tiers desired beyond the baseline criteria will inform requirements or other methods of demonstrating conformity to the outcomes. Flexibility and agility are required of any approach to a cybersecurity label for consumer IoT products given the broad and changing range of products, risks, capabilities, and architectures**. Use of existing resources such as standards, programs, and schemes can enable implementation of the**

criteria recommended in this report and encourage continued development and expansion of these resources. This approach allows for a diverse set of technical implementations to be identified by a scheme owner while enabling innovation over time.

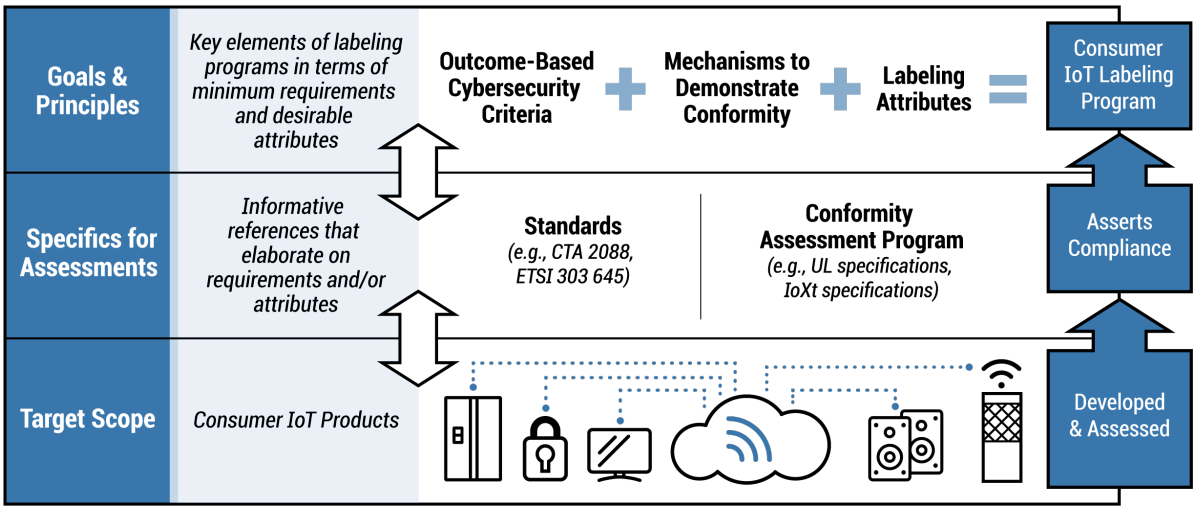

Figure 1: Building a consumer IoT labeling program using existing standards and programs

Figure 1 illustrates ways in which a consumer IoT labeling scheme owner could use existing resources. A consumer IoT labeling scheme owner may use existing conformity assessment programs and work with the owners of those programs to help build out, in whole or in part, the consumer IoT labeling program. A scheme owner may also use other existing resources such as standards to help build out a program, which could provide additional benefits (e.g., alignment with international consumer IoT labeling programs). Ultimately, it is a scheme owner's discretion to use any existing standard or program as part of the consumer IoT product labeling program.

Example uses of existing resources by a scheme owner

Existing IoT product or product component conformity assessment programs may meet the consumer IoT labeling program scheme owner's goal for some or all IoT products, in which case the scheme owner could use those existing programs as part of the labeling program. A consumer IoT labeling scheme owner may also determine that one or more standards meet the product criteria for some or all IoT products or product components. This could allow the scheme owner to use the standards as a basis of more specific requirements that can be used to assess conformance to the product criteria.

2.6 Harmonization Considerations

Any consumer IoT product labeling program will exist in a changing ecosystem of IoT conformity assessment schemes. Therefore, harmonization among schemes may offer benefits to developers, customers, or both. Fragmentation with other IoT schemes in the U.S. or internationally may create challenges for the consumer IoT marketplace and customers alike.

Since there may be conformity assessment programs available for IoT product components individually, within or outside the context of IoT, consideration of harmonization and fragmentation with the existing schemes used by these programs is important. For example, some existing IoT standards and programs focus on the IoT device rather than the larger IoT product [CTA2088]. For products or equipment outside of the scope of IoT, other product components may have harmonization considerations as well. For example, if scheme owners do not take care to appropriately scope and harmonize the consumer IoT product labeling program relative to others (e.g., a consumer software labeling program also explored by NIST in response to EO 14028), there could be confusion about applicability of these programs to some IoT product components like mobile apps. Table 2 highlights some specific examples of the benefits and challenges.

Table 1: Example considerations of harmonization for the consumer IoT product labeling program

Examples of…	
Benefits of harmonization	*Challenges of fragmentation*
• Clear focus and direction for adoption of cybersecurity reflected in the aligned outcomes • Predictability of cybersecurity for consumers across products that use harmonized requirements	• IoT product developers must build to multiple sets of requirements, complicating bringing the same product to market in multiple jurisdictions • Possible confusion over different programs and divergent requirements

NIST recommends considering harmonization with other schemes, but notes that harmonization may not always be possible, especially in the heterogeneous and diverse consumer IoT marketplace. Technical criteria, conformity assessment, and labeling requirements may not be able to completely align with any or all other programs'. A scheme owner should consider the benefits of harmonization and challenges of fragmentation when considering the degree of harmonization.

3 Labeling Considerations

The IoT product cybersecurity labeling provisions in the EO aim to aid consumers in their IoT purchase decisions by enabling comparisons among products and educating them about IoT cybersecurity considerations. This transparency may also encourage IoT product developers to consider cybersecurity aspects of their IoT products and ways to achieve greater consumer trust and confidence in the IoT products – and ultimately, to improve the management of related cybersecurity risks.

A label's impact on consumer purchase decisions can be influenced by multiple factors, such as time pressure when making a purchase decision and competing priorities (e.g., product functionality, availability of non-connected similar products, and cost). A labeling program can facilitate the purchase of more secure IoT products by considering related needs and opportunities to educate consumers based on robust consumer-focused testing. Section 3 provides: an overview of different approaches to labeling; the NIST recommended approach for an IoT label; considerations for how the label might be provided to a consumer; how to mitigate potential issues with the recommended approach; and consumer education considerations.

These labeling recommendations are intended to support non-expert, home users of IoT products. More technically detailed communication for expert users is out of scope for this document.

This document does not discuss specific label design elements, such as the use of icons, text, colors, or typography. However, when a label is designed, **the usability of the label design as well as the usability of consumer education material should be assessed via rigorous consumer testing**. **Including a demographically diverse, U.S. census-representative sample of consumers of varying disabilities and abilities in consumer testing is critical for determining that the label is broadly understandable and ensuring testing results are not biased.** The sample size should be large enough for sufficient statistical power when analyzing test results.

Consumer testing prior to program implementation is valuable, but initial perceptions and expressions of intent to purchase may differ from actual consumer behavior. **Periodic testing with a diverse sample of consumers after a program is implemented is essential and can include market studies to assess the continued appropriateness and usability of the label approach, the impact on consumer purchase decisions, and the growth of brand recognition over time.**

3.1 Recommended Label Approach

In proposing an approach for IoT product cybersecurity labeling, NIST relied on the following guiding principles:

1. The labeling approach should be appropriate to the proposed IoT product cybersecurity label technical criteria.
2. The labeling approach should be usable by a diverse range of consumers without requiring them to have specialized cybersecurity knowledge.

Recognizing that all labeling approaches have their strengths and weaknesses, **NIST recommends that a binary label (a single label indicating a product has met a baseline standard) should be adopted for an IoT cybersecurity label**. **NIST also recommends coupling the binary label with a layered approach** in which one of the following is included on the label to lead consumers to additional details online:

- a URL (e.g., as included in Singapore's cybersecurity label [SINGAPORE]), not a shortened URL, which is not easily attributed to the source domain
- a scannable code (e.g., a QR code).

3.2 Label Presentation

Labels should be available to consumers before and at the time and place of purchase (in-store or online) as well as after purchase. An IoT product cybersecurity label should be flexible in supporting both physical and digital formats as appropriate.

3.3 Consumer Education

Binary labels should be accompanied by a robust consumer[10] education[11] campaign. Such an initiative should be developed to establish and increase label recognition, provide transparency to consumers about important aspects of the program, and ensure a common way for IoT product stakeholders to talk about the labels. *Who* provides this information (e.g., labeling program administrator, IoT product developers) will depend on the final construct of a labeling program. **Because consumer education will be an involved undertaking, it should be a shared responsibility among multiple IoT product security stakeholders** (e.g., scheme owners, retailers who are often the first point of contact for consumers, manufacturers, industry and non-profit security groups, academia, or the government).

At a minimum, consumers should have online access – not necessarily included in the label itself – to the following information:

- Intent and scope: What the label means and does not mean, including addressing potential misinterpretations (e.g., stating that meeting the label security criteria reduces risk but does not eliminate it entirely, and that labeled products are not necessarily more secure than unlabeled products); inclusion of a statement that a label does not imply product endorsement by the label program.
- Product criteria: What cybersecurity properties are included in the baseline and why and how these were selected; include information on how the criteria address security risks

[10] Note that although this section describes education materials for consumers, education for developers /manufacturers and retailers is also of great importance and can borrow from the consumer education materials as much as possible to ensure consistency.

[11] Note that this education material is focused on the labeling program and is in addition to and distinct from IoT product developers meeting the proposed baseline criteria for product documentation outlined above.

both to the consumer and to others (e.g., if co-opted into a botnet) for common intended uses of the products.

- A glossary of applicable technical terms, written in plain language.
- General information about conformity assessment: How cybersecurity properties are evaluated.
- Declaration of conformity: The product's specific declaration of conformity to the baseline criteria, including the date the label was last awarded.
- Scope: The kinds of products eligible for the label and an easy way for consumers to identify labeled products.
- Changing applicability: The current state of product labeling as new cybersecurity threats and vulnerabilities emerge.
- Security considerations for end-of-life IoT products and implications for functionality if the product is no longer connected
- Expectations for consumers: The responsibility consumers share in securing software and how their actions (or inactions) can impact the software's cybersecurity.
- Contact information for the labeling program and information on how consumers can lodge a complaint against a vendor regarding a product label.

Particular care should be taken with the messaging and framing of consumer education material. Similar to the layered label approach described above, **a layered approach for consumer education materials is recommended** as it allows for basic information in a first level of consumer education material with links to more detail if desired.

4 Conformity Assessment Considerations

Conformity assessment provides a means of demonstrating that specified requirements are fulfilled. Several conformity assessment approaches can be used depending on specified requirements, the risk of nonconformity, and overall objectives. A conformity assessment scheme consists of a set of rules and procedures that:

- describes the objects of conformity assessment (e.g., a consumer IoT product);
- identifies the specified requirements (e.g., technical requirements as described in Section 2 of this document);
- identifies the activities for performing conformity assessment (e.g., testing, inspection, certification, self-declaration of conformity); and
- defines roles and the types of organizations performing each role (e.g., first-, second- or third-parties).

A conformity assessment scheme defines how conformity assessment activities, roles, and output are structured and managed. **The scheme owner determines the structure and management and performs oversight to ensure that the scheme is functioning consistently in keeping with overall objectives.** Scheme owners can be public or private sector organizations.

Given the range of consumer IoT products, related use cases, associated risks, and a relative lack of applicable international standards for consumer IoT products, **a single conformity assessment approach is not likely to achieve desired objectives.** In the context of consumer IoT products, the purchaser may be unequipped to meaningfully assess the cybersecurity of an IoT device, so conformity assessment – including provision of meaningful, consumer-oriented information about the implication of that assessment – could be critical. This document does not recommend a particular set of conformity assessment requirements related to the baseline IoT product criteria.

Rather, **NIST recommends that a consumer IoT labeling scheme owner is necessary to tailor the recommended product criteria, define conformity assessment requirements, develop the label and associated information, and conduct related consumer outreach and education.** Having a scheme owner facilitates fulfilling the primary objective of providing consumers with understandable and actionable cybersecurity-related information about a product.

There are several IoT conformity assessment activities that could be leveraged to demonstrate that consumer IoT devices conform to technical requirements, either exclusively or in combination. These include:

- Supplier's declaration of conformity (self-attestation) where the declaration of conformity is performed by the organization that provides the consumer IoT device. This is a self-attestation against a defined set of criteria.
- Third-party testing or inspection where there is determination or examination, respectively, of the consumer IoT device based on defined criteria.
- Third-party certification of the consumer IoT device where a statement is issued based on a comprehensive review that an IoT product has fulfilled defined criteria.

References

[ATT&CK] The MITRE Corporation (2015) *ATT&CK.* Available at: https://attack.mitre.org/

[CTA2088] Consumer Technology Association (2020) ANSI/CTA-2088: Baseline Cybersecurity Standard for Devices and Device Systems. Available at: https://shop.cta.tech/collections/standards/products/baseline-cybersecurity-standard-for-devices-and-device-systems-cta-2088

[EO14028] Executive Order 14028 (2021) Improving the Nation's Cybersecurity. (The White House, Washington, DC), DCPD-202100401, May 12, 2021. https://www.govinfo.gov/app/details/DCPD-202100401

[IR8259] Fagan M, Megas KN, Scarfone K, Smith M (2020) Foundational Cybersecurity Activities for IoT Device Manufacturers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8259. https://doi.org/10.6028/NIST.IR.8259

[IR8259A] Fagan M, Megas KN, Scarfone K, Smith M (2020) IoT Device Cybersecurity Capability Core Baseline. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8259A. https://doi.org/10.6028/NIST.IR.8259A

[IR8259B] Fagan M, Marron J, Brady KG, Jr, Cuthill BB, Megas KN, Herold R (2020) IoT Non-Technical Supporting Capability Core Baseline. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8259B. https://doi.org/10.6028/NIST.IR.8259B

[ISO9241] International Organization for Standardization/International Electrotechnical Commission (2018) *ISO 9241-11:2018 Ergonomics of human-system interaction – Part 11: Usability: Definitions and concepts* (ISO Geneva, Switzerland). Available at https://www.iso.org/standard/63500.html

[SINGAPORE] Cyber Security Agency of Singapore (2020) *Singapore's Cybersecurity Labelling Scheme*. Available at https://www.csa.gov.sg/Programmes/cybersecurity-labelling/for-consumers

Appendix A—Glossary

IoT Product	An IoT device and any other product components necessary to use the IoT device.
IoT Product Component(s)	Equipment (i.e., hardware and software) other than the primary device that can be hosted remotely, locally, or on other equipment (e.g., a mobile app on the customer's smartphone) that supports the IoT device in its functionality.
Authorized Individuals, services, and other IoT product components	An entity (i.e., a person, device, service, network, domain, developer, or other party who might interact with an IoT device) that has implicitly or explicitly been granted approval to interact with a particular IoT device.
IoT Product Developer	The entity that creates an assembled final IoT product. Some cybersecurity outcomes may be supported by the IoT product developer's suppliers or other contracted third-parties with support responsibilities related to the IoT product or its components.
Customer and Others in the IoT Product Ecosystem	The person receiving a product or service and third-parties (e.g., other IoT product developers, independent researchers, media and consumer organizations) who have an interest in the IoT product, its components, data, use, assumptions, risks, vulnerabilities, assessments, and/or mitigations.
Information Relevant to Cybersecurity	Information describing use of, assumptions, risks, vulnerabilities, assessments, and/or mitigations related to the IoT product, its components, and data.
Product Component Host	The organization, individual, and/or system that hosts the product component. Product component hosts may provide support for or supersede the need to test criteria since they are expected to implement, control, and verify the criteria.
Conformity Assessment	Demonstration that specified requirements are fulfilled.
Scheme	Set of rules and procedures that describes the objects of conformity assessment, identifies the specified requirements and provides the methodology for performing conformity assessment.
Scheme Owner	Person or organization responsible for the development and maintenance of a conformity assessment system or conformity

	assessment scheme.
Supplier's Declaration of Conformity (SDoC)	Declaration where the conformity assessment activity is performed by the person or organization that provides the 'object' (such as product, process, management system, person or body) and the supplier provides written confidence of conformity.
Testing	Determination of one or more characteristics of an object of conformity assessment, according to a procedure.
Inspection	Examination of an object of conformity assessment and determination of its conformity with detailed requirements or, on the basis of professional judgement, with general requirements.
Certification	Third-party attestation related to an object of conformity assessment, with the exception of accreditation.
Layered Binary Label	Label that has only one design and is applied to IoT products that meet appropriate requirements but allows for unique layers that provide specific information about the IoT product (e.g., URL or scannable code).