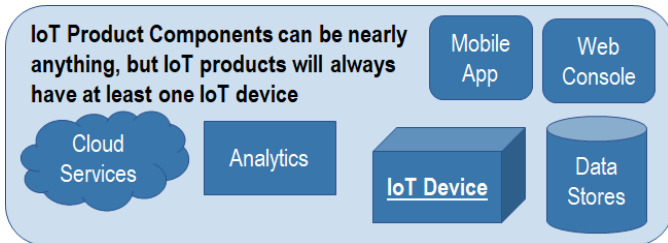


NIST CYBERSECURITY & PRIVACY PROGRAM

CONSUMER IOT PRODUCT CYBERSECURITY BASELINE

As part of an assignment under the [Presidential Executive Order on Improving the Nation's Cybersecurity \(14028\)](#) issued on May 12, 2021, NIST is responsible for a multi-faceted initiative related to [cybersecurity labeling for consumers](#). That includes labeling for Internet of Things (IoT) products.



WHAT IS A CONSUMER IoT PRODUCT?

Consumer **IoT products** are IoT products that are intended for personal, family, or household use though may be found in enterprise, especially small business environments as well.

WHAT IS AN IoT PRODUCT?

An IoT product includes the **IoT device** or IoT devices and any additional **components** (e.g., backend, mobile app) that are necessary to use the IoT device. All IoT products have at least one IoT device.

WHAT IS AN IoT DEVICE?

IoT devices have at least one sensor or actuator for interacting directly with the physical world and at least one network interface (e.g., Ethernet, Wi-Fi, Bluetooth) for interfacing with the digital world.

WHAT IS AN IoT PRODUCT COMPONENT?

An IoT device or other digital equipment or service (e.g., backend, mobile app) used to create IoT products.

WHAT IS THE NIST CONSUMER IoT CYBERSECURITY BASELINE?

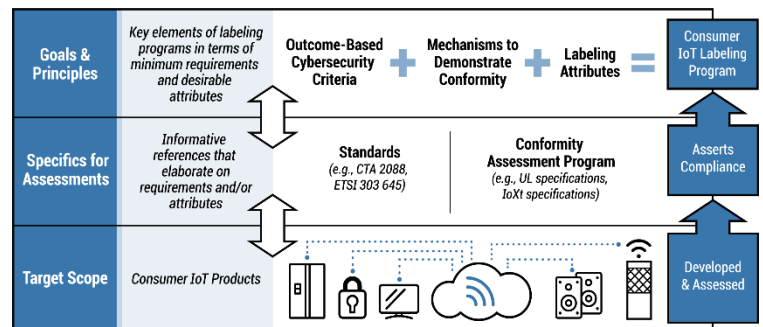
The baseline identifies a minimum set of **criteria**, articulated as cybersecurity outcomes that should be supported by most consumer connected products. The consumer IoT baseline built on the existing core recommendations that were developed to address all types of IoT devices (consumer, industrial, agriculture, retail).

ARE THERE LEVELS OF ASSURANCE IN THE BASELINE?

No, of the program owner or other stakeholder identifies that a product has a higher level of risk, the baseline may require a specific **profile** that further constrains implementation or introduces *additional* criteria.

WHY CYBERSECURITY OUTCOMES?

Consumer IoT encompasses a wide range of connected products and product capabilities. Criteria describe the expected cybersecurity outcome but rely on standards that can help elaborate how the outcome is met.



WHAT ARE CRITERIA & SUB-CRITERIA?

Criteria establish high level cybersecurity **outcomes** that a product should be able to achieve. Different approaches might be needed (depending on the architecture, capabilities etc.). Each criterion contains sub-criteria—which provides greater detail, specificity, or granularity.

Example: *Documentation* is the criterion (see images to the right).

The sub-criteria include, for example, documentation regarding the data created and handled by the IoT product, expected lifespan, and anticipated cybersecurity costs related to the IoT product (e.g., price of maintenance)—as well as length and terms of support, secure software development, and supply chain practices used.

CAN THESE OUTCOMES APPLY TO ALL CONSUMER IoT PRODUCTS?

The criteria were developed with all consumer IoT product types in mind. Thus, they are broadly applicable to the market and identify **cybersecurity outcomes that can be applied to all consumer IoT products**. There are many kinds of consumer IoT products, and different products may require additional or more specific outcomes to be met than in the general case.

Example: Configuration settings will vary based on the features and capability of a product and the Product Configuration criteria may need to be tailored as such.

Standards and conformity assessment programs can play a role in understanding how the criteria would be met by specific kinds of consumer IoT products and may be used to develop assessment procedures for a specific consumer IoT product or category.







More information about this work is available on a [dedicated website](#).





Information about NIST’s broader portfolio of work in cybersecurity and privacy can be found [here](#).

Questions should be directed to: iotsecurity@nist.gov.

WHAT ARE THE TEN RECOMMENDED NIST CYBERSECURITY CRITERIA?

NISTIR 8425 identifies **six** criteria that directly apply to IoT products their components and **four** cybersecurity criteria that apply specifically to the IoT product developer:

 Asset Identification	IoT product can be uniquely identified and should manage an inventory of its IoT product components.
 Product Configuration	IoT product’s configuration can be securely changed and restored to a secure default.
 Data Protection	IoT products protect data stored by, sent from, or received by the product components.
 Interface Access Control	IoT product restricts access to interfaces to only authorized individuals, services, and/or product components for any given use.
 Software Update	Means are available to keep IoT product and component software updated using a secure mechanism.
 Cybersecurity State Awareness	IoT products can help detect cybersecurity incidents affecting or affected by IoT product components and their data.

 Documentation	Information related to cybersecurity of the IoT product is captured throughout the lifecycle of the product, such as the plans, processes, and policies for how the IoT product’s cybersecurity is supported.
 Information and Query Reception	The customer and others can send information and queries related to the cybersecurity of the IoT product to the product developer.
 Information Dissemination	Information relevant to cybersecurity (e.g., vulnerability reports, update notifications) can be sent to pertinent individuals and/or organizations, sometimes, but not always including the customer.
 Product Education & Awareness	Customers can be informed about and can understand how to use the cybersecurity features of IoT products.