Consumer Cybersecurity Labeling for IoT Products: Discussion Draft on the Path Forward

1 Introduction

This document provides an update on work by the National Institute of Standards and Technology (NIST) to initiate a "pilot" program on cybersecurity labeling for IoT products as required under Executive Order (EO) 14028, "Improving the Nation's Cybersecurity." NIST proposes an approach and key considerations to be taken into account in a consumer IoT product cybersecurity labeling program, including proposed baseline product criteria as well as labeling and conformity assessment considerations. **NIST will identify key elements of labeling program in terms of minimum requirements and desirable attributes – rather than establishing its own program; it will specify desired outcomes, allowing providers and customers to choose best solutions for their devices and environments.** One size will not fit all, and multiple solutions might be offered by label providers. Additional information and considerations are included in the appendices. Nevertheless, NIST has concluded that multiple variations of labeling approaches likely would cause confusion among consumers and limit the effectiveness of such efforts. It is critical that labeling criteria and the labels themselves be consistent across products and labeling program offerings.

Additional details about NIST's approach are provided in Appendix B of this document. Due to the tight timetable for meeting the assignments in the EO and the extensive input and feedback provided already, NIST is not proposing a formal comment period. However, NIST welcomes feedback on this proposal, especially at the December 9, 2021, workshop on the labeling efforts. NIST also will review timely comments submitted to labeling-eo@nist.gov.

2 Potential Roadmap to a Cybersecurity Label for Consumer IoT Products

Since initiating its efforts regarding a cybersecurity label for consumer IoT products as required under EO 14028, NIST has worked to identify key elements of labeling programs in terms of minimum requirements and desirable attributes – rather than establishing its own programs. One size will not fit all, given the range of consumer IoT products.

A critical challenge is that consumers generally do not have the expertise to distinguish between different technical or conformity assessment requirements underlying a label even though variability in approaches across different IoT product types or use cases is appropriate. Variability in approaches for similar product types or use cases that all receive the same or similar labels could cause confusion.

This challenge, coupled with the information and feedback NIST received through workshops and comments, has led to the following key proposals for consideration.

- Baseline product criteria for consumer IoT products are expressed as outcomes rather than specific statements as to how they would be achieved.
- Given the variety of ways those baseline criteria could apply, no single conformity assessment approach is appropriate.
- 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.

- In order to ensure consistent application of the previous recommendations, the role of a consumer labeling scheme owner is critical. This could be a public or private sector organization. A scheme could be defined at a sector level, or an overall scheme owner could be responsible for multiple categories. The scheme owner would be responsible for tailoring the product criteria, defining conformity assessment requirements, developing the label and associated information, and conducting related consumer outreach and education.

This document provides additional information and context related to these proposals. The intent is to generate additional stakeholder input to inform final criteria for approaching cybersecurity labeling of consumer IoT products that could be effectively implemented by a scheme owner.

3 Baseline Product Criteria

The proposed baseline product criteria for the consumer IoT product cybersecurity labeling program reflect the intent to develop **product-focused outcomes** that can guide the labeling program. This section describes the scope and approach of the proposed baseline product criteria and states each criterion. These criteria can be used by a scheme owner to identify or define statements/requirements that reflect the outcomes for the labeling program. This could leverage existing assessment approaches as well as international standards. Additional information about NIST's approach, motivations, and rationale can be found in the Appendix B.

3.1 Scope of an IoT Product

Consumer 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. In some cases, this IoT product is purchased as one piece of equipment (i.e., an IoT device), but that equipment requires support from other components to operate, such as a remote backend or companion user application on a personal computer or smartphone. **In the context of this labeling scheme, an IoT product is defined as an IoT device and any additional product components that are necessary to using the IoT device beyond basic operational features.**[1] For example, an unconnected smart lightbulb may still illuminate in one color, but its smart features, such as color changes, cannot be used with other product components.

Using the above definition to identify IoT product components as they are meant for this labeling scheme, product criteria shall apply to the IoT product overall, as well as to each individual IoT product component (e.g., IoT device, backend, companion app).[2] Some proposed criteria apply to the IoT product developer rather than to the IoT product directly. These criteria are expected to be satisfied

[1] 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.

[2] Given the nature of consumer IoT product, it is expected that most 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 lack the need for certain criteria.

through actions and supported by assertions and evidence from the developer rather than from the IoT product itself.

Key terms have been hyperlinked to their definitions in the glossary in Appendix A. Each criterion is named in bold, its outcome stated, then sub-outcomes that provide more clarity to the outcome are provided. For some sub-outcomes, additional detail to the outcome (i.e., normative text) is provided following **bolded** text, while additional explanation and examples (i.e., informative text) is provided following *italicized* text. In addition to these outcome definitions, a statement of the cybersecurity utility for each criterion is also provided, and the criteria are followed by a table that shows how real-world vulnerabilities and mitigating against them are related to the proposed criteria.

3.2 Proposed Baseline Product Criteria

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.

Cybersecurity utility: The ability to identify assets, including IoT products and its components, which 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 have varying risk appetites and may know of more specific threats and risks that they can configure their IoT products to avoid.

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 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.[3]

Cybersecurity utility: Maintaining confidentiality, integrity, and availability of data is foundational to cybersecurity for IoT products. Customers will expect that data is protected and protection of data helps ensure safe and intended functionality from 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) so as 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 locked down
    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 for the interfaces and users of the interfaces
2. The IoT product, via some, but not necessarily all components, executes means to protect and maintain interface access control. **At a minimum, the IoT product shall:**
    a. Validate 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/outages

Cybersecurity utility: Inventorying and controlling access to all interfaces both internal and external 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[4] 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

[3] 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, mDNS, LLDP, and IEEE 1905.1) to communicate with some product components in limited, but necessary circumstances.

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

via the IoT product), except parts of the software update handled by the product component host.

Cybersecurity utility: Software may have vulnerabilities discovered after the IoT product has been deployed, which means software update capabilities that can ensure secure delivery of security patches is important for cybersecurity.

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 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.

Documentation: The IoT product developer creates, gathers, and stores 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 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 which has an off switch on the device vs. a security camera for use outside the home which 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. 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, anticipated cybersecurity costs related to the IoT product (e.g., price of maintenance), and length and terms of support
    b. All IoT components, including 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., lack of need for the capability 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)
    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 at a minimum**:
    i. Steps taken during its 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 process of coordinating vulnerability response activities among component suppliers and third-party vendors
    iv. Policy for disclosing reported vulnerabilities

v. Process 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 and 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 for 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 cybersecurity of the IoT product and its product components and respond to queries related to cybersecurity of the IoT product and its product components from customers and others, **including**:
    a. The ability for 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 for 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, they may have questions or reports of issues that can help improve the cybersecurity of the IoT product for customers 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 device
    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 need 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 or mitigation the customer should take
c. Cybersecurity and vulnerability alerts and information about resolution of any vulnerability
d. An overview of the information security practices and safeguards used by the IoT product developer
e. Accreditation, certification, and/or evaluation results for the IoT product developer's cybersecurity-related practices
f. 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.

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, etc.) 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 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 (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.

Table 1 illustrates some examples of IoT product vulnerabilities that contributed to security incidents. These vulnerabilities, and the potential to exploit them, demonstrate the need for the associated product criteria.

Table 1: Real-world IoT Product Vulnerabilities and Relevant Proposed Baseline Criteria

Vulnerability	Relevant Proposed Baseline Criteria
Marai Malware Variants Attacks – Use of weak authentication to enable the loading of malware onto the device and use that device in DDOS and other attacks.	
Unauthorized access to the IoT device	Asset Identification Interface Access Control Information Dissemination Education and Awareness
Malicious code can be loaded on the IoT device	Software Update Cybersecurity State Awareness Education and Awareness
Commands can be launched using the device	Interface Access Control Documentation
Unauthorized Publication of Fitness Tracker Data – Fitness tracker location data for military personnel was publicly posted even when product was configured for privacy.	
Web application vulnerabilities	Product configuration Cybersecurity State Awareness Documentation Information Dissemination
Mobile application vulnerabilities	Product Configuration Cybersecurity State Awareness Documentation Information Dissemination
Ability for de-identified data to be re-identified	Product Configuration Data Protection Documentation
Unauthorized access to home security camera data – Unauthorized access to data and views of the inside and outside of buildings occurred with multiple brands of security cameras.	
Weak authentication	Interface Access Control
Unauthorized data sharing	Data Protection Documentation Information Dissemination
Non-responsive to questions and complaints to the developers	Information and Query Reception
Lack of monitoring capabilities and procedures	Asset Identification Product Configuration Documentation
Lack of data recording/collection controls	Asset Identification Product Configuration Documentation Information Dissemination Education and Awareness

Used IoT Devices – Secondhand IoT devices putting previous owners at risk [GOODIN]	
Access to account credentials	Product Configuration Interface Access Control Education and Awareness Cybersecurity State Awareness
Access to network details	Product Configuration Education and Awareness
Access to sensitive data	Data Protection Education and Awareness
Unauthorized Access to Baby Monitors – Unauthorized individuals exploiting weak authentication to access data and microphones in baby monitors in multiple brands. In some cases, product developers failed to respond to vulnerability reports.	
Unauthorized remote commands	Interface Access Control Documentation Information and Query Reception
Access to clear text view of all the commands to and through the device	Data Protection Documentation
IoT device settings changes	Interface Access Control Documentation Education and Awareness
Fish Tank Thermometer – Unauthorized access to the fish tank thermometer enabled hackers to reach sensitive database and exfiltrate data	
Unauthorized access to device	Interface Access Control Documentation
Unauthorized remote commands	Product Configuration Education and Awareness
Failure to recognize compromised state	Cybersecurity state awareness

4 Labeling Considerations

From a consumer perspective, 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 also is intended to 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 at the point of purchase 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. This section provides an overview of different approaches to labeling, the NIST proposed approach for an IoT label, considerations for how the label might be provided to a consumer, how to mitigate potential issues with the proposed approach, and consumer education considerations.

This document does not discuss specific label design elements, such as the use of icons, text, colors, or typography. However, when a label is eventually designed, **there should be an assessment of the usability of the label design as well as the usability of consumer education material via rigorous**

consumer testing. Consumer testing prior to program implementation is valuable, but initial perceptions and expressions of intent to purchase may differ from actual consumer behavior. **Therefore, periodic testing after program implementation is essential and can include market studies to assess the impact on consumer purchase decisions and the growth of brand recognition over time.** Additional context on NIST's methodology for formulating the labeling considerations, additional information about the labeling considerations, and a discussion of usability and testing considerations can be found in the Appendix B.

4.1 Proposed 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.

All labeling approaches have their strengths and weaknesses. Taking those into account within the anticipated context of the IoT security label, **NIST proposes that a single *binary label* is likely most appropriate**. **NIST also is proposing coupling the binary label with a *layered approach*** in which a short URL (as included in Singapore's cybersecurity label [SINGAPORE]) or scannable code (e.g., a QR code) on the binary label leads consumers to additional details online.

4.2 Label Presentation

Label presentation – how and where a label is presented to consumers – is another important consideration. **Labels should be available to consumers at the time and place of purchase (in-store or online) as well as after purchase.** Therefore, an IoT product cybersecurity label should be flexible in supporting both physical and digital formats as appropriate.

4.3 Consumer Education

As a complement to the labeling approach, binary labels should be accompanied by a robust consumer[5] education[6] campaign. A robust consumer education program should be developed to increase label recognition and to provide transparency to consumers about important aspects of the labeling program. *Who* provides this information (e.g., labeling program administrator, IoT product developers) will depend on the final construct of the labeling program. **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, addressing potential misinterpretations (e.g., false sense of security or view that labeled products are completely secure while unlabeled products are not secure)
- Product criteria – what cybersecurity properties are included in the baseline and why and how these were selected

[5] Note that although this section describes education materials for consumers, education for developers /manufacturers and retailers is also of great importance.

[6] 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.

- General information about conformity assessment – how cybersecurity properties are evaluated
- Declaration of conformity – the product's specific declaration of conformity against 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 non-connected functionality
- Consumer expectations – how consumers' actions (or inactions) can impact the cybersecurity of a product

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 for those who desire it.

5 Conformity Assessment Considerations

Conformity assessment is demonstration that specified requirements are fulfilled. There are several conformity assessment approaches that can be used depending on the specified requirements to be applied, the risk of nonconformity, and the overall objectives for conducting conformity assessment.

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 3 of this document);
- identifies the methodology(ies) 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).

The conformity assessment scheme defines how conformity assessment activities, roles, and output are structured and managed. The scheme owner determines that 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, **no single conformity assessment approach is appropriate.** 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. As a result, this document does not propose a particular set of conformity assessment requirements related to the baseline IoT product criteria.

Rather, NIST suggests that a consumer IoT labeling scheme owner is necessary to tailor the 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. A consumer IoT cybersecurity labeling scheme owner also reduces the potential for consumer confusion that could result from different criteria and/or conformity assessment approaches for similar product types or use cases that all receive the same or similar labels.

Existing IoT product labeling schemes utilize several approaches to demonstrate that consumer IoT devices conform to defined 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 of the consumer IoT device based on defined criteria.
- Third-party certification of the consumer IoT device.

6 Conclusion

NIST anticipates that once finalized, the guidelines proposed here will be used by one or more organizations to deploy a consumer IoT cybersecurity labeling program or "scheme" in the United States. Ideally, that scheme also would attract interest in other areas of the world, building on existing mechanisms for interoperability and mutual recognition.

Appendix A: Glossary of Terms from Baseline Product Criteria

The following terms used in the technical criteria are defined here for clarity:

1. IoT Product
    - An IoT device and any other product components *necessary* to using the IoT device.
    - Unless justified, all criteria apply to the entire IoT product.
2. 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.
    - Unless justified, all criteria apply to each IoT product component.
        i. For example, a common justification for a criterion not being partially or entirely met by the IoT component itself is that the criterion is met by the product component host.
3. 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. [8259A].
    - Authorized entities can vary for specific features and data and should be determined during development – or a mechanism is needed for the customer to grant authorization.

- Authorization should be paired with authentication (See Access Control).

4. IoT product developer
    - The IoT product developer is the entity that creates an assembled final IoT product.
    - Some 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.
5. 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.
6. Information Relevant to Cybersecurity
    - Information describing use of, assumptions, risks, vulnerabilities, assessments, and/or mitigations related to the IoT product, its components, and data.
7. 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.

Appendix B: Additional Information and Considerations

The following frequently asked questions provide additional context to NIST's approach to consumer IoT product cybersecurity labeling called for under the May 12, 2021, Executive Order.

Background

1. Which parts of Executive Order (EO) 14028 does this white paper respond to?

This NIST white paper addresses three aspects of a consumer Internet of Things (IoT) cybersecurity labeling program, as tasked in EO 14028. Provisions addressed are:

> (s) The Secretary of Commerce acting through the Director of NIST, in coordination with representatives of other agencies as the Director of NIST deems appropriate, shall initiate pilot programs informed by existing consumer product labeling programs to educate the public on the security capabilities of Internet-of-Things (IoT) devices and software development practices, and shall consider ways to incentivize manufacturers and developers to participate in these programs.
>
> (t) Within 270 days of the date of this order, the Secretary of Commerce acting through the Director of NIST, in coordination with the Chair of the Federal Trade Commission (FTC) and representatives of other agencies as the Director of NIST deems appropriate, shall 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. The Director of NIST shall

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.

2. What did NIST hear at the September workshop related to the consumer IoT label program?

NIST has solicited information and presented ideas for cybersecurity labeling for IoT products, primarily at the September 14-15 "Workshop on Cybersecurity Labeling Programs for Consumers: Internet of Things (IoT) Devices and Software" and by publishing a white paper, "DRAFT Baseline Security Criteria for Consumer IoT Devices." NIST received extensive feedback during the workshop and in comments on the white paper. Key themes emerged:

Feedback on Technical Criteria

1. Cybersecurity challenges of IoT product components vary and need careful integration into a full product approach. Because IoT product components have different sources, maturity and risks, there are challenges in defining criteria across all components. Some components (e.g., cloud) may have a more extensive history of cybersecurity certification than others. Supply chain transparency and pre-existing cybersecurity certifications of product components can be useful starting points for addressing these challenges.

2. International fragmentation remains a concern for IoT product developers/manufacturers. IoT products and product components are sourced and distributed internationally. Multiple cybersecurity approaches need to be taken into account when establishing a solid international baseline for the cybersecurity of consumer IoT products.

3. The relationship of the cybersecurity criteria to privacy considerations creates concerns. Protecting data from unauthorized disclosure remains a critical motivation for cybersecurity efforts and several comments reflected this nexus of concerns.

4. Not all devices have the resources to implement all cybersecurity capabilities. The range of devices including those with very limited resources and life expectancy means that some devices will be inherently unable to meet a cybersecurity baseline.

5. Many commenters provided specific feedback on individual criteria for clarify and/or improved cybersecurity outcomes.

Feedback on Label

1. Conveying complex cybersecurity information to a diverse range of consumers will be challenging. Since most IoT consumers lack cybersecurity expertise, there was concern that consumers will not be able to understand the significance of the label or technical criteria behind the label.

2. Some commenters stressed that different IoT products and contexts of use may have different risk levels. However, it would be unrealistic to expect consumers to know what is appropriate for their own use or to require them to seek out and evaluate additional information about risk levels in the midst of a product purchase.

3. There were concerns related to how to convey the scope and meaning of a label to consumers. Many commenters were concerned that a label may create a false sense of security about the product or, in the case of a voluntary labeling scenarios, that consumers may mistakenly think that labeled products are more secure than unlabeled products. There was consensus that a robust consumer education program should accompany the label in order to facilitate consumer understanding and build trust in the label.

4. Usability of the label and accompanying consumer education materials are key. The label and education materials should be accessible to a diverse range of consumers with differing abilities who come from a variety of cultural, educational, generational, and technical backgrounds. Robust consumer testing to assess usability and impact of the label on consumers' purchase decisions is critical to the label's success.

5. A label should be flexible in order to reflect changing security and label status. Many commenters recommended the use of digital labels (e-labels) that could be easily updated to reflect product security changes. Consumers also need to be aware of security and functionality implications when products are no longer supported by the developer.

6. Retailers and third-party service providers will have a role in educating consumers about the label. As the first point of contact for consumers, in-store and online retailers will be important partners in exposing consumers to the IoT label, promoting labeled products, and providing initial explanations of what the label means. This would help to meet the need to raise consumer awareness through education-related efforts.

Feedback on Assessment

1. Concerns about exacerbating market fragmentation – There are several approaches to defining cybersecurity requirements for specific jurisdictions and markets. These approaches create a patchwork of requirements and labeling approaches. Since products are sold internationally, market fragmentation can become a significant issue to IoT product developers.
2. Need for reciprocity in assessments – There was encouragement for reciprocity in assessment across jurisdictions. For example, if an IoT product has been assessed as meeting a cybersecurity criterion that assessment should be valid when documenting adherence to that same cybersecurity criterion in different jurisdictions.
3. Challenge of self-assessment vs. third party assessment – IoT cybersecurity criteria can be difficult for third parties to assess. Cybersecurity criteria that have to do with process or actions of the IoT product developer can be especially problematic for third party assessment. Self-assessment has a role in cybersecurity conformance assessment.

3. How are tiers being considered?

While considerations for tiers regarding cybersecurity capabilities and assessment were part of the initial definition of this effort, tiers are not part of the current draft recommendations. While some existing IoT cybersecurity labeling approaches use differentiated tiers, there is no single approach to defining cybersecurity tiers. 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 testing tools (e.g., penetration testing) were used in assessing the product
- Independent testing beyond self-certification was used in assessing the product
- Evaluation of the IoT product developer has taken place

In their connection to networks, IoT products have a common need for baseline cybersecurity. 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.

4. **How has NIST organized the three parts of the labeling program and how they have been scoped, developed, or updated?**

- Baseline Product Criteria
  - Initial product label should focus on a baseline or minimum set of cybersecurity outcomes and allow the market to identify whether there are classes of devices that require a variation of this initial set.
  - The criteria should encompass the IoT device and all components of the IoT product.
  - The criteria proposed build on the previously developed NIST core baseline of device cybersecurity capabilities [NISTIR 8259A] and core baseline of non-technical supporting capabilities [NISTIR 8259B] as an initial starting point.
  - The baseline criteria have a demonstrated utility and relationship to past cybersecurity incidents that impacted national interests, customers and developers alike.
  - The criteria provide an outcome-oriented approach that describes the device's cybersecurity (i.e., the cybersecurity criteria are described in terms of *what* needs to be achieved rather than *how* it is to be achieved), enabling broad usage across the consumer IoT space.
- Labeling Recommendations
  - The background of the intended audience – with potentially very limited cybersecurity expertise – must be considered.
  - A binary primary label easily available at the time of purchase (e.g., physical label on packaging) with a layer of additional information available online is proposed as the best way to address this consideration.
- Conformity Assessment
  - An outcome-oriented approach influences the choice of conformity approach(es) for a labeling scheme.
  - A consumer IoT labeling scheme owner will need to elaborate the assessment requirements for specific classes of IoT consumer products and recognize that no one size fits all IoT consumer products.

Proposed Baseline Product Criteria

5. Why did NIST take a product-focused approach to the baseline criteria?

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 directly with the IoT device), and
- 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 attack vectors that impact the IoT device, customer, and others (e.g., via attacks on systems or the Internet at large). Since these auxiliary components can create new or unique risks to the IoT product, the entire IoT product, including auxiliary components, must be securable.

6. What is NIST's motivation for the outcome-based approach to the baseline product criteria?

Considering the heterogeneity of consumer IoT products, components, use cases, risks, and mitigations, to best guide the development of the labeling scheme, NIST proposes to focus on an outcome-oriented approach to defining the product criteria. This means that the criteria outlined in Section 3.2 are not specific as to how they would be achieved. Rather, they are stated in a way that documentation such as standards or conformity assessment approaches can demonstrate support for the outcomes. This approach offers multiple benefits:

- Flexibility in meeting the criteria to support different approaches to cybersecurity, 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 goals reflect those changes rather than specifying current solutions. This allows solutions and mitigations to be upgraded and changed over time without significant changes in the product criteria for labeling.
- Allows for a vibrant IoT product conformity and labeling landscape because the outcome-based criteria can be mapped to existing conformity assessment approaches. They also can be used in the final implementation of new, and potentially broader, labeling schemes.
- Outcomes speak more 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 this approach allows for the flexibility required by a diverse marketplace of IoT products, the role of the scheme owner will be critical to ensure that supporting evidence meets the expected outcomes.

7. How would the proposed baseline product criteria be applied to an IoT product and its components?

Criteria would apply to every IoT product, but some components may not be able or need to support all criteria. That might be the case due to product risk considerations or IoT devices may be constrained, companion software apps may have limited access and functionality, or backends may be highly distributed – with many cybersecurity tasks delegated via contracts and supply chain. In these and all complex IoT product use cases care must be taken to properly and adequately assess:

- 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

NIST offers the following general, broad guidelines for consideration of each technical product criteria:

Product Identification: Likely necessary. May be omitted for some IoT product components if product component identities are not generated, managed, or used by the IoT product. Some IoT product components may not need to inventory other components due to implementation or deployment considerations – for example, short lifespan of the IoT device(s).

Product Configuration: May not be needed if configuration by the customer of IoT product features offers no cybersecurity benefits. Configuration of some kinds of components (e.g., backends) may not be necessary if cybersecurity management of the component is not being done by the customer.

Data Protection: Will likely be necessary on all components either in implementation (e.g., use of cryptography) or product/component design (e.g., initial data sent as analog signal).

Interface Access Controls: Always necessary on all components. All network interfaces (which will be most common) should be properly protected by best practice for the interface technology/protocol. Other kinds of interfaces (e.g., GUIs) should follow appropriate best practices to be properly protected. All interfaces that an individual could use to access the IoT product or its components must support adequate authentication to verify the individuals' identities and properly authorize their actions.

Software Update: Likely necessary for most IoT product components in some form. May be omitted if software is never intended to be updated due to implementation or deployment considerations (e.g., short lifespan of IoT device(s)). Software update of some kinds of components (e.g., backends) may not need to be directly assessed if cybersecurity management of the component is not being done by the customer. Decisions about the need for such updates should be part of the review of non-technical capabilities criteria

performed in support of Documentation verifying secure development and product component testing.

Cybersecurity State Awareness: Will be necessary for all IoT products and should cover all IoT product components since vulnerabilities and threats can arise from any component. Information captured does not need to be available to the customer, but should be held for use by an appropriate party (e.g., the IoT product developer, an auditor/investigator) for a cybersecurity purpose (e.g., to develop a vulnerability patch, research an incident).

Documentation: Will always be necessary, but specific information may not always be meaningful to all IoT products.

Information and Query Reception: Will always be necessary given the nature of the consumer marketplace and the need for proactive support of cybersecurity by IoT product developers.

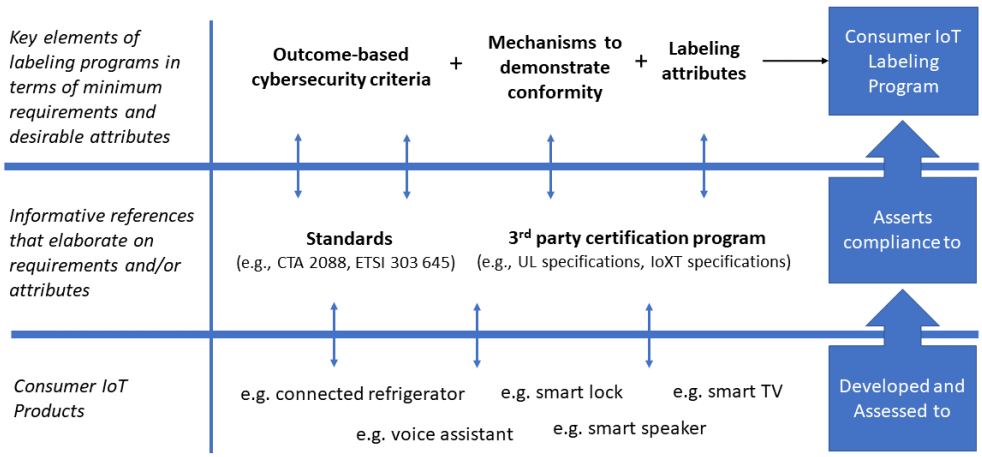
Information Dissemination: Will always be necessary given the nature of the consumer marketplace and the need for proactive support of cybersecurity by IoT product developers.

Education and Awareness: Will always be necessary, but specific information may not always be meaningful to all IoT products.

8. How can the baseline product criteria be connected to requirements for a labeling program?

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.

NIST proposes an approach focused on developing the key elements and desired outcomes of a cybersecurity label. These would establish the foundation that could enable a marketplace of standards, programs, and schemes to evolve that meet the executive order's goals. This approach allows for a diverse set of technical implementations to be identified by the scheme owner while enabling innovation over time.



NIST has identified three key elements that could provide the foundation for an approach to a cybersecurity label for consumer IoT devices:

- What cybersecurity capabilities the product must demonstrate (Product Criteria)
- How the information is provided (Labeling Recommendations)
- How there can be confidence in the label (Conformity Assessment)

These three elements combine to form a labeling approach that provides information to consumers with appropriate assurance.

Labeling Considerations

9. How did NIST determine the labeling recommendations?

In formulating consumer labeling and education considerations, NIST synthesized information related to labels and labeling programs from government, academia, industry, and non-profit sources. This included but was not limited to position papers and input obtained during the NIST Workshop on Cybersecurity Labeling Program for Consumers on September 14-15, 2021, as well as comments on draft criteria issued on August 31, 2021.

When considering sources, NIST assigned greater weight to experiences and lessons learned from real-world, market-tested labeling programs, including those administered by the Federal Trade Commission (FTC) and the Environment Protection Agency (EPA) Energy Star program, which is generally regarded as one of the most successful and recognizable government-administered programs.

Prior research findings on labels in both security and non-security fields were also considered, with more weight attributed to those studies that gauge actual consumer behavior in the marketplace over those measuring self-reported intent, which may be subject to social acceptability bias.

NIST further considered how the cybersecurity context may differ from other common label contexts (e.g., food or energy), such as the unclear return on investment for cybersecurity and cybersecurity concepts typically being poorly understood and not easily relatable among the general public [STANTON][NCSA].

Information and questions provided by other private and non-profit groups also provided important insights into potential consumer-related pitfalls and considerations when implementing cybersecurity labels.

10. What are the different types of consumer-oriented labels?

Labels are generally categorized into three types: descriptive, graded, and binary. Some variations or combinations of these may be used, especially with a layered approach in which a second layer of label detail can be obtained online.

A descriptive (or informational) label provides facts about properties or features of a product without any grading or evaluation. Information may be displayed in a variety of ways, such as in tabular format or with icons or text. Examples of descriptive labels in practice include Nutrition Facts [FDA] and Lighting Facts [FTC].

A binary label (sometimes called a "seal of approval") is a single label indicating a product has met a baseline standard. Examples include Energy Star [EPA], USDA Organic [USDA], and the government of Finland's cybersecurity label [FINLAND].

A tiered (or graded) label indicates the degree to which a product has satisfied a specific standard, sometimes based on attaining increasing levels of performance against specified criteria. Tiers or grades are often represented by colors (e.g., red-yellow-green), numbers of icons (e.g., stars or security shields), or other appropriate metaphors (e.g., precious metals: gold-silver-bronze). Examples include vehicle safety ratings [NHTSA] UL IoT security rating [UL], the government of Singapore's cybersecurity labeling scheme [SINGAPORE], and the European Union's energy efficiency letter grades [EU].

A layered label approach, while not a type of label per se, involves one of the three types of labels initially presented to the consumer with additional information or more detailed labels offered in supplementary (usually online) material. For example, a first-order product label may contain a reference to a website or a Quick Response (QR) code that takes a consumer to more detailed information online. An example of a layered label is CMU's proposed IoT Security and Privacy Label [CMU].

11. Why is NIST recommending a layered binary label?

NIST is proposing that the IoT label l be based on a declaration of conformity with specific product criteria. This negates the value of a *descriptive label*, which relies on consumer interpretation of what is acceptable [ROTHMAN].

A *tiered label* is not suitable because the proposed product criteria consist of a single, minimum baseline. If tiers are introduced in the future to include further criteria – for example, additional product criteria defined by increasing perceived risk, additional testing tools in product assessment, or independent testing beyond self-certification – the label can then be adjusted.

Binary labels are generally considered more usable and are often preferred by consumers over other alternatives [BLYTHE][JOHNSON]. In an IoT cybersecurity label study, binary cybersecurity labels had a positive effect on purchase intention [JOHNSON]. Moreover, the simplicity of binary labels results in less cognitive burden as compared to descriptive and graded labels [KOENIGSTORFER] since the label does not rely on consumers having to determine which properties or tiers are most appropriate and important for their own context of use [GARG][FELT][EMAMI-NAEINI-2]. This simplicity is especially needed within the cybersecurity context given the diversity of IoT consumers many lack expertise in cybersecurity risks, mitigations, and consequences. Overall, binary labels are more effective in those situations – such as the IoT purchase context – in which consumers may lack the time, expertise, or desire to be presented with more information [HODGKINS].

Layered labels can help with consumer education about the labeling effort, provide a means to access the product's declaration of conformity, and enable comparison to other labeling schemes (e.g., those used in other countries). Layers have the advantage of potentially satisfying the information needs and wants of a wide range of cybersecurity expert and non-expert consumers, some of whom research has revealed want to learn more about what is behind cybersecurity labels [EMAMI-NAEINI-1][JOHNSON]. Those who do not care to know more need not be exposed to the details, while those who desire more information can access another layer of information. While access to a second layer should be quick and easy, it is unclear how

willing consumers may be to scan a QR code or visit a website to obtain additional information, so consumer testing in this regard will be essential.

12. Are there additional considerations related to label presentation?

Physical labels on IoT product packaging should follow applicable labeling standards and be located in a conspicuous, but not intrusive, place [STIFEL][JOHNSON]. The date or year of when the product received the label should also be included.

Digital labels (e-labels) (e.g., as described in the ISO/IEC electronic labelling standard [ISO22603]) should be available for all products for several reasons.

- These labels can serve as an additional layer of detail for physical labels when utilizing a layered approach.
- Digital labels also provide a means for consumers to view current label status after purchase or after transfer of product ownership.
- E-labels allow for labeling to be dynamic, reflecting changes in the product lifecycle or cybersecurity status due to changing risks [STIFEL].
- Digital labels with a machine-readable component can be used by security vendors, tools, auditors, and service providers to automatically assess the vulnerability of IoT products and prompt consumers to remediate issues.

The presentation and framing of the labels in the marketplace should also be carefully considered. For example, in one research study, displaying products in order from highest to lowest privacy rating encouraged consumers to purchase more highly-rated products, even when those products cost more [GOPAVARAM]. Retailers should be engaged as active partners in label delivery.

13. Why is it important to include consumer education in any labeling program?

The EO specifies that the labeling program must address consumer awareness and education, reflecting the complexities of cybersecurity challenges for consumers when considering purchases of products. Labels are intended to help address these complexities, but awareness and education efforts will be vital elements of an effective labeling program.

There are potential weaknesses of any labeling approach with respect to consumer perceptions. NIST recognizes that in a voluntary cybersecurity labeling scenario, binary labels may lead to dichotomous thinking in which a product with a label is considered "good" while products without a label are considered "bad" [JOHNSON][KLEEF][ANDREWS]. In reality, the presence or absence of a voluntary label would not necessarily indicate better cybersecurity attributes or increased risk. There is also a concern about potential "halo" effects – the tendency for creating a positive impression of a product based on the fact it has a label [ANDREWS]. In the cybersecurity label context, a halo effect would be a false sense of security. However, recent studies related to IoT cybersecurity labels have shown that consumers generally understand that labeled products are not 100% secure, with the halo effect only manifested in a small minority of consumers [JOHNSON][HARRIS INTERACTIVE].

To counter the potential of dichotomous thinking or halo effects, binary labels should be accompanied by a robust consumer education campaign (see Consumer Education below). This

education campaign is also necessary to build brand recognition since binary labels (especially for new or lesser-known labels) may fail to garner consumer attention [KOENIGSTORFER], and the effectiveness of binary labels is highly correlated with familiarity [GARG].

14. What are some additional considerations for consumer education?

Most information (with the exception of detailed technical information, such as a declaration of conformity) should be accessible to a wide range of consumers and be presented in language that is understandable to non-experts, typically written at an 8th grade reading level. Translations of education materials into common languages spoken in the U.S. should be provided to support the substantial number of consumers who are not proficient in English, including those both in the U.S. and abroad. Given that many consumers may not fully appreciate cybersecurity threats and vulnerabilities – and their IoT product's related risks and susceptibility – the application of risk communication principles can be especially helpful for establishing the importance and relevance of the label. Tying cybersecurity to non-cybersecurity benefits (e.g., availability, reliability) may be valuable in establishing relevance.

To facilitate brand recognition among a demographically diverse population, ideally a public education campaign should be launched via a variety of communication channels, including web sites, social media, and news outlets. A study related to IoT cybersecurity labels commissioned by the UK Government identified potential outlets appropriate to various demographic groups [HARRIS INTERACTIVE]. Similar market research for a U.S. population would be informative and should be prioritized.

15. What are some other considerations to ensure the label is appropriate and usable for consumers?

Beyond proposing a suitable label scheme and considerations for consumer education, a specific label design is out of scope for this document since design selection ideally would be based on extensive consumer testing. Usability and consumer testing are important considerations for a consumer IoT cybersecurity label.

Usability Considerations

Usability is "the extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use" [ISO9241]. Applying this definition within the context of consumer cybersecurity labels, the "system, product, or service" is the label itself. "Users" are synonymous with IoT consumers. For the cybersecurity labeling effort, the primary goal is for consumers to be informed about IoT product cybersecurity capabilities when making purchase decisions. "Context of use" refers to the conditions under which a label will be used, the characteristics of the consumer, and how the consumer will use the label (label-related tasks).

"Effectiveness, efficiency, and satisfaction" are the foundational components of usability. In addition, usability.gov [USABILITY] references two other factors contributing to efficiency which are relevant: ease of learning and memorability. Table 2 lists usability components along with a brief description of each and potential considerations for consumer cybersecurity labels. The label design should also account for accessibility factors that may significantly impact and overlap with the usability components listed, for example, when used by consumers with disabilities or the aging.

Table 2: Usability components as applied to consumer cybersecurity labels

Usability Component	Description	Consumer Cybersecurity Label Considerations
Effectiveness	**Accuracy and completeness** with which consumers achieve specified goals	Consumers should be able to accurately interpret the label's meaning and successfully compare two or more products to determine which has met a baseline level of cybersecurity using relevant standards and criteria. Elements of the label – e.g., symbols, icons, text, or colors – should be commonly understood by most consumers in the U.S. and potentially beyond).
Efficiency	**Resources used** in relation to the results achieved	Consumers should be able to quickly gain a broad sense of the product's cybersecurity level without being required to seek out additional information. There should be an easy, quick way or ways for the consumer to get more details about the label, the product's security performance, and the labeling program for consumers who may want that option.
	Ease of learning: how fast a consumer who has never seen the label before can accomplish basic tasks	The label should have a minimalistic design and be understandable by those without expertise in cybersecurity or information technology. Since consumers are diverse, there may be those who wish to seek out additional details about the criteria behind the label. Documentation should be described in plain language suitable for most consumers. Those consumers who want more technical detail can be referred to a technical criteria reference.
	Memorability: after being exposed to/using the label, whether a consumer can remember enough to use it effectively in the future	The label should be standardized to facilitate eventual widespread recognition and allow consumers to make uniform comparisons across similar products.
Satisfaction	**Extent** to which the consumer's physical, cognitive, and emotional responses that result from the use of the label meet the consumer's needs and expectations	Consumers should perceive the labels as value-added, understandable, and useful in their product purchase decisions. Consumers should also perceive the label as aesthetically/visually appropriate.

Consumer Testing

To determine a label's appropriateness, selected label designs and consumer education materials should undergo rigorous consumer testing prior to launching a labeling program. Usability testing evaluates the components outlined in Table 2. Those testing methods may vary.

For example, in the early design phase, a "within subjects" usability test, in which people are shown more than one possible design, could determine preference among multiple designs.

After the choices of possible designs are narrowed down, candidate designs may be compared and evaluated in a "between-subjects" usability test in which each participant sees only one label design, performs a series of tasks (like providing an interpretation of the label or comparing products), and answers subjective satisfaction questions after the tasks. Findings regarding potential consumer misconceptions or preferences can be incorporated into a revised design or targeted for consumer education materials. Consumer education materials should also be subject to consumer testing to ensure their usability.

Including a demographically diverse, U.S. census-representative sample of consumers of varying disabilities and abilities in the testing is critical for ensuring the label is broadly understandable and testing results are not biased. The sample size should be large enough for sufficient statistical power when analyzing test results.

There is also value in studying – before a program is launched – the potential impact of the label on consumers' actual purchase decisions to gauge whether a labeling program actually achieves the EO's stated goals. For example, because certain psychological biases (e.g., halo effect) may affect consumers' decision making, a deeper understanding of consumers' perceptions of the labels, the potential impact of biases on purchase decisions, and possible strategies for encouraging consumers to select more secure products will be critical to the success of a labeling program. In addition, pre-launch consumer testing should begin to gauge the level of trust consumers may have in the labels, including perceived credibility of the technical criteria, program administrator, and conformity assessment method.

References

[ANDREWS] Andrews JC, Burton S, Kees, J (2011) Is simpler always better? Consumer evaluations of front-of-package nutrition symbols. *Journal of Public Policy & Marketing* 30(2):175–190.

[BLYTHE] Blythe JM, Johnson SD (2018) Rapid evidence assessment on labelling schemes and implications for consumer IoT security. *UK Department for Digital, Culture, Media & Sport Policy Paper* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/949614/Rapid_evidence_assessment_IoT_security_oct_2018_V2.pdf

[CMU] Carnegie Mellon University (2021) *IoT Security and Privacy Label.* Available at https://iotsecurityprivacy.org/

[EMAMI-NAEINI-1] Emami-Naeini P, Dixon H, Agarwal Y, Cranor LF (2019) Exploring how privacy and security factor into IoT device purchase behavior. *CHI Conference on Human Factors in Computing Systems* (ACM, Glasgow, UK) , pp 1-12.

[EMAMI-NAEINI-2] Emami-Naeini P, Agarwal Y, Cranor LF, Hibshi H (2020) Ask the experts: What should be on an IoT privacy and security label? *IEEE Symposium on Security and Privacy* (IEEE, Oakland, CA) pp. 447-464.

[EPA] Environmental Protection Agency (2021) *Energy Star Label*. Available at https://www.energystar.gov/

[EU] European Commission (2021) *About the energy label and ecodesign*. Available at https://ec.europa.eu/info/energy-climate-change-environment/standards-tools-and-labels/products-labelling-rules-and-requirements/energy-label-and-ecodesign/about_en

[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

[FELT] Felt AP, Ha E, Egelman S, Haney A, Chin E, Wagner, D (2012) Android Permissions: User Attention, Comprehension, and Behavior. *Symposium on Usable Privacy and* Security (ACM, New York, NY) pp 3:1–3:14.

[FINLAND] Finnish Transport and Communications Agency (2021) *Finnish Cybersecurity Label.* Available at https://tietoturvamerkki.fi/en/

[FDA] U.S. Food and Drug Administration (2020) *The New Nutrition Facts Label*. Available at https://www.fda.gov/food/nutrition-education-resources-materials/new-nutrition-facts-label

[FTC] Federal Trade Commission (2017) *The FTC "Lighting Facts" Label: Questions and Answers for Manufacturers*. Available at https://www.ftc.gov/tips-advice/business-center/guidance/ftc-lighting-facts-label-questions-answers-manufacturers

[GARG] Garg, V (2021) A Lemon by Any Other Label. *International Conference on Information Systems Security and Privacy* (SCITEPRESS, Vienna, Austria) pp 558-565.

[GOODIN] Goodin, D (2021) Thinking about selling your Echo Dot—or any IoT device? Read this first. *Ars Technica*. Available at: https://arstechnica.com/gadgets/2021/07/passwords-in-amazon-echo-dots-live-on-even-after-you-factory-reset-them/

[GOPAVARAM] Gopavaram, S, Dev, J, Das, S, Camp, LJ (2021) IoT Marketplace: Willingness-To-Pay vs. Willingness-To-Accept. *Annual Workshop on the Economics of Information Security*.

[HARRIS INTERACTIVE] Harris Interactive (2019) Consumer Internet of Things Security Labelling Survey Research Findings. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950429/Harris_Interactive_Consumer_IoT_Security_Labelling_Survey_Report_V2.pdf

[HODGKINS] Hodgkins CE (2016) Communicating healthier food choice – Food composition data, front-of-pack nutrition labelling and health claims. (Doctoral dissertation, University of Surrey, United Kingdom)

[ISO22603] International Organization for Standardization/International Electrotechnical Commission (2021*) ISO/IEC 22603-1:2021 Information technology — Digital representation of product information — Part 1: General requirements* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/73561.html

[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

[JOHNSON] Johnson, SD, Blythe, JM, Manning, M, Wong, GT (2020) The impact of IoT security Labelling on consumer product choice and willingness to pay. *PloS One*, 15(1).

[KLEEF] Kleef E Van, Dagevos H (2015) The Growing Role of Front-of-Pack Nutrition Profile Labeling: A Consumer Perspective on Key Issues and Controversies. *Critical Reviews in Food Science and Nutrition* 55(3):291–303.

[KOENIGSTORFER] Koenigstorfer J, Wą sowicz-Kiryło G, Styśko-Kunkowska M, Groeppel-Klein A (2014) Behavioural effects of directive cues on front-of-package nutrition information: The combination matters! *Public Health Nutrition* 17(9):2115–2121.

[NCSA] National Cybersecurity Alliance (2021) Oh, Behave! The annual cybersecurity attitudes and behaviors report 2021. https://staysafeonline.org/wp-content/uploads/2021/09/Oh-behave-The-Annual-Cybersecurity-Attitudes-and-Behaviors-Report-2021.pdf

[NHTSA] National Highway Traffic Safety Administration (2021) *Ratings*. Available at https://www.nhtsa.gov/ratings

[ROTHMAN] Rothman RL, Housam R, Weiss H, Davis D, Gregory R, Gebretsadik T, Shintani A, Elasy TA (2006). Patient understanding of food labels: the role of literacy and numeracy. *American Journal of Preventive Medicine* 31(5):391–398.

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

[STANTON] Stanton B, Theofanos MF, Prettyman SS, Furman S (2016) Security fatigue. *IT Professional*, 18(5):26-32.

[STIFEL] Stifel M, Gilbert D, Peterson M (2019) Security Shield: A label to support sustainable cybersecurity. *Public Knowledge*. https://www.publicknowledge.org/blog/security-shield-a-label-to-educate-consumers-and-promote-sustainable-cybersecurity/

[UL] UL (2021) *IoT Security Rating*. Available at https://ims.ul.com/IoT-security-rating

[USABILITY] U.S. General Services Administration (2021) *Usability.gov*. Available at https://www.usability.gov/

[USDA] U.S. Department of Agriculture (2021) *USDA Organic*. Available at https://www.usda.gov/topics/organic