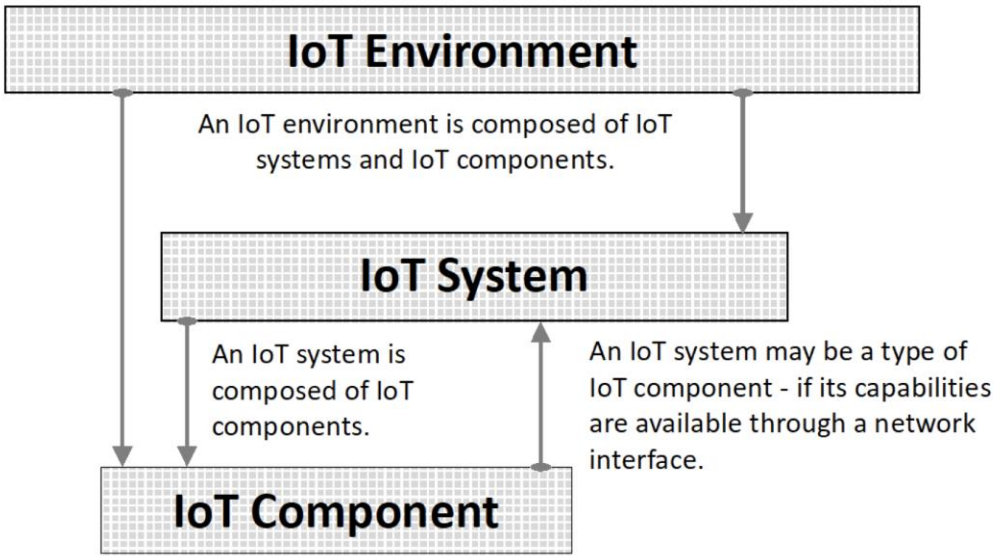
Identifying Standards and Guidance for a Consumer IoT Product Development Handbook

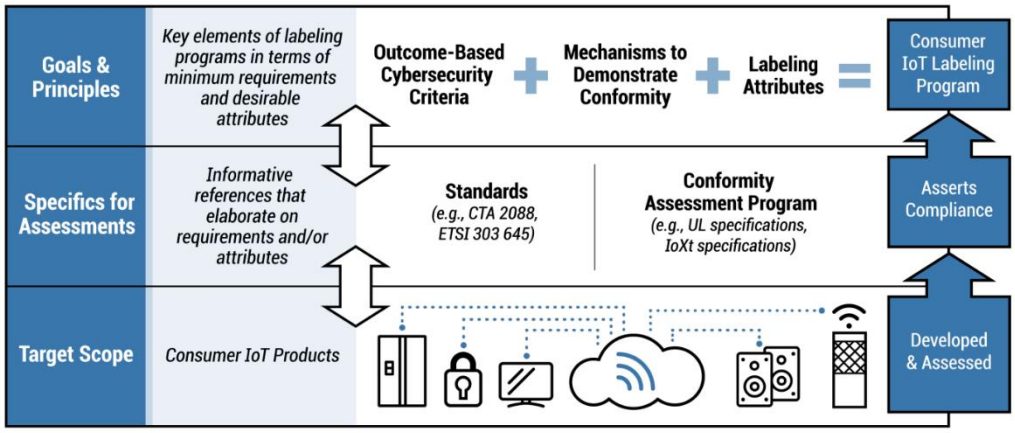
In the response to EO 14028 and later in *Profile of the IoT Core Baseline for Consumer IoT Products,* NISTIR 8425, NIST defines the IoT product as "an IoT device or IoT devices and any additional product components that are necessary to use the IoT device beyond basic operational features." This definition built upon NIST's prior work in *IoT Device Cybersecurity Capability Core Baseline*, NISTIR 8259A, and *IoT Non-Technical Supporting Capability Core Baseline*, NISTIR 8259B. Cybersecurity of IoT devices, though critical, is incomplete if cybersecurity of other IoT product components is not considered as well since the IoT device and other IoT product components will be a system. Significant risk can be introduced by vulnerable IoT product components that are used by even a hardened IoT device since these additional IoT product components will likely have access to the IoT device, the data it sends, or the data it receives. Therefore, the cybersecurity technical and non-technical outcomes defined in the NISTIR 8425 consumer profile apply to IoT products and not just IoT devices. This essay is intended as an initial discussion of possible standards that may be related to the NISTIR 8425 outcomes that address all IoT product components.

The NISTIR 8425 outcomes are aimed at the IoT product as an IoT system that will be deployed and connected in the customer's IoT environment. The figure below from *Internet of Things (IoT) Component Capability Model for Research Testbed*, NISTIR 8316 shows how IoT components, systems, and environments relate.



In the context of this essay, *outcomes* are guidelines that describe **what** is expected and can be applied to different use cases and contexts. Cybersecurity outcomes are useful to guide product developers as they design and support the product over its lifecycle, but more specific information may be needed to define how to implement IoT products or product components so that they meet an outcome. *Requirements* define **how** a component can meet an outcome for a specific use case, context,

technology, IoT product component type, etc. The figure below shows how standards can serve as the basis for understanding achievement of cybersecurity outcomes.



NIST has identified examples of standards and guidance that may be applicable to the NISTIR 8425 cybersecurity outcomes as they pertain to IoT products, including IoT devices but particularly other IoT product components, to begin understanding the feasibility of applying multiple standards of different focus to reflect the total scope of the IoT product. This essay presents a summary of the standards NIST has found thus far. Beyond identifying their association with the cybersecurity outcomes and related concepts, NIST has not further evaluated the standards identified in this essay relative to the outcomes (e.g., whether standards satisfy outcomes). Discussion of these standards is meant as a starting point to identify any applicable standards for achieving the outcomes across different IoT product components. These standards may be helpful to IoT product developers as they build securable products, but further community feedback and technical analysis is necessary as NIST explores these and other related standards. NIST welcomes additional suggestions of applicable standards and guidance for the contexts discussed in this essay.

This essay divides the discussion between technical cybersecurity and non-technical cybersecurity, both of which are critical to the cybersecurity of IoT products. Technical cybersecurity is the measures taken in the hardware and software of the IoT product's components to address and reduce risks. Non-technical cybersecurity is the measures an organization takes to support cybersecurity over a product's lifecycle. Technical cybersecurity may be addressed component by component, but non-technical cybersecurity, such as the process organizations use to develop products and maintain the security of products over their lifecycle will likely be best applied to the entire product or even entire portfolios of products, not just one component.

Technical Cybersecurity Considerations

Particular product types may have specific standards that can be used to develop requirements for the technical outcomes. For example, NIST created a profile for consumer-grade routers based on four standards that contained requirements for the router device. Not all product types will have specific standards or guidance, especially considering the wide range of IoT use cases. This means a set of standards for IoT devices in general is needed.

IoT product components other than the IoT device (e.g., companion mobile apps) may vary among product instances, even of the same type of IoT product. For example, one brand of smart light bulb may

use a backend, while another may not. Standards and guidance for a specific technology or product type (e.g., consumer grade routers) may not provide specific requirements for supporting components (e.g., companion mobile apps) even if many requirements for the IoT device are included. This means cybersecurity for IoT product components other than the IoT device (e.g., mobile app, cloud backend) may often rely on general standards not specific to the product type, and so standards to approach these components in general are also applicable.

IoT Devices

Due to the growing prevalence of IoT, standards have begun to appear that address cybersecurity for IoT devices. NIST has identified the following standards that relate to IoT devices:

- ISO/IEC 27402 (Cybersecurity – IoT security and privacy – Device baseline requirements)
- ANSI/CTA-2088-A - Baseline Cybersecurity Standard for Devices and Device Systems
- ETSI 303-645 - Cyber Security for Consumer Internet of Things: Baseline Requirements
- All tiers of Singapore's Cyber Security Agency's Cybersecurity Labeling Scheme

Additional IoT Product Components

IoT product components can consist of software or software and hardware. Requirements related to IoT product components other than the IoT device should be approached with this in mind. For software-based product components (e.g., mobile apps), NIST has identified the following existing standards and guidance:

- NIST's Recommended Criteria for Cybersecurity Labeling of Consumer Software - *This document provides clear, testable claims for software cybersecurity.*
- OWASP's Application Security Verification Standard, Mobile Application Security Testing Guide, and Web Security Testing Guide - *These standards and guidance documents provide extensive requirements for different types of software.*

For product components that have hardware in addition to software (e.g., networking equipment included with IoT devices), ISO 9001 (Quality management systems — Requirements) can augment the software cybersecurity standards/guidance documents to inform requirements for the IoT product component. New hardware usually introduces new interfaces, including digital communication interfaces and protocols. In this case, use of applicable protocol and cybersecurity standards for those interfaces and protocols is recommended.

Platform

IoT product components developed using specific standardized technologies or platforms may have more specific cybersecurity standards/guidance documents that relate to the component and could be used to inform requirements related to the NISTIR 8425 outcomes. For example, the Cloud Security Alliance's Security, Trust, Assurance and Risk (STAR) Program is useful for assessing security of cloud platforms. Platform standards/guidance will augment rather than replace the standards/guidance used to assess the security of the developed software since both the platform and code it hosts must be secure.

Non-Technical Cybersecurity Considerations

Unlike for technical outcomes, where software and hardware cybersecurity approaches can be different and sometimes tuned for different technologies, many technologies do not require specific non-

technical cybersecurity capabilities for customers and users to securely use products. Rather, requirements related to non-technical cybersecurity outcomes would be the same for many digital products and services. Therefore, rather than consider standards related to these outcomes on a component-by-component basis, as in the prior section for technical outcomes, the non-technical outcomes can utilize broadly applicable standards for the IoT product as a whole. This section discusses such standards for each of the four non-technical outcomes defined in NISTIR 8259B: Documentation, Information and Query Reception, Information Dissemination, and Education and Awareness. NIST was able to identify some potential standards for all non-technical outcomes, including most non-technical sub-outcomes. Recommendations of potential standards to fill any gaps or that are related to any sub-outcome are welcome.

Documentation

Documentation brings together many subfields of cybersecurity (e.g., secure development and lifecycle, systems cybersecurity, vulnerability remediation, supply chain risk management), and thus is related to a multitude of standards. That said, many of the standards that inform documentation are established, well-accepted, international voluntary consensus standards that would be recommended for developers of any software or other digital product in any context. Thus, many of the standards and practices therein are related and supportive of each other. The table below lists the Documentation sub-outcomes from NISTIR 8425 and pairs them with the related standards.

Cybersecurity Outcome	**Potential References**
Documentation 1a. Assumptions made during the development process and other expectations related to the IoT product.	ISO 9001 (Quality management systems — Requirements) ISO/IEC TS 19249 (Information technology — Security techniques — Catalogue of architectural and design principles for secure products, systems and applications)
Documentation 1b. All IoT components, including but not limited to the IoT device, that are part of the IoT product.	Software Bill of Materials (SBOM) Hardware Bill of Materials (HBOM) Framework for Supply Chain Risk Management
Documentation 1c. How the baseline product outcomes are met by the IoT product across its product components, including which baseline product outcomes are not met by IoT product components and why (e.g., the capability is not needed based on risk assessment).	*On risk management:* ISO 31000 (Risk management — Guidelines) NIST SP 800-37 Rev. 2 - Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
Documentation 1d. Product design and support considerations related to the IoT product.	ISO/IEC 27036 (Cybersecurity — Supplier relationships) ISO/IEC 27034 (Information technology — Security techniques — Application security) ISO/IEC 5055 (Information technology — Software measurement — Software quality measurement — Automated source code quality measures) NIST Cybersecurity Supply Chain Risk Management (CSCRM)

Cybersecurity Outcome	Potential References
Documentation 1e. Maintenance requirements for the IoT product.	ISO/IEC/IEEE 14764 (Software engineering — Software life cycle processes — Maintenance)
Documentation 1f. The secure system lifecycle policies and processes associated with the IoT product.	ISO/IEC 15288 (Systems and software engineering — System life cycle processes) ISO/IEC 12207 (Systems and software engineering — Software life cycle processes) ISO/IEC 15408 (Information security, cybersecurity and privacy protection — Evaluation criteria for IT security) ISO/IEC 27001 (Information security management systems — Requirements) ISO/IEC 27002 (Information security, cybersecurity and privacy protection — Information security controls) ISO/IEC 27005 (Information security, cybersecurity and privacy protection — Guidance on managing information security risks) NIST Secure Software Development Framework (SSDF) Cybersecurity and Infrastructure Security Agency (CISA)'s Secure by Design
Documentation 1g. The vulnerability management policies and processes associated with the IoT product.	ISO/IEC 29147 (Information technology — Security techniques — Vulnerability disclosure) ISO/IEC 30111 (Information technology — Security techniques — Vulnerability handling processes)

Information and Query Reception

Reception of cybersecurity information is most critically related to vulnerability management, but can also support customers in other ways. Existing standards focus on vulnerability and incident management, as shown in the table below. Even without standards to guide the practice, NIST recommends manufacturers and supporting entities be open to broader forms of interaction with customers and users. Technical support available to customers that guides them through troubleshooting and can answer other questions users may have can bolster secure use of IoT products. The table below shows the vulnerability and incident management standards related to the Information and Query Reception sub-outcomes.

Cybersecurity Outcome	Potential References
Information and Query Reception 1a. 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).	ISO/IEC 29147 (Information technology — Security techniques — Vulnerability disclosure) ISO 10004 (Quality management — Customer satisfaction — Guidelines for monitoring and measuring)
Information and Query Reception 1b. 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/or its components.	ISO 10004 (Quality management — Customer satisfaction — Guidelines for monitoring and measuring) ISO/IEC 27035-1 (Information technology — Information security incident management — Part 1: Principles and process)

Information Dissemination

The Information Dissemination outcome discusses two kinds of support: broadly communicated information and targeted, directly shared information. The table below shows standards related to the

first sub-outcome of Information Dissemination, which discusses the ability to broadly distribute cybersecurity.

Cybersecurity Outcome	Potential References
Information Dissemination 1a. Updated terms of support (e.g., frequency of updates and mechanism(s) of application) and notice of availability and/or application of software updates.	[No standards currently identified]
Information Dissemination 1b. End of term of support or functionality for the IoT product.	ETSI 303-645 (Cyber Security for Consumer Internet of Things: Baseline Requirements): Provision 5.3-13
Information Dissemination 1c. Needed maintenance operations.	ISO/IEC/IEEE 14764 (Software engineering — Software life cycle processes — Maintenance)
Information Dissemination 1d. New IoT device vulnerabilities, associated details, and mitigation actions needed from the customer.	ISO/IEC 29147 (Information technology — Security techniques — Vulnerability disclosure) ISO/IEC 27035-1 (Information technology — Information security incident management — Part 1: Principles and process)
Information Dissemination 1e. 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).	ISO/IEC 29147 (Information technology — Security techniques — Vulnerability disclosure) ISO/IEC 27035-1 (Information technology — Information security incident management — Part 1: Principles and process)

Targeted communications such as those described in Information Dissemination 2 are much more contextual:

> 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., IoT product component manufactures and/or supporting entities, common vulnerability tracking authorities, accreditors and certifiers, third-party support and maintenance organizations) about cybersecurity relevant information.

Thus, this outcomes and its sub-outcomes will generally be guided by standards mapped to other outcomes (e.g., ISO/IEC 29147), and so no specific, additional standards have been currently identified for Information Dissemination's second sub-outcome. Note that profiles for specific technologies or product types may identify additional standards or requirements pertinent to Information Dissemination's second sub-outcome.

Education and Awareness

NISTIR 8425's Education and Awareness outcome has one sub-outcome: 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. This sub-outcome is further defined by five minimum criteria:

1. The presence and use of IoT product cybersecurity capabilities.
2. 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.

3. How an IoT product and its product components can be securely reprovisioned or disposed of.
4. 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.
5. 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).

ISO/IEC/IEEE 26512 (Systems and software engineering - Requirements for acquirers and suppliers of information for users) and/or ISO/IEC/IEEE 26514 (Systems and software engineering — Design and development of information for users) may inform requirements related to the Education and Awareness outcome.

Call for Comments

NIST welcomes feedback on these ideas as we work to develop guidance in this critical area. Your feedback in any capacity or on any topic discussed here is welcome. Please consider the following points that NIST seeks specific feedback on:

1. Potential standards discussed throughout this essay that are appropriate to the IoT product components and cybersecurity outcomes they're paired with.
2. Gaps in the coverage by standards of particular IoT product components or cybersecurity outcomes and possible solutions for the gap(s).
3. Additional standards that can be used to inform requirements for IoT products, IoT product components, and cybersecurity outcomes.
4. Feasibility of applying multiple standards of different focus related to cybersecurity to reflect the total scope of the IoT product.

NIST will present and discuss these questions and the material in this essay at an open-forum discussion on December 7th, 2023 hosted at the National Cybersecurity Center of Excellence with a Live Virtual Attendance option available due to limited space (Register here). Written comments can be sent to iotsecurity@nist.gov by December 21st, 2023.