DRAFT Baseline Security Criteria for Consumer IoT Devices
August 31, 2021
Comments Due October 17, 2021 to labeling-eo@nist.gov

Introduction

Executive Order (EO) 14028, "Improving the Nation's Cybersecurity," tasks the National Institute of Standards and Technology (NIST), in coordination with the Federal Trade Commission (FTC) and other agencies, to initiate pilot programs 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. NIST also is to consider ways to incentivize manufacturers and developers to participate in these programs. This white paper proposes baseline security criteria for consumer IoT devices. This is one of three dimensions of a consumer Internet of Things (IoT) cybersecurity labeling program that would be responsive to Sections 4 (s) and (t) of the EO. The other dimensions are criteria for conformity assessment and the label. In addition to the feedback sought on this white paper, NIST will also consult with stakeholders on those additional considerations.

NIST will identify key elements of labeling programs in terms of minimum requirements and desirable attributes. Rather than establishing its own programs, NIST will specify desired outcomes, allowing providers and customers to choose the best solutions for their devices and environments. One size may not fit all, and multiple solutions might be offered by label providers.

Background and Methodology

This white paper presents draft baseline security criteria for consumer IoT devices developed using the [NISTIR 8259A] baseline of device cybersecurity capabilities and the [NISTIR 8259B] baseline of non-technical supporting capabilities as an initial starting point. These documents already reflect extensive private and public sector input and NIST's analysis of informative references to determine appropriate core baselines.

The capabilities described in NISTIR 8259A, *IoT Device Cybersecurity Capability Core Baseline* and NISTIR 8259B, *IoT Non-Technical Supporting Capability Core Baseline,* represent criteria that address a broad range of customer needs and goals. These needs and goals are discussed extensively in NISTIR 8259, which documents how cybersecurity considerations can be incorporated into the IoT product development process. These are core baselines and need to be tailored (or profiled) for specific use cases or sectors. This profiling can involve editing the capabilities to address specific concerns as well as extensions or additions to the baseline capabilities and sub-capabilities.

Through a review of the landscape of related informative references from governments, non-profit, and private sector sources, NIST developed a profile of those baselines. In selecting

technical criteria for extending or editing the baseline from this range of sources, NIST applied the following considerations:

1. **Utility for cybersecurity:** Do the technical criteria provide improved security or securability for consumers of IoT devices?

2. **Feasibility of implementation:** Can the technical criteria be reasonably met by consumer IoT devices, their manufacturers and supporting parties (e.g., supply chain partners), and will the resulting IoT product be usable for the customer?

3. **Support for labeling and conformity assessment:** Do the technical criteria meet the needs of the follow-on conformity assessment and labeling criteria?
    a. *For labeling:* Do the technical criteria support the information on or behind the label criteria?
    b. *For conformity:* Are the technical criteria suitable for conformity assessment?

NIST seeks comment on all aspects of cybersecurity labeling technical criteria for IoT devices. Specific areas for consideration include:

- Whether these are appropriate criteria for a broad range of consumer devices
- Whether additional criteria are needed, including criteria that specifically address other components of the product beyond the device
- Whether Tables 1, 2, and 3 have the right level of detail in the discussion of the criteria to ensure consistency in meeting the cybersecurity expectations
- What might be the appropriate definitive text for these criteria be stated to facilitate conformity assessment
- The extent to which consumer IoT devices with very limited capabilities (e.g., microcontroller-based devices) can address the criteria
- The potential for assessment and certification of IoT product components (e.g., cloud backend, hub, mobile app) independent of one another

A Label Representing the Security of the Product

Many IoT consumers will see their purchase of an IoT product and not distinguish the IoT device from other components of the product. One notable extension of the baseline that may be appropriate is consideration of the cybersecurity of the *IoT product* rather than that of only the IoT device. During its landscape review, NIST identified other components considered in the informative references for IoT security such as cloud backends, mobile applications and secure hubs. Understanding the purpose of additional components and the cybersecurity expectations that may need to be supported by each will enable more effective risk consideration and mitigation, resulting in a more securable IoT product for consumers to use.

An IoT product might be defined as including an IoT device and any other product components that are *necessary* to using the IoT device beyond basic operational features (e.g., an

unconnected smart lightbulb may still illuminate in one color, but its smart features cannot be used with other product components unless they are connected).

The scope of an entire IoT product including those discrete product components outside the IoT device has guided the creation of the consumer IoT profile. The consumer IoT profile documenting a draft set of technical criteria for IoT products is in Tables 1, 2 and 3.

- Table 1 criteria will have to be satisfied by the IoT product and will be allocated among IoT product components depending on the product and component architecture.
- Table 2 criteria are only meaningful at the product level.
- Table 3 provides additional criteria under each respective IoT Product Cybersecurity Capability for consideration that may apply, particularly to IoT products that include multiple components. These are ways that the IoT product components can help each other to achieve the overall cybersecurity goals.

Table 1: IoT Product Cybersecurity Capabilities Developed from NISTIR 8259A Using Informative References

IoT Product Cybersecurity Capability	Potential Criteria
Asset Identification: The IoT product can be uniquely identified and can inventory all of the IoT product's components.	1. A unique logical identifier, possibly generated by the *product component host*. 2. A unique physical identifier at an external or internal location on the device accessible to the consumer. Note: the physical and logical identifiers may represent the same value, but that is not required.
Product Configuration: The configuration of the IoT product can be changed, and such changes can be performed by only authorized individuals and other IoT product components.	1. The ability to change the product component's software configuration settings including disabling unwanted features. 2. The ability to restrict configuration changes to authorized individuals and other IoT product components only. 3. A default setting for the initial configuration which makes the product component secure for expected use cases.[1] Any security features should be enabled by default. 4. The ability for authorized individuals and other IoT product components to restore the product component to the default secure configuration.

[1] This initial configuration will be highly dependent on the IoT device and what it does, but in general will enable all necessary features (e.g., cybersecurity features) while disabling all unnecessary features (especially interfaces) as a means to minimize the attack space and vectors.

IoT Product Cybersecurity Capability	Potential Criteria
Data Protection: The IoT product can protect the data it stores (across all IoT product components) and transmits (both between IoT product components and outside the IoT product) from unauthorized access and modification.	1. The ability to use demonstrably secure cryptography (e.g., modules consistent with FIPS 140-3) for cryptographic algorithms (e.g., encryption with authentication, cryptographic hashes, digital signature validation) to protect the confidentiality and integrity of all the product component's stored (e.g., collected and received data, internal software) and transmitted data. Note: available cryptographic modules maybe dependent on or limited by the *product component host*. 2. The ability to protect the product component's stored data from unauthorized change (e.g., protect against injected code or data manipulation attacks). 3. The ability for authorized persons to render all data on the product component that is not the initial default configuration (see *Device Configuration*) and any initial software included on the device (including updates) inaccessible to anyone, whether previously authorized or not. Note: for components implemented in a shared environment (e.g., auxiliary backend), this may be limited to data and configurations associated with the IoT product customer. 4. The ability for authorized individuals, other IoT product components, and/or systems to delete data at rest from the product component. Note: for components implemented in a shared environment (e.g., auxiliary backend), this may be limited to data associated with the IoT product customer.
Logical Access to Interfaces: The IoT product can restrict logical access to its local and network interfaces, and to the protocols and services used by those interfaces, to only authorized individuals and IoT product components.	1. The ability to logically or physically disable any local and network interfaces that are not necessary for the core functionality of the product component 2. The ability to logically restrict access to each network interface to only authorized persons or devices. 3. The ability of the product component to validate that the input received through its interfaces matches specified definitions of format and content. 4. The ability to authenticate individuals and other IoT product components using appropriate mechanism to technology, risk and use case. Authenticators could be biometrics, passwords, etc. 5. The ability to support secure use of authenticators (e.g., passwords) including: a. if necessary, ability to locally manage authenticators b. ability to ensure a strong, non-default authenticator is used (e.g., not delivering the product with any single default password or enforcing a change to a default password before the product component is deployed for use) Note: some or all of these elements may be supported or managed by the *product component host*.
Software Update: The software of all IoT product components can be updated by authorized individuals and other IoT product components only by using a secure and configurable mechanism, as appropriate for each IoT product component.	1. The ability to update the product component's software through remote (e.g., network download) 2. The ability for the product component to verify and authenticate any update before installing it. 3. The ability to enable or disable notifications about updates. Note: updating of some product components by be dependent on or performed by the *product component host*.

IoT Product Cybersecurity Capability	Potential Criteria
Cybersecurity State Awareness: The IoT product can detect cybersecurity incidents affecting or effected by its components and the data they store and transmit.	1. The ability to log cybersecurity-related state information (e.g., software update installations, failed log in attempts, configuration changes). 2. The ability to restrict access to the state information so only authorized individuals and IoT product components can view it. 3. The ability to prevent any unauthorized edits of state information by any entity. Note: generating, storing, and protecting state information on some product components may be dependent on or performed by the *product component host*.
Product Security: The IoT product can perform other features and functions across some or all of its components to make IoT products minimally securable for the sector.	1. The ability for the device to continue operating (possibly with limited digital functionality) in the case of a network outage or other connectivity disruption. Operational features of the device should continue to function without connectivity (e.g., TVs should be able to continue to display local content, refrigerators should continue to cool inside the cabinet). Note: behavior in the event of an outage may be dictated for some product components by the *product component host*.

Table 2: Non-Technical Supporting Capabilities Developed from NISTIR 8259B Using Informative References

Non-Technical Supporting Capability	Potential Criteria
Documentation: The ability for the manufacturer and/or the manufacturer's supporting entity, to create, gather, and store 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. Document assumptions made during the development process and other expectations related to the IoT product, such as: a. Expected customers and use cases b. 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 doesn't have an off switch on the device), and characteristics c. Network access and requirements (e.g., bandwidth requirements) d. Data created and handled by the IoT product e. Expected data inputs and outputs (including error codes, frequency, type/form, range of acceptable values, etc.) f. Assumed cybersecurity requirements for the IoT product g. Laws and regulations with which the IoT product and related support activities comply h. Expected lifespan, anticipated cybersecurity costs related to the IoT product (e.g., price of maintenance), and term of support 2. Document what other IoT components other than the IoT device (e.g., cloud backend, mobile app, secure hub) are necessary to using the IoT product's functionality beyond basic operational features (e.g., an unconnected smart lightbulb may still illuminate in one color, but its smart features cannot be used with other product components unless they are connected). 3. Document the **IoT product cybersecurity capabilities** that are implemented within the IoT product and its product components and how to configure and use them. 4. Document which IoT product cybersecurity capabilities from this profile are not implemented in the IoT product and its components and why (e.g., lack of need

Non-Technical Supporting Capability	Potential Criteria
	for the capability based on risk assessment). 5. Document product design and support considerations related to the IoT product, such as: a. 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) [2] b. IoT platform[3] used in the development and operation of the IoT product its product components, including related documentation c. Protection of software and hardware elements used to create the IoT product and its product components (e.g., secure boot, hardware root of trust, and secure enclave) d. Consideration of the known risks related to the IoT product and known potential misuses e. Secure software development and supply chain practices used f. Accreditation, certification, and/or evaluation results for cybersecurity-related practices g. The ease of installation and maintenance of the IoT product by a consumer 6. Document maintenance requirements for the IoT product, such as: a. Cybersecurity maintenance expectations and associated instructions or procedures (e.g., vulnerability/patch management plan) b. how the manufacturer identifies authorized supporting parties who can perform maintenance activities. (e.g., authorized repair centers) c. Cybersecurity considerations of the maintenance process (e.g., how does customer data unrelated to the maintenance process remain confidential even from maintainers) 7. Document the secure system lifecycle policies and processes associated with the IoT product, including: a. The steps taken during its development to ensure the IoT product and its product components are free of any known, exploitable vulnerabilities. b. 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. c. Any post end-of-support considerations, such as in the event that a vulnerability is discovered which would significantly impact the security, privacy, or safety of customers who continue to use the IoT product and its product components. 8. Document the vulnerability management policies and processes associated with the IoT product, including the following: a. Methods of receiving reports of vulnerabilities (see Information and Query

[2] While this information would be provided by a Software Bill of Materials (SBOM), what is being discussed here is significantly less elaborate than what is normally meant by an SBOM. More details on SBOM can be found at https://www.ntia.gov/SBOM.

[3] An IoT platform is typically a third-party vendor-provided/hosted SaaS-based tool that is used to support IoT device and endpoint management, connectivity and network management, data management, processing and analysis, application development, cybersecurity, access control, monitoring, event processing, and interfacing/integration. Documentation about such a third party can provide important information about supply chain cybersecurity practices and vulnerabilities to allow for the IoT user to more accurately determine risks related to the use of an IoT platform.

Non-Technical Supporting Capability	Potential Criteria
	Reception below) b. Process of recording reported vulnerabilities c. Policy for responding to reported vulnerabilities, including process of coordinating vulnerability response activities amongst component suppliers and third-party vendors d. Policy for disclosing reported vulnerabilities e. 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, or known insecurities.
Information and Query Reception: The ability for the manufacturer and/or supporting entity to receive information and queries from the customer and others related to cybersecurity of the IoT product and its product components.	1. The ability for the manufacturer and/or supporting entity to identify a point of contact to receive maintenance and vulnerability information (e.g., bug reporting capabilities and bug bounty programs) from their customers and others in the IoT product ecosystem 2. The ability for the manufacturer and/or supporting entity to respond to customer and third-party (e.g., repair technical acting on behalf of the consumer) queries about cybersecurity of the IoT product and its components (e.g., customer support).
Information Dissemination: The ability for the manufacturer and/or supporting entity to broadcast and distribute (e.g., to the customer or others in the IoT product ecosystem) information related to cybersecurity of the IoT product and its product components.	1. The procedures to support the ability for the manufacturer and/or supporting entity to alert the public (i.e., potential customers) and customers of the IoT product directly about cybersecurity relevant information such as: a. update 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 2. The procedures to support the ability for the manufacturer and/or supporting entity to alert appropriate ecosystem entities (e.g., common vulnerability tracking authorities, accreditors and certifiers, third-party support and maintenance organizations) about cybersecurity relevant information such as: 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 consumer 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 manufacturer and/or supporting entity e. Accreditation, certification, and/or evaluation results for the manufacturer and/or supporting entity's cybersecurity-related practices f. A risk assessment report or summary for the manufacturer's business environment risk posture 3. The procedures to support the ability for the manufacturer and/or supporting entity to notify customers of cybersecurity-related events and information related to an IoT product throughout the support lifecycle, such as: a. New IoT device vulnerabilities, associated details, and mitigation actions b. Breach discovery related to an IoT product and its product components used by the customers and explanations of how to make any associated fixes or

Non-Technical Supporting Capability	Potential Criteria
	actions to prevent similar breaches of other products and/or product components.
Education and Awareness: The ability for the manufacturer and/or supporting entity to create awareness of and educate customers and others in the IoT product ecosystem about cybersecurity-related information, considerations, features, etc. of the IoT product and its product components.	1. Educate customers of the IoT product and others in the ecosystem (e.g. authorized repair technicians) about the presence and use of IoT product cybersecurity capabilities. For example, it may be important to educate customers and others about: a. How to change configuration settings and cybersecurity implications of changing settings, if any b. How to configure and use access control functionality (e.g., set and change passwords) c. How software updates are applied and any instructions necessary for the customer on how to use software update functionality d. 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 manufacturer. e. How to manage device data including creation, update and deletion. 2. Educate customers and others about how an IoT product and its product components can be securely reprovisioned or disposed of. 3. Educate customers and others about 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. 4. The product packaging provides information consumers 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).

Table 3: Potential Additional IoT Product Criteria Developed from NISTIR 8259A Using Informative References

IoT Product Cybersecurity Capability	Potential Additional Criteria
Asset Identification: The IoT product can uniquely identify and inventory all of the IoT product's elements/components.	1. The ability to read other product component identifiers. 2. The ability to create an inventory of information about other product components, including but not limited to identifiers. 3. The ability to keep the inventory up to date.
Product Configuration: The configuration of the IoT product can be changed, and such changes can be performed by only authorized individuals and other IoT product components.	1. The ability to change other product component configuration settings. 2. The ability to restrict changes to other product component configuration settings to authorized individuals and other IoT product components only. 3. A default setting for the initial configurations of other product components which makes those product components secure for their expected use cases. 4. The ability for authorized individuals and other IoT product components to restore the device to the default secure configuration.

IoT Product Cybersecurity Capability	Potential Additional Criteria
Data Protection: The IoT product can protect the data it stores (across all IoT product components) and transmits (both between IoT product components and outside the IoT product) from unauthorized access and modification.	1. 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: a. The ability to use a short-range and/or local network transmission protocol (e.g., Zigbee, Bluetooth, mDNS, LLDP, and IEEE 1905.1) to communicate with some product components as necessary, but protection of this data at rest on this product component and protected when transmitted to all other product components and when transmitting outside the IoT product.
Logical Access to Interfaces: The IoT product can restrict logical access to its local and network interfaces, and the protocols and services used by those interfaces, to only authorized individuals and IoT product components.	1. The ability to support controlling access to other product components. Necessary elements of this support may include: a. The ability to prevent unauthorized transmissions to or access other product components. b. The ability to validate data sent to other product components matches specified definitions of format and content. c. The ability to participate in a secure authentication mechanism with other product components (e.g., help gather authenticators, assert authorization based on authentication). d. The ability to limit use of unnecessary communication channels by product components.
Software Update: The software of all IoT product components can be updated by authorized individuals and other IoT product components only by using a secure and configurable mechanism, all as appropriate for each IoT product component.	1. The ability to support a secure update mechanism targeting other product components. Necessary elements of this support may include: a. The ability to verify and authenticate an update on behalf of another product component. b. The ability to enable or disable notifications about updates, as directed by an authorized individual, for other product components. c. The ability to transmit an update to another product component.
Cybersecurity State Awareness: The IoT product can detect cybersecurity incidents affecting or effected by its components and the data they store and transmit.	1. The ability to access and state information across the IoT product (i.e., locally and from other product components). 2. The ability to detect cybersecurity incidents using IoT product state information.
Product Security: The IoT product can perform other features and functions across some or all of its components to make IoT products minimally securable for the sector.	1. The ability for the product component to securely reestablish connections externally and with other product components when connectivity returns, in the event of an outage.

Increasingly Comprehensive Levels of Testing and Assessment (Tiers)

The EO states that the criteria for consumer IoT products must reflect increasingly comprehensive levels of testing and assessment. More cybersecurity controls may be needed for devices that pose inherently greater risks such as a door lock or stove. Manufacturers may elect to implement a basic level of cybersecurity in their products or may opt for a higher degree of security to enhance their product's capabilities and provide additional value. Manufacturers also have options regarding how their products' conformity with security standards criteria can be assessed. An effective labeling scheme should convey to a consumer the relative level of security provided by a specific IoT product. Thus, the labeling program must address multiple tiers of security achieved by various products:

- The bottom tier (or level) provides a minimum meaningful amount of assurance about the security of an IoT product.
- Each subsequent tier should provide additional security, assurance, and/or protection.

Implementing additional criteria and demonstrating conformity can involve more time and expense and may be more time-consuming to achieve. A label that clearly conveys information to the consumer about the elevated security capability the product provides and consequently may encourage consumers to select a particular product can be an incentive for manufacturers to make that investment.

Conformity Assessment Approaches

Existing 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.

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.

Criteria for the Label

Labeling conventions as currently used in various IoT-oriented labeling programs around the world focus on how an IoT product cybersecurity label is comprised, designed, and delivered. Labels may be physical and/or digital and are intended to communicate compliance with a set

of cybersecurity criteria. In some instances, there is a singular label signifying that basic security features are provided; in others the label may indicate which one of several security tiers has been achieved. In yet other instances the label may provide a catalog of cybersecurity information about the IoT device or product.

A critical dimension of product labeling is the utility of the label for the intended audience. In this case, it is important that consumer IoT product cybersecurity labels are:

- **Understandable by the consumer:** the label's content and presentation must convey its intended information in a manner that it will be understood by largely non-technical purchasers of the product.
- **Actionable by the consumer:** the label must meaningfully aid the consumer in determining whether the product's security is appropriate to the intended use.
- **Effective in conveying the product's value:** the label should clearly convey when a product provides a greater level of security, so that a consumer can understand why there may be a greater value to the individual and to society more broadly – and why there may be a cost differential among competing products with similar functionality but different security performance.

Next Steps

The criteria proposed in this white paper are a critical first element for a consumer IoT labeling program. A complete labeling program must also address:

- Final technical criteria for an IoT product and all product components;
- Increasingly comprehensive levels of testing and assessment (tiers);
- Conformity assessment approach(es); and
- Criteria for the label.

NIST will seek feedback from stakeholders on these topics during the workshop scheduled for September 14-15, 2021, as well as through other means.

Bibliography

[AGELIGHT] AgeLight Digital Trust Advisory Group (2020). IoT Safety Architecture & Risk Toolkit (IoTSA) v4.0. Retrieved from https://agelight.com/iot.html

[AUG] Australian Government (2021). Health Star Rating System. (Australian Government, Canberra, Australia). http://www.healthstarrating.gov.au/internet/healthstarrating/publishing.nsf/Content/home

[CMU] Carnegie Mellon University (2021) IoT Security and Privacy Label (Carnegie Mellon University, Pittsburgh, PA) https://iotsecurityprivacy.org/

[CSA] Cloud Security Alliance (2021). IoT Security Controls Framework v2. https://cloudsecurityalliance.org/artifacts/csa-iot-security-controls-framework-v2/

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

[CTIA] CTIA (2021). Cybersecurity Certification Test Plan for IoT Devices v1.2.2. Retrieved from https://ctiacertification.org/test-plans/

[DOE] US Department of Energy (2021). Energy Star Label. https://www.energystar.gov.
[ENISA BASELINE] ENISA Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

[ENISA BASELINE] ENISA (2017). Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures. https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

[ENISA SUPPLY CHAIN] ENISA (2020). Guidelines for Securing the IoT Secure Supply chain for IoT. https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

[EO14028] The White House (2021). EO #14028: Executive Order on Improving the Nation's Cybersecurity. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[ETSI] ETSI (2020. ETSI EN 303 645: Cyber Security for Consumer Internet of Things: Baseline Requirements v2.1.0. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.00_30/en_303645v020100v.pdf

[FINLAND] Finnish Transport and Communications Agency (2021) *Finnish Cybersecurity Label* (Government of Finland, Helsinki, Finland) https://tietoturvamerkki.fi/en/

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

[GSMA] GSMA (2019). IoT Device Certification Landscape. https://www.gsma.com/iot/wp-content/uploads/2019/09/IoT-Device-Certification-Report.pdf

[Intertek] Intertek Cyber Assurance https://www.intertek.com/cyber-assured/

[IoT Alliance] IoT Alliance of Australia IoT Security Guideline (2017) https://www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Security-Guideline-V1.2.pdf

[Intertek] Intertek Cyber Assured. https://www.intertek.com/cyber-assured/

[IoT Alliance] IoT Alliance Australia (2017). Internet of Things Security Guideline v1.2. https://www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Security-Guideline-V1.2.pdf

[IoTSF] IoT Security Foundation (2020). IoT Security Compliance Framework release 2.1. https://www.iotsecurityfoundation.org/wp-content/uploads/2020/05/IoTSF-IoT-Security-Compliance-Framework-Questionnaire-Release-2.1.zip

[ISCALABS] ISCA Labs (2021). Internet of Things (IoT) Security Testing Framework v2.01. https://www.icsalabs.com/sites/default/files/ICSALABS_IoT_reqts_framework_v2.01_210714.pdf

[ISO27402] ISO/IEC JTC1 SC27 WG4 (2021). ISO/IEC 27402: Cybersecurity – IoT Security and Privacy – Device Baseline Requirements (2nd committee draft).

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

[NEMA] NEMA Cyber Hygiene Best Practices Part 2 (NEMA CPSP 3-2019). Obtained for free from https://www.nema.org/standards/view/cyber-hygiene-best-practices-part-2

[NEMA] National Electrical Manufacturers Association (NEMA) (2019). Cyber Hygiene Best Practices Part 2. Obtained for free from https://www.nema.org/standards/view/cyber-hygiene-best-practices-part-2

[NISTIR8259] Fagan M, Megas KN, Scarfone K, Smith M (2020). NIST IR 8259: Foundational Cybersecurity Activities for IoT Device Manufacturers. National Institute of Standards and Technology (NIST). https://doi.org/10.6028/NIST.IR.8259

[NISTIR8259A] Fagan M, Megas KN, Scarfone K, Smith M (2020). NIST IR 8259A: IoT Device Cybersecurity Capability Core Baseline. National Institute of Standards and Technology (NIST). https://doi.org/10.6028/NIST.IR.8259A

[NISTIR8259B] Fagan, M, Megas, KN, Marron, J, Brady, KG, Jr., Cuthill, BB, Herold R (2020). NIST IR 8259B (draft): IoT Non-Technical Supporting Capability Core Baseline. National Institute of Standards and Technology (NIST). https://doi.org/10.6028/NIST.IR.8259B [OWASP ISVS] OWASP IoT Security Verification Standard (ISVS). Open source GitHub repository. https://github.com/OWASP/IoT-Security-Verification-Standard-ISVS

[OWASP ISVS] The Open Web Security Project (OWASP) (2021). IoT Security Verification Standard (ISVS). Open source GitHub repository. https://github.com/OWASP/IoT-Security-Verification-Standard-ISVS

[OWASP Top 10] The Open Web Security Project (OWASP) (2018). The OWASP Top 10 Internet of Things. https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project

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

[UK COP] United Kingdom (UK) Department of Digital, Culture, Media and Sport (DCMS) (2018). Code of Practice for Consumer IoT Security.
https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security

[UL MCV 1376] Underwriters Laboratory, Inc. (2019). UL MCV 1376: Methodology for Marketing Claim Verification: Security Capabilities Verified to level Bronze/Silver/ Gold/Platinum/Diamond. https://www.ul.com

[UL TOP 20] Underwriters Laboratory, Inc. (2017). IoT Security Top 20 Design Principles.
https://ims.ul.com/sites/g/files/qbfpbp196/files/2018-05/iot-security-top-20-design-principles.pdf

[UL SECURITY RATING] Underwriters Laboratory, Inc. (2021). IoT Security Rating.
https://ims.ul.com/IoT-security-rating