Before the
DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, MD 20899

In the Matter of	)
	)
DRAFT Baseline Security Criteria for Consumer IoT Devices	)
	)
	)

COMMENTS OF THE CONSUMER TECHNOLOGY ASSOCIATION

The Consumer Technology Association ("CTA")®[1] appreciates the opportunity to provide input to the National Institute of Standards and Technology ("NIST") regarding its white paper, *DRAFT Baseline Security Criteria for Consumer IoT Devices* ("White Paper").[2]

CTA appreciates NIST's development of this White Paper, which provided a helpful starting point for discussion during the first workshop on Cybersecurity Labeling for Internet of Things (IoT) Devices and Consumer Software held September 14-15, 2021.[3] As NIST works to fulfil the Administration's directives pursuant to Executive Order 14028 on *Improving the Nation's Cybersecurity*, CTA believes the White Paper—bolstered and refined by input received from the workshop and written comments—will be a valuable contribution as a comprehensive

[1] As North America's largest technology trade association, CTA® is the tech sector. Our members are the world's leading innovators—from startups to global brands—helping support more than 18 million American jobs. CTA owns and produces CES®—the most influential tech event on the planet.

[2] NIST White Paper, *DRAFT Baseline Security Criteria for Consumer IoT Devices* (Aug. 31, 2021), https://www.nist.gov/system/files/documents/2021/08/31/IoT%20White%20Paper%20-%20Final%202021-08-31.pdf ("White Paper").

[3] NIST, "Workshop and Call for Papers on Cybersecurity Labeling Programs for Consumers: Internet of Things (IoT) Devices and Software" (updated Sep. 24, 2021), https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/workshop-and-call-papers-cybersecurity-labeling.

menu of criteria to help evaluate future technical and non-technical capabilities lists.[4]

However, these baseline *criteria* must not be confused with baseline *requirements*.[5] NIST well-appreciates that capabilities for IoT devices necessarily vary across use cases and risk contexts. As noted in NISTIR 8259A, the capabilities presented in Table 1 of that guidance serve as "a starting point to help provide the means stakeholders may need to meet common cybersecurity needs and goals."[6] Further, "device cybersecurity *capabilities will often need to be added or removed* from an IoT device's design, integration, or acquisition to best address an organization's common cybersecurity risks."[7] This White Paper provides a focal point for discussion regarding elements a future cybersecurity label for consumer IoT might include; it does not provide the minimum requirements of a label itself. The White Paper appropriately

[4] Executive Order 14028, *Improving the Nation's Cybersecurity* (May 12, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[5] Likewise, the pilot program should—consistent with NISTIR 8228, NISTIR 8259, and the IoT Cybersecurity Improvement Act of 2020—differentiate conventional IT devices, such as smartphones and laptops, from IoT devices (which are finished products). *See* Internet of Things Cybersecurity Improvement Act of 2020, Pub. L. 116-207, codified at 15 U.S.C. 278g-3a note (defining IoT as "devices that— (A) have at least one transducer (sensor or actuator) for interacting directly with the physical world, have at least one network interface, and are not conventional Information Technology devices, such as smartphones and laptops, for which the identification and implementation of cybersecurity features is already well understood; and (B) can function on their own and are not only able to function when acting as a component of another device, such as a processor."); NISTIR 8259, *Foundational Cybersecurity Activities for IoT Device Manufacturers*, at 1 (May 2020), https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf. Traditional IT devices like smartphones and laptops have different computing characteristics than the wide array of consumer IoT devices, and such IT devices are already subject to rigorous security design and management requirements suitable to their particular characteristics. Conversely, the security of components within a device must be considered within the context of the finished product and therefore should not be treated as distinct IoT. Tying the pilot program's definition to NIST's existing definition, which was recognized by Congress, will foster harmonized treatment of IoT security and enable NIST to develop more tailored guidance to produce more meaningful security outcomes.

[6] NIST, NISTIR 8259A: *IoT Device Cybersecurity Capability Core Baseline*, Appendix A Table 1: *The Device Cybersecurity Capability Core Baseline for Securable IoT Devices*, at 14 (May 2020), https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259A.pdf.

[7] *Id.* at 3.

notes that NISTIR 8259A and NISTIR 8259B "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."[8] In that paragraph, the White Paper should go on to clearly explain its relationship to the baselines and that the White Paper is not, itself, a baseline. This point may too easily be missed once the document is published, and CTA encourages NIST to add explicit language to clarify that the criteria should not be confused with requirements.

NIST should also discuss and provide clarity regarding how a later process should prioritize and select criteria from the menu of criteria offered in the White Paper. In order to cover all downstream IoT device use cases and increase the awareness of participant developers, new technical standards such as draft ISO-27402 define not only a list of capabilities, but also an application process including security risk management steps. Such an application process allows each product category to receive suitable treatment regarding security capabilities and assessed risk. NIST should expand on the role of risk management in the White Paper.

Some criteria may provide more significant security benefits based on the intended use of a device. For example, Table 1, "Asset Identification," identifies both physical and logical identifiers under Potential Criteria. A physical identifier is more helpful for devices installed in accessible places, but less so when, e.g., buried or on towers or underwater. A logical identifier is more helpful for managed network systems where professional staff may be looking at a network-based inventory or forensic data. NIST should consider ways to account for different priorities across use cases in a cybersecurity labeling scheme.

NIST should also clarify that, in any future application of this document, the selected

[8] White Paper at 1.

criteria must be fully defined, objective and measurable—not subjective or vague (e.g., requiring documentation of the "ease of installation and maintenance of the IoT product" is not measurable).

As described in CTA's position paper submitted in anticipation of NIST's initial labeling workshop, any labeling scheme to address cybersecurity should avoid attempts to copy programs like EnergyGuide, which communicate different types of information on topics with distinct characteristics, and instead build on several key principles.[9] Namely, a cybersecurity labeling scheme should:

1. Be based on industry consensus standards, recognizing that no single standard or set of criteria will be appropriate for all IoT device categories or use cases;
2. Avoid fragmentation in the marketplace through deliberate long-term international coordination;
3. Be built on risk assessment as much as security capabilities, accounting for the intended application of a device at the point of design;
4. Eschew ad-hoc requirements that are not part of regional or international standards;
5. Be tailored to different categories of devices and corresponding risk profiles without implying inferior security for devices that appropriately meet different tiers;
6. Avoid conveying a false sense of security through labels and educational campaigns that clearly convey expectations to consumers;
7. Account for limited space on product packages, including allowing for electronic labeling;
8. Incorporate existing conformity assessment programs into the label's development;
9. Recognize both third party assessment and self-attestation to foster efficiency and avoid overloading the labeling ecosystem and
10. Accompany a significant consumer education campaign.

[9] CTA, "CTA Position Paper on Cybersecurity Labeling, Conformity Assessment and Self-Attestation" (Aug. 17, 2021), https://www.nist.gov/system/files/documents/2021/09/03/CTA%20Position%20Paper%20on%20Cybersecurity%20Label%20Considerations%20Final.pdf.

Building on the considerations above, we provide detailed feedback on the White Paper's criteria in a third column beside Table 1 and Table 2 in Appendix A below. The comments in many cases draw on CTA's experiences creating and implementing ANSI/CTA-2088, *Baseline Cybersecurity Standard for Devices and Device Systems*.[10]

CTA appreciates the opportunity to provide input on this White Paper. Properly positioned, it has potential to be very beneficial. We urge NIST to consider the feedback below as it works to refine this document for further use. As ever, CTA looks forward to ongoing partnership with NIST in support of a more secure IoT ecosystem.

Respectfully submitted,

CONSUMER TECHNOLOGY ASSOCIATION

By: */s/ Mike Bergman*
Mike Bergman
VP, Technology and Standards

/s/ Rachel Nemeth
Rachel Nemeth
Sr. Director, Regulatory Affairs

Consumer Technology Association
1919 S. Eads Street
Arlington, VA 22202
(703) 907-7644

October 18, 2021

[10] CTA, R14WG1 – CTA-2088 – Baseline Cybersecurity Standard for Devices and Device Systems (pub. Jan. 19, 2021), https://standards.cta.tech/apps/group_public/project/details.php?project_id=594.

APPENDIX A: CTA Comments on White Paper Table 1 and Table 2

Table 1: IoT Product Cybersecurity Capabilities Developed from NISTIR 8259A Using Informative References		
IoT Product Cybersecurity Capability	**Potential Criteria**	**CTA Comments**
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.	NIST must exercise caution regarding requirements for device identifiers. CTA-2088 notes that stable device identifiers, such as the International Mobile Equipment Identity or "IMEI," create a privacy risk. CTA-2088 therefore requires that such specifications include instructions to "disclose only to authorized parties" (wherein a trusted device can also be a "party" in this context).
	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.	NIST should treat the ability to disable unwanted features as a perk but not a necessity. Manufacturers cannot always determine what features a customer does not want prior to the point of sale, nor can a manufacturer necessarily make all features—or even any, in some categories—disabled. CTA

		recommends NIST revise this criterion to state "optionally including disabling certain features."
	2. The ability to restrict configuration changes to authorized individuals and other IoT product components only.	NIST should clarify this criterion allows changes by "…authorized individuals and other *trusted* IoT product components only."
	3. A default setting for the initial configuration which makes the product component secure for expected use cases.	
	4. The ability for authorized individuals and other IoT product components to restore the product component to the default secure configuration.	Certain simple device types, such as use-once IoT devices, may not need to support this criterion. CTA recommends adding an option to account for such devices with the following language: "…or a notice that re-provisioning is not possible and therefore secure disposal is required."
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.	NIST should broaden the scope of this criterion beyond just "cryptographic algorithms" to include "cryptographic methods," which encapsulate algorithms, protocols, etc. CTA-2088 uses similar language to reflect the industry best practice of using verified and accepted methods.
	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.	NIST should clarify that "authorized" applies to "other IoT product components" and to "systems." Any device or system able to modify the subject device configuration should include some element of AuthN/AuthZ. NIST may consider revising this criterion to include "other *trusted* IoT product components and *trusted* systems" where "trusted" is a defined term.
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.	NIST should use caution when mandating the ability to restrict access to network interfaces to "authorized persons." A more general term, such as "authorized entities," would allow for, e.g., entities like manufacturers to perform necessary activities (such as "push updates").

	3. The ability of the product component to validate that the input received through its interfaces matches specified definitions of format and content.	NIST should add "length" to this criterion so that it includes "definitions of length, 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.	See comment above.
	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)	NIST should clarify that this criterion allows for a pre-defined default password that is unique to each device. Customer Premises Equipment or "CPE" routers commonly use this method wherein a manufacturer encodes a password and prints it on a housing sticker. NIST may consider revising this criterion to state: "not delivering the product with any non-unique default password."
	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	1. The ability to update the product component's software through remote (e.g., network download)	CTA suggests adding "cryptographically secure method for authorized entities."
	2. The ability for the product component to verify and authenticate any update before installing it.	

secure and configurable mechanism, as appropriate for each IoT product component.	3. The ability to enable or disable notifications about updates.	NIST should clarify that this criterion does not mean enabling the user to disable updates. If NIST intends this criterion to mean that a device enables a silent automatic update mode, NIST should consider that such a capability can compromise stable installs in some use cases, e.g., in smart home devices, where a silent update may "break" a working install. Furthermore, with the current wording, the need to enable/disable notification of software updates depends on the usage and use case of the IoT device and is a user convenience, not a necessity for secure operation.
	Note: updating of some product components by be dependent on or performed by the product component host.	
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).	Logs use limited system resources, may degrade device performance and may have limited value in the IoT device context. Logs are typically not accessible or understandable by end users, are typically not available to device manufacturers, and may contain personally identifying information or data. Criterion should not assume log use when the vast majority of customers or

		use cases do not include professional network management.
	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.	Changes in IoT functionality in response to changes in environmental conditions (such as network outages or connectivity disruptions) are matters of product functionality and user convenience, not security. A better formulation might be: "IoT devices should maintain their security features even when environmental conditions change (such as network outages or connectivity disruptions)."

Table 2: Non-Technical Supporting Capabilities Developed from NISTIR 8259B Using Informative References		
Non-Technical Supporting Capability	**Potential Criteria**	**CTA Comments**
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:	NIST should clarify that this documentation supports a manufacturer's *internal* activities such as secure development lifecycle or "SDLC" and that NIST does <u>*not*</u> expect this type of documentation to be shared with customers. Few customers would find such information meaningful or useful. More broadly, NIST and its stakeholder community should use this pilot program to develop thoughtful distinctions between what information manufacturers need to support IoT security versus what information consumers need to support purchasing decisions and secure IoT device use.
	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)	The security benefit of disclosing "bandwidth requirements" is unclear as bandwidth is simply a

		function of data delivered over time. A better formulation might simply be “connectivity requirements” or “security requirements.” This requirement should be tailored to help convey network resources (sites) that the manufacturer designed the device to visit in normal operation. This amounts to ‘soft’ device intent notification, as opposed to the Manufacturer Usage Description (“MUD”) standard or other ‘hard’ device intent notification.
	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 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)	Inclusion of "all hardware and software components" makes this criterion extremely overbroad. Most hardware (e.g., condensers, transistors, antennae, etc.) and software (e.g., video players, image processing, etc.) in a connected TV for example have no security implications.
	b. IoT platform 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	Ease of installation and maintenance are matters of product functionality and user convenience, not security.
	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 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).	NIST should remove this criterion as it reaches beyond the scope of security capabilities. "The ability for the manufacturer…to respond to customer…" effectively constitutes a warranty. NIST may consider revising this criterion to include the "ability to respond to outside inquiries" (without the keyword "customer").
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	NIST should clarify that this item covers actual incidents or discovered vulnerabilities. The

	and certifiers, third-party support and maintenance organizations) about cybersecurity relevant information such as:	wording in the item immediately below "applicable" documentation would seem to narrow the scope of information dissemination to the documentation related to an incident. This sense doesn't come through clearly. Combined with the extensive (internal, we assume) documentation list above, this phrasing may be misinterpreted into a requirement for huge stacks of documentation as a matter of course. CTA recommends two revisions: first, to make this item 2 more clearly scoped for incidents or vulnerabilities; and second, clarify that "applicable" documentation and other actions are relative to the specifics of the issue at hand, not a commonly comprehensive block of information that is sent with every alert. These revisions to the documentation requirement will foster good recordkeeping by the manufacturer, and target alerts to relevant information.
	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 actions to prevent similar breaches of other products and/or product components.	