Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Cybersecurity Labeling for Internet of Things	)	PS Docket No. 23-239
	)	

COMMENTS OF CONSUMER TECHNOLOGY ASSOCIATION

J. David Grossman
Vice President, Policy & Regulatory Affairs

Mike Bergman
Vice President, Technology & Standards

Rachel S. Nemeth
Senior Director, Regulatory Affairs

Consumer Technology Association
1919 S. Eads Street
Arlington, VA 22202
(703) 907-7651

August 19, 2024

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Cybersecurity Labeling for Internet of Things	)	PS Docket No. 23-239
	)	

COMMENTS OF CONSUMER TECHNOLOGY ASSOCIATION

Consumer Technology Association (CTA)®[1] respectfully submits these comments in response to the Federal Communications Commission ("Commission" or "FCC") Public Safety and Homeland Security Bureau's (Bureau's) Public Notice (*Notice*) on *Implementation of the Cybersecurity Labeling for Internet of Things Program*.[2] By implementing the IoT Cybersecurity Labeling Program (Program) consistent with the recommendations below, the Commission will set a strong foundation for a consumer-friendly, public-private partnership to increase the security of consumer IoT devices.

I. INTRODUCTION AND SUMMARY

CTA appreciates the Commission's ongoing work to develop the Program in a way that establishes a strong foundation of trust in the U.S. Cyber Trust Mark (Mark) with the ability to implement the Program quickly and evolve over time. To support this goal, the *Notice* seeks comment on various implementation matters, including, among other issues: (i) how to design the general structure and requirements for a decentralized IoT product registry by which

[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 powerful tech event in the world.

[2] *Cybersecurity Labeling for Internet of Things*, Public Notice, PS Docket No. 23-239, DA 24-617 (PSHSB rel. June 27, 2024) (*Notice*).

consumers (using a smart device) can scan a QR code to reach the uniform labels of IoT products bearing the Mark; (ii) whether to require manufacturers to make additional disclosures beyond those listed in the *Order* establishing the Program;[3] (iii) how to ensure competitive neutrality among Cybersecurity Labeling Administrators (CLAs) and the Lead Administrator and (iv) whether to treat manufacturer applications as presumptively confidential.

As a foundational matter regarding the decentralized IoT product registry, CTA urges the Bureau to adopt a CLA-hosted, manufacturer-updated architecture as an implementation of the intent and technical requirements of the *Order*. This approach will facilitate the security, availability and integrity of IoT labels as well as support multiple display options and empower both manufacturers and the Commission to regularly update information so that consumers can use the IoT label easily and accurately. A CLA-hosted architecture will also help to reduce burdens on manufacturers and support the Program's expansion over time.

CTA provides additional suggestions at this stage to support the timely and effective implementation of the Program. First, manufacturers should disclose only those sensors included in their IoT products that offer cybersecurity utility, pursuant to NISTIR 8425 Section 2.2.2. Other information, such as the data a particular sensor collects or shares, is outside the scope of the Program. Also, this data is often already available to the consumer and would crowd the IoT product label. Second, the Bureau should leverage CTA's draft Scheme Assessment Framework (draft ANSI/CTA-2119) as a transparent, objective safeguard to assess Schemes[4] and entities

[3] *Cybersecurity Labeling for Internet of Things*, Report and Order and Further Notice of Proposed Rulemaking, PS Docket No. 23-239 (rel. Mar. 15, 2024) (*Order*).

[4] In this context, a Scheme is a "Set of rules and procedures that describes the objects of conformity assessment, identifies the specified requirements and provides the methodology for performing conformity assessment"; *see* Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products, NIST, Feb. 2022, https://doi.org/10.6028/NIST.CSWP.02042022-2.

(e.g., CLAs and CyberLABs) that support the Program to ensure competitive neutrality, particularly at the outset of the Program's implementation. Third, CTA supports the Bureau's tentative proposal to treat manufacturer applications for the Mark as presumptively confidential, as this will incentivize manufacturer participation without harming the public interest. Finally, CTA reiterates that a key component of the Mark's success will be the government's leadership in a broad consumer education campaign.[5] As part of this effort, the government should leverage available resources across agencies such as the Cybersecurity and Infrastructure Security Agency (CISA) and the National Institute of Standards and Technology (NIST) to promote a whole-of-government approach to the Program.

We elaborate on these recommendations below and look forward to continued collaboration with the Bureau to operationalize the Mark.

II. A CLA-HOSTED, MANUFACTURER-UPDATED DECENTRALIZED REGISTRY WILL ENHANCE UTILITY FOR CONSUMERS AND OPTIMIZE MAINTENANCE OVER TIME

The *Order* lays out a vision of a flexible, distributed architecture with specific technical requirements. Based on thorough discussion with CTA members as well as other Program stakeholders that participate in CTA's Cyber Labeling Steering Committee and R14 Cybersecurity and Privacy Management technical working groups, CTA recommends that the Bureau adopt the decentralized registry in the form of a CLA-hosted architecture that leverages existing capabilities from entities already well-positioned to serve as CLAs, while also enabling manufacturers to update information regarding their IoT products as needed. A CLA-hosted registry can better ensure the integrity and availability of the common application program

[5] *See* Comments of CTA, PS Docket No. 23-239, at 31-32 (filed Oct. 6, 2023); *see also* Letter from Association of Home Appliance Manufacturers, et. al., PS Docket No. 23-239, at 2 (filed Nov. 8, 2023).

interface (API) envisioned in the *Order*, while still enabling manufacturers to update product information in a timely manner. This approach would allow the registry to support multiple display options for consumers, as proposed in the *Notice*, and empower registry operators to implement adequate security, privacy and availability controls to protect that information.[6] As a general matter, the frequency of updates to the registry should follow material changes to the registry information; however, the Bureau should wait to formalize requirements on this point until it has recommendations from the 90-day stakeholder process directed by the *Order*.

A. The Bureau Should Adopt a CLA-Hosted, Manufacturer-Updated Decentralized Registry

Consistent with the Commission's conception of the registry in the *Order*, the Bureau should implement a decentralized registry architecture in which (1) the CLA is responsible for rendering (i.e., "hosting") the QR code landing pages for the IoT products it authorizes; and (2) the manufacturer maintains the data of its IoT products and updates the cached version of that data at the CLA. A central redirection server would allow for necessary maintenance, such as moving a landing page to another domain without invalidating QR codes on printed boxes. Specifically, CTA recommends that the Bureau authorize a registry supported by the following components:

- **Packaged IoT Product bearing the Mark with QR Code:** As described in the *Order*, IoT products bearing the Mark will also display a QR code (on the product packaging) that can be scanned for an encoded URL. This URL will take the consumer to a redirect that then resolves to a landing page with the Mark IoT product label, which provides information on certain data elements regarding the IoT product's security.

- **Consumer Smart Device:** Consumers will use a smart device, such as a smart phone or tablet, to scan the QR code on the IoT product to reach the Mark IoT product label.

[6] *Notice* ¶¶ 23-24.

- **Central Redirect Server:** A Central Redirect Server will be the target for all QR code URLs. When a consumer scans a QR code, the Central Redirect Server will redirect the HTTP request to the actual home of the QR code landing page. This Server requires a database (of the QR code URLs and matching landing page URLs) and a small program to crossmatch and deliver. As the Central Redirect Server only performs this single function, CTA anticipates that it will be relatively simple and inexpensive to deploy. The Central Redirect Server will maintain the functioning of the registry in instances where the landing page domain must move or when the host of the landing page is no longer in business. It will allow businesses flexibility because the hosting of the landing page will not be fixed to one entity by package printing of the QR code.

- **CLA:** The CLA will host the IoT product data initially, receive updates from manufacturers and respond to landing page requests.

- **CLA Servers:** A CLA Server will provide a database and web server implementation. Many entities who perform functions that make them likely candidates for FCC-approved CLAs already have this capability.

- **Manufacturer Servers:** The manufacturer will maintain the data for its IoT products bearing the Mark and update the cached version of this information hosted by the CLA. Certain aspects of the IoT product record—such as the Mark certification status—may not be under direct control of the manufacturer and will be updated separately.

The above recommendations are reflected in the diagram attached as Appendix A. As that diagram shows, in this proposed architecture, both manufacturers and the Commission could continuously provide up-to-date information to CLA Servers to ensure IoT product label information stays current, while the Central Redirect Server ensures HTTP requests reach the appropriate IoT label landing page (even in cases where the registered target changes after the product packaging reaches consumers).[7]

Although the *Notice* contemplates manufacturers potentially hosting QR code landing pages themselves,[8] subject matter experts in CTA's Cyber Labeling Steering Committee and R14

[7] *See* Appendix A below.

[8] *Notice* ¶ 22 (noting that the Bureau believes product data would be hosted by the manufacturers or in partnership with their selected third party and made available through the common API that is secure by

Cybersecurity and Privacy Management technical working groups share concerns regarding that approach. First, participants will not be able to manage landing page quality at the scale industry anticipates from a successful Program. In addition, responsiveness, rate-limiting, DDoS protection and other responsibilities of the landing page servers would be a burden if individually required of all manufacturers, which could lead to uneven compliance and support.

Conversely, a CLA-hosted registry will fulfill the Commission's vision for a modest initial registry with potential to accommodate increasing demands as the Program grows. It can leverage the existing infrastructure and expertise of likely Program participants.[9] Under this approach, manufacturers will be responsible for maintaining their own product data and keeping the data current as the *Notice* suggests,[10] and CLAs will support the consumer landing page, ensuring a uniform consumer experience. Such a split also reflects that CLAs are in the best position to update certain product details outside the manufacturer's control (such as whether a product has fallen out of compliance with the Mark's requirements). CTA agrees with the Bureau that there should be multiple ways for consumers to retrieve IoT product label information, and the proposed ".gov" landing page would be a helpful—if not immediately essential—effort.[11]

design and seeks comment, e.g., on how manufacturers should maintain and implement interactions with their products' data).

[9] *See Order* ¶ 116.

[10] *Notice* ¶ 22.

[11] *See Notice* ¶ 24.

B. A CLA-Hosted Registry Can Better Ensure the Integrity and Availability of the API, While Still Enabling Manufacturers to Update Product Information in a Timely Manner

The Commission determined that manufacturers will provide IoT product information to the registry through a common API that is secure by design.[12] The *Notice* seeks input on how the API should be structured and used.[13] The Commission can most effectively implement this API and reduce burdens on manufacturers supporting the decentralized registry by planning for the CLAs to provide QR code landing pages and having manufacturers support a mutually agreeable software interface (i.e., the "common API") between them.[14] The Commission correctly emphasizes that this API should be secured, which implies that the API itself will not be public. Although establishing a secured API is more burdensome than setting up a public one, maintaining a public API leaves the system open to abuse. CLA candidates known to CTA have secure data interfaces to their participants already and are in a better position to support a secured API than individual manufacturers that will participate in the Program.

Under the proposed CLA-hosted distributed registry approach discussed above, CLAs can ensure the integrity and availability of the API by leveraging industry-standard techniques

[12] 47 C.F.R. § 8.222(a).

[13] *Notice* ¶ 22.

[14] Importantly, the *Order* does not define "API" strictly in terms of programming nomenclature (e.g., regarding calls, responses, data structures, etc.). Instead, "API" may be interpreted generally as a software-defined interface that enables the goals of the Program, consistent with Commission precedent. *See, e.g., Accessibility of User Interfaces, and Video Programming Guides and Menus*, Third Report and Order, FCC 24-79, ¶ 28 n.126 (rel. July 19, 2024) (noting "An API is an application programming interface. We understand that some devices or applications covered by our rules may use other tools comparable to APIs, such as application programming kits (APKs) or software development kits (SDKs). All references herein to APIs shall be read to include any such comparable development tools that allow one device or application to coordinate with another."). CTA supports this more flexible approach, as manufacturers and certain CLA candidates already maintain programmatic data exchanges that would suit the Program's needs. Requiring that these entities switch to a strict definition of API would add unnecessary labor and time to implementing the Program.

for authorization and authentication. Some entities that intend to apply as CLAs already implement such controls. If CLAs host the common API and manufacturers use it as implied in the *Order*, they could implement rate-limiting, and rate-limiting would need to be implemented in only those CLA locations. Recognizing that the registry will contain some "fixed" fields (e.g., the date of testing) and that some fields may change (e.g., a manufacturer's support URL or end of the support period), this CLA-hosted model will still allow manufacturers to maintain and implement interactions with their product's data in connection with the API by hosting their own product data and periodically updating the cached copy of that data at the CLA. It will also enable CLAs to update information that cannot or should not be changeable by the manufacturer (e.g., if the manufacturer's product is added to the FCC's Covered List, then the Commission may want the CLA to preemptively change the product status in the CLA-hosted database).

C. The Registry Can Support Multiple Display Options as Proposed in the *Notice*

CTA agrees with the Bureau's tentative determination that at least three different registry display options may be supported: (i) product-specific data hosted by the manufacturer or its selected third party; (ii) vendor data provided for presentation by a commercial retailer and (iii) aggregated data provided for presentation of multiple products.[15] For clarity, the CLA is the designated third party with respect to product-specific data hosted by the manufacturer or its selected third party in the CLA-hosted decentralized architecture. In this architecture, the manufacturer owns the core data and the CLA caches a copy and presents a landing page to the consumer. For vendor data provided for presentation by a commercial retailer, the retailer already has direct communications with the manufacturer, who provides necessary information for current product shopping and comparison pages. This existing data includes package size and

[15] *Notice* ¶ 23.

weight, key features and specifications and other information. Extending this information to the Program is relatively straightforward. If there is an additional interface available, a retailer may choose to exercise it, for example, to confirm the current IoT product certification status. With regard to aggregated data provided for presentation of multiple products, retailers commonly provide this service to consumers also, and consumers are accustomed to receiving and understanding such aggregated data. The *Order* and the *Notice* contemplate a landing page on a ".gov" domain.[16] This feature can be supported by an additional interface as well. CTA's R14 WG7 is developing a machine-readable data structure for such an interface.[17]

D. Registry Operators Should Implement Adequate Security, Privacy and Availability Controls

The Commission notes that registry operators should implement adequate security, privacy and availability controls and correctly emphasizes that these controls should be commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification or destruction of the information collected, maintained and used.[18] However, in this voluntary program funded solely by manufacturer fees, strict adherence to government standards of information security would be a significant deterrent to participation for entities – the potential Lead Administrator and CLAs – that are not familiar with the rigor of agency and federal procurement IT system requirements. Certification to government standards

[16] *See Notice* ¶ 24 n.56.

[17] As CTA's R14 Working Group 7 advances work on a standardized label format that complies with the requirements and intent of the *Order*, it is appropriate to define the machine-readable version of the label data in the same document, (draft) CTA-2120. The Working Group has chosen JSON data format for this purpose and has a draft JSON "schema" completed to this purpose. The intent is that the API use RESTful techniques to exchange this JSON data, fulfilling the API intent expressed in the *Order* in a standardized way that uses a very common industry approach. These details must be confirmed in the 90-day stakeholder process.

[18] *See Notice* ¶ 19.

is a lengthy process and incurs a high cost to bring the entity into compliance and to earn certification. Adopting a standard that requires registry operators to implement security, privacy and availability controls that meet FISMA low/moderate standards or a commercial equivalent may prevent most or all prospective Lead Administrator and CLA candidates from participating.[19] For example, the ISO 27001 certification process can take a year or more at a cost upwards of $100,000. While these numbers are approximate, they provide guidance as to the significant bar that strict FISMA or other requirements would impose on the Program. CTA suggests that the 90-day stakeholder process include discussion on "commercial equivalents" that considers how to keep the burden on candidate CLAs as low as possible, while supporting the security, privacy and availability needs of the Program.

E. Manufacturers Are Best Positioned to Determine When to Update the Registry Information and Make Changes as Appropriate

To balance administrative burdens with the importance of maintaining accurate, up-to-date information for consumers, manufacturers should determine when there has been a material change, requiring a change in the registry information.[20] CTA recognizes that the Bureau may wish to place constraints on or trigger such updates, such as when the API must indicate that the product is no longer certified. The Bureau should wait to make these types of decisions until the registry data fields are fully defined in CTA-2120 and the results of the Lead Administrator's 90-day stakeholder process provide the necessary information to inform those decisions.

[19] *See id.* ¶ 24.

[20] This approach is consistent with suggestions from other stakeholders, e.g., to balance administrative burdens against the importance of maintaining secure IoT products in an evolving threat environment by requiring manufacturers to renew their request for an IoT product's authorization to bear the Mark when there has been a material change to the device, NIST or recognized industry guidance, or the threat environment. *See* NCTA March 8 ex parte at 3.

III. MANUFACTURERS SHOULD DISCLOSE THOSE SENSORS THAT MAY BE CONSIDERED IN THE CONTEXT OF CYBERSECURITY RISKS BUT NOT UNRELATED ELEMENTS OR PRACTICES

The Mark is a cybersecurity program informed by cybersecurity subject matter experts and intended for cybersecurity awareness. It is appropriately and narrowly tailored to inform consumers about the cybersecurity posture of IoT devices and help mitigate cybersecurity risks for consumers. Manufacturer disclosures should avoid either overwhelming consumers with too much information or duplicating information often disclosed elsewhere where a consumer already knows to look (such as a privacy policy). Consistent with the baseline requirements identified in NISTIR 8425, manufacturers should be required to list *some* types of sensors contained in the complying product (i.e., sensors that read video, sound, and position), but not sensors that do not pose meaningful cybersecurity risk (e.g., barometric pressure readers).

NISTIR 8425's baseline criteria relies on the concept of "cybersecurity utility," i.e., something that has purpose and value in the context of cybersecurity risk mitigation. Some data elements—e.g., data encryption capabilities—speak directly to cybersecurity utility and fall clearly within the scope of NISTIR 8425 criteria. Other data elements—e.g., data sharing—may have privacy utility but do not speak directly to the securability of the product. A third category of data elements—e.g., the means of data collection—may have overlapping cybersecurity and privacy utility. Some types of sensors, specifically those that read video, sound and position information, fall into this third category specifically because of their cybersecurity utility and regardless of any perceived value in a privacy context.

CTA supports manufacturer disclosure of these types of sensors for IoT products seeking the Mark because their presence directly informs requirements to document data created and handled by the IoT product and informs consumers on how to manage device data, including creation, update and deletion of data on the IoT product.[21] Conversely, the Program should not require manufacturers to disclose what data is collected by the sensors in their IoT products and whether that data is shared with third parties. That information may provide utility for privacy risk management but does not provide cybersecurity utility in support of NISTIR 8425 criteria. Therefore, it is out of scope for the Program. This grounding in cybersecurity utility should continue to inform decisions regarding what data elements fall within the scope of the Program to ensure it remains aligned with and informed by NISTIR 8425, consistent with the Commission's goal for the registry to "assist the public in understanding security-related information about the products that bear the Cyber Trust Mark"[22] and in the spirit of the Program rules.[23]

IV. CTA'S DRAFT SCHEME ASSESSMENT FRAMEWORK PROVIDES A TRANSPARENT AND OBJECTIVE SAFEGUARD TO ASSESS SCHEMES AND ENTITIES IN A COMPETITIVELY NEUTRAL FASHION

The Bureau wisely seeks comment on whether there are safeguards it might adopt to ensure the stakeholder process remains competitively neutral and the recommendations the Lead Administrator makes to the Commission (e.g., standards and testing criteria and label design) are stakeholder consensus-based and competitively neutral.[24] CTA suggests addressing this with a uniform Scheme Assessment Framework as provided by (draft) ANSI/CTA-2119.

[21] *See* NISTIR 8425 Section 2.2.2 IoT Product Non-Technical Supporting Capabilities.

[22] *Order* ¶ 113.

[23] *See, e.g.,* 47 C.F.R. § 8.221(a)(5), which requires the Lead Administrator in collaboration with CLAs and other stakeholders to recommend any appropriate modifications to the Program standards and test procedures to stay aligned with NIST guidelines. It follows that the registry requirements likewise should remain aligned with NISTIR 8425.

[24] *Notice* ¶ 13.

The *Order* itself already contains some safeguards to ensure competitive neutrality. For example, the rules require CLAs to obtain common accreditation and attest to common capabilities and expertise.[25] However, to expedite initial deployment of the Program, the Commission will accept and conditionally approve applications from entities that meet the other FCC Program requirements and commit to obtaining accreditation pursuant to all the requirements associated with ISO/IEC 17065 with the appropriate scope within six months of the effective date by the adopted standards and testing procedures. Therefore, the "initial deployment" phase of the Program will involve certifying products and authorizing the use of the Mark before accreditation is completed, implying potentially months of product certifications prior to this milestone.[26] This is a critical distinction. Accreditation provides third party assurance because it brings in an impartial outside expert to evaluate entities and schemes. But to permit certification prior to accreditation, the Program must rely on first party assurances, statements and attestations. Safeguards in evaluating these assurances, statements and attestations cannot result in the equivalent of third-party surety, but some useful tools can level out the process and make it more neutral.

When accreditation is possible, it will be in the context of CLAs and CyberLABs using a specific Scheme that complies with the outcome-based NISTIR 8425 criteria. To evaluate whether a Scheme meets the criteria, CTA has offered (draft) ANSI/CTA-2119 Scheme Assessment Framework. In addition, the Commission may ask CyberLABs to attest that they can perform the assessments and collect the documentation specified in CTA-2119 in accordance with the NISTIR 8425 criteria. CLAs can be asked to attest that they have the necessary

[25] 47 C.F.R. § 8.219.

[26] 47 C.F.R. § 8.220(c)(6).

cybersecurity expertise to review a test report that contains the functional assessments and documentation specified in CTA-2119. Therefore, this industry consensus standard provides a transparent and objective safeguard for assessing Schemes and entities in a competitively neutral fashion.

V. TREATING MANUFACTURER APPLICATIONS AS PRESUMPTIVELY CONFIDENTIAL WILL INCENTIVIZE PARTICIPATION

CTA agrees that manufacturer applications should be treated as presumptively confidential.[27] This includes test reports and materials submitted either as routine application process materials, or in line with participant responses to the Commission, CyberLAB and/or CLA requests. In the first case, manufacturer test reports and applications will have a significant amount of confidential data.[28] Routine disclosure of elements of these reports and applications would significantly deter participation in this voluntary program. Conversely, failing to provide confidential treatment of these in-process documents would serve little-to-no public interest, because the label itself discloses important product information.

Materials submitted in line with participant responses to the Commission, CyberLAB and/or CLA requests should be treated as presumptively confidential for the same reason. For example, the Commission should affirm that the Program will not require public disclosure of the contents of a manufacturer's Software Bill of Materials (SBOM) or Hardware Bill of Materials (HBOM).

[27] *Notice* ¶ 17 (proposing that the Bureau treat applications as presumptively confidential and CLAs should be required to maintain this confidentiality).

[28] *See id.* (anticipating that "the manufacturer applications submitted to CLAs will contain commercially sensitive and proprietary information that the manufacturers customarily treat as confidential, including, but not limited to, test reports").

VI. THE GOVERNMENT MUST LEAD A BROAD CONSUMER EDUCATION CAMPAIGN THAT LEVERAGES AVAILABLE RESOURCES TO SUPPORT THE PROGRAM'S SUCCESS

CTA appreciates the Commission's recognition of the importance of consumer education in the context of the Mark. Ensuring that consumers know to look for the Mark, understand what it means, and know how to use the Mark to evaluate products is all intrinsic to the mission of the Program.[29] Every stakeholder in the Program has a role to play in this effort. However, broad consumer education should primarily be the responsibility of the federal government. CTA urges the Commission to work with federal partners in a coordinated manner to leverage available resources and existing mechanisms to drive awareness and understanding of the U.S. Cyber Trust Mark.

VII. CONCLUSION

CTA appreciates the Bureau's continuing work to implement the Program. The Bureau can materially advance Program implementation at this stage by: (1) adopting a CLA-hosted, manufacturer-updated registry architecture, (2) limiting disclosure requirements to data elements that offer cybersecurity utility for NISTIR 8425 (e.g., by requiring manufacturers to disclose some sensors but not what information is collected or shared), (3) leveraging CTA's Scheme Assessment Framework to ensure competitive neutrality across CLAs and the Lead Administrator, (4) treating manufacturer applications as presumptively confidential and (5) working with federal partners to leverage available resources for a government-led consumer

[29] As Commission has recognized, the success of the U.S. Cyber Trust Mark program will rely on a robust education campaign with effort across the program's stakeholders to promote recognition, brand trust and transparency. *NPRM* ¶ 53. CTA and other stakeholders have underscored that U.S. government should lead this effort, with key focus on driving consumer awareness of the brand and how to interpret the label, with the private sector augmenting the government's campaign through advertising, websites and social media. *See* CTA Comments at 31-32.

education campaign. CTA looks forward to continued engagement with the Commission to stand up a successful Program.

Respectfully submitted,

CONSUMER TECHNOLOGY ASSOCIATION

By: /s/ *J. David Grossman*
J. David Grossman
Vice President, Policy & Regulatory Affairs

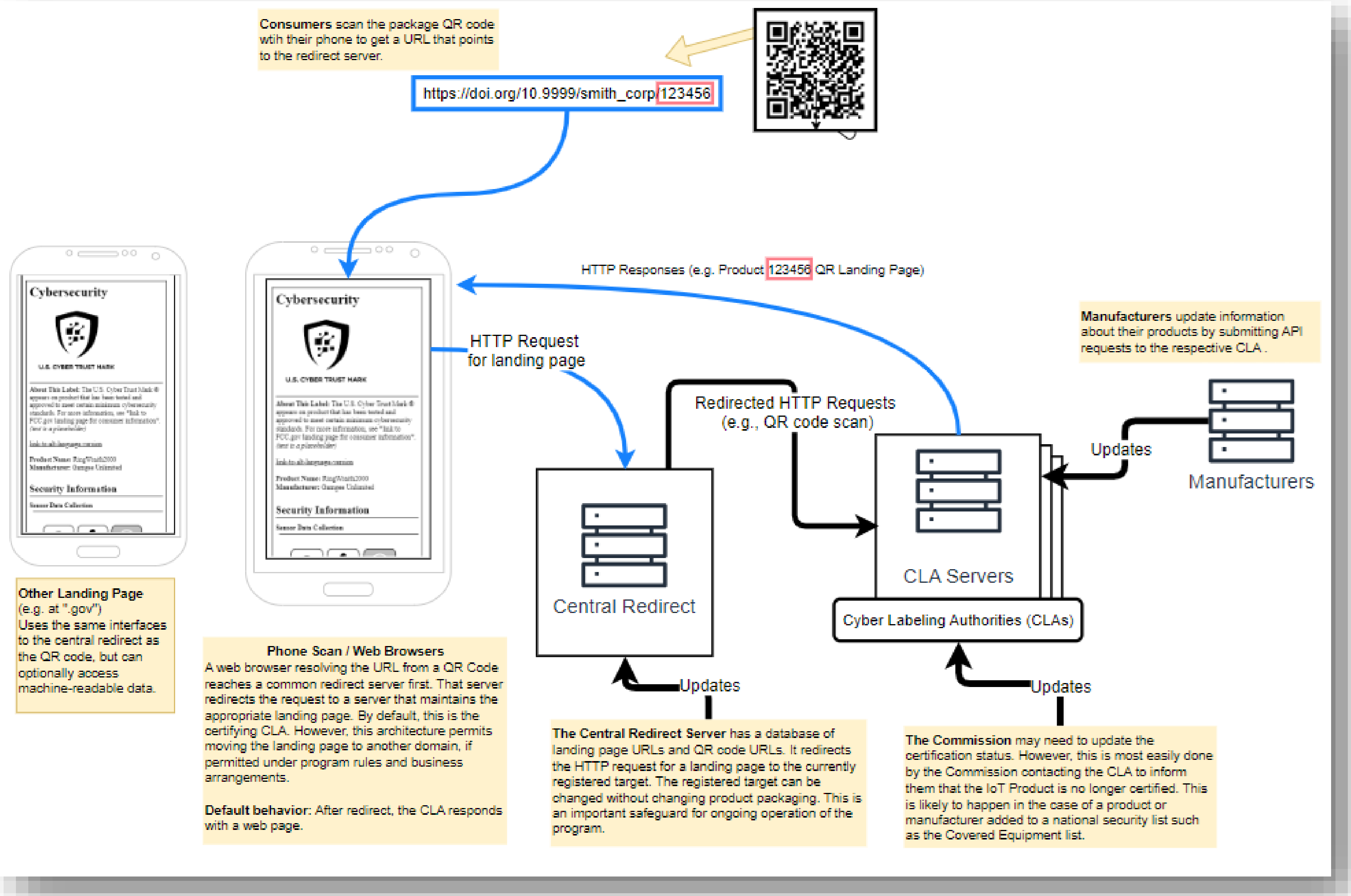
/s/ *Mike Bergman*
Mike Bergman
Vice President, Technology & Standards

/s/ *Rachel S. Nemeth*
Rachel S. Nemeth
Senior Director, Regulatory Affairs

Consumer Technology Association
1919 S. Eads Street
Arlington, VA 22202
(703) 907-7651

August 19, 2024

APPENDIX A: CLA-HOSTED, MANUFACTURER-UPDATED DECENTRALIZED REGISTRY



Consumers scan the package QR code wtih their phone to get a URL that points to the redirect server.

Manufacturers update information about their products by submitting API requests to the respective CLA .

Other Landing Page
(e.g. at ".gov")
Uses the same interfaces to the central redirect as the QR code, but can optionally access machine-readable data.

Phone Scan / Web Browsers
A web browser resolving the URL from a QR Code reaches a common redirect server first. That server redirects the request to a server that maintains the appropriate landing page. By default, this is the certifying CLA. However, this architecture permits moving the landing page to another domain, if permitted under program rules and business arrangements.

Default behavior: After redirect, the CLA responds with a web page.

The Central Redirect Server has a database of landing page URLs and QR code URLs. It redirects the HTTP request for a landing page to the currently registered target. The registered target can be changed without changing product packaging. This is an important safeguard for ongoing operation of the program.

The Commission may need to update the certification status. However, this is most easily done by the Commission contacting the CLA to inform them that the IoT Product is no longer certified. This is likely to happen in the case of a product or manufacturer added to a national security list such as the Covered Equipment list.