Before the
Federal Communications Commission
Washington, DC

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

COMMENTS OF CTIA

Umair Javed
Senior Vice President and General Counsel

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

David Valdez
Vice President, Privacy and Cybersecurity

John A. Marinho
Vice President, Technology and Cybersecurity

Justin Perkins
Director, Cybersecurity and Policy

Mike Beirne
Director, Regulatory Affairs

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200
www.ctia.org

August 19, 2024

TABLE OF CONTENTS

I. INTRODUCTION

CTIA welcomes the opportunity to comment on the Federal Communications Commission ("FCC" or "Commission") Public Safety and Homeland Security Bureau's ("Bureau") Public Notice ("Notice") seeking comment on Implementation of the Cybersecurity Labeling For Internet of Things ("IoT") Program.[1] CTIA shares the Commission's goals of promoting IoT device security and improving consumer confidence and understanding about the security of connected devices. To help ensure the success of the program, CTIA and its members offer feedback on how the Commission can establish a framework for program administration to encourage "efficient and timely" rollout and promote robust participation in the program.[2] In offering these recommendations, CTIA draws on its years of experience as a leader in IoT security, which includes administering its own program for IoT cyber certifications,[3] collaborating with the National Institute of Standards and Technology ("NIST"),[4] and advancing IoT security across a wide variety of industry venues.

[1] Public Notice, Public Safety and Homeland Security Bureau Requests Comment on Implementation of the Cybersecurity Labeling for Internet of Things Program, PS Docket No. 23-239, DA 24-617 (rel. June 27, 2024) ("Notice").

[2] Notice ¶ 1.

[3] CTIA Certification, *Internet of Things (IoT) Cybersecurity Certification*, https://ctiacertification.org/program/iot-cybersecurity-certification/ (last visited Aug. 19, 2024).

[4] *See, e.g.*, Comments of CTIA, *NIST's Consumer Cybersecurity Labeling Pilots: The Approach and Contributions*, NIST Request for Contributions (filed Mar. 15, 2022); Comments of CTIA, *Draft Baseline Security Criteria for Consumer IoT Devices*, Draft NIST Cybersecurity White Paper (filed Oct. 18, 2021), http://bit.ly/45iZfa4.

CTIA commented on the Notice of Proposed Rulemaking ("NPRM")[5] and is pleased to provide input on implementation issues raised by the Bureau in the Notice, which seeks to develop some issues left open in the March 2024 Order ("Order").[6] *First*, CTIA urges the Commission to clearly identify the costs associated with the U.S. Cyber Trust Mark ("Mark") program and to develop funding approaches that meet the needs of the program without discouraging voluntary participation. Perhaps the most significant costs will be associated with consumer education, for which federal funding should be secured. Other costs that need consideration and clarification include maintenance of the .gov registry, and the scope and cost of post-market surveillance activities.

Second, CTIA provides input on the criteria for Cybersecurity Label Administrator ("CLA") selection, with the goal of promoting efficient identification of qualified candidates. The Bureau should require relevant experience but avoid unnecessary delay and expense by taking a flexible approach with respect to ISO/IEC 17065 accreditation requirements for CLAs. While ISO/IEC accreditation can be a helpful metric for organizations with limited practical experience, it can be costly and time-consuming to obtain and is unnecessary for prospective CLAs that have demonstrated track records in managing similar certification programs.

[5] Comments of CTIA, PS Docket No. 23-239 (filed Oct. 6, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10061240505270; Reply Comments of CTIA, PS Docket No. 23-239 (filed Nov. 10, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/111093246368.

[6] *Cybersecurity Labeling for Internet of Things*, PS Docket No. 23-239, Report and Order and Further Notice of Proposed Rulemaking, FCC 24-26 (rel. Mar. 15, 2024) ("Order").

II. THE GOVERNMENT SHOULD CLEARLY IDENTIFY FUNDING SOURCES FOR VITAL ELEMENTS OF THE IOT CYBER TRUST MARK INITIATIVE.

A. Consumer Education Will Be Essential and Requires Substantial Resources that Should Be Provided by the Federal Government.

Consumer education about the Cyber Trust Mark is critically important. As the Commission has recognized, a "robust consumer education campaign" is essential to make the Mark program effective.[7] This campaign needs to involve "manufacturers, retailers, industry, and non-profit groups," as well as other federal agencies.[8] As the Commission recognizes in the Order, "adequate consumer education must inform consumers of the limitations of the Mark as well as the benefits of having a product that meets baseline cybersecurity requirements."[9] It is therefore important that the consumer education campaign be designed and executed in a thoughtful manner to ensure that labeling and certification marks provide sufficient information to empower consumers to make informed decisions.[10] This effort will require significant resources, which the federal government is in the best position to provide.

The Order recognizes that retailers are among the stakeholders that must play an important role in consumer education.[11] As a key interface between a customer and

[7] Order ¶ 138.

[8] *Id.* ¶¶ 137-38 (naming federal agencies that should be involved in the consumer education campaign, such as the Department of Homeland Security, the Federal Bureau of Investigation, the Federal Trade Commission, and the Consumer Product Safety Commission).

[9] *Id.* ¶ 138.

[10] *See* Caven et. al., *Comparing the Use and Usefulness of Four IoT Security Labels,* CHI '24: Proceedings of the CHI Conference on Human Factors in Computing Systems, Honolulu, HI, May 2024 (2024), https://dl.acm.org/doi/fullHtml/10.1145/3613904.3642951 ("security labels should strive for clarity and relevance").

[11] Order ¶ 138 ("[T]he success of the IoT Labeling Program would require a robust consumer education campaign involving a collaboration with manufacturers, *retailers*, industry, and non-

manufacturer, and the channel through which specific information may be most easily conveyed at the point of sale, retailers will play a large role in determining whether a Mark education campaign succeeds. It is important to recognize that support and buy-in from major retailers in various categories will be key to program adoption, which is closely related to consumer understanding about the value of the Mark. These retailers include "big-box" retailers, consumer electronics retailers, and online retailers and e-commerce sites. However, retailers cannot and should not bear primary responsibility for conducting the sort of consumer education campaign that is essential for the success of the Program.

Creating and sharing a coordinated, consistent message about the value, importance, and meaning of the Mark and successful testing of that messaging will also be key. The Order gives the Lead Administrator primary responsibility for developing a consumer education plan, to be submitted to the Bureau for its approval.[12] However, the Order does not address how the Lead Administrator may be empowered or expected to fund education efforts.

The Commission and Bureau should not assume that the Lead Administrator can simply pass costs through to CLAs, since CLA organizations' plans to monetize their CLA role may not permit them to fund a successful consumer education program. For example, if CLAs are expected to recoup substantial program costs through fees for certifications, it is likely that prospective CLA applicants will be discouraged from participating in the program. High certification fees could lead to a vicious cycle in which the certification applicant pool decreases, causing per-application costs to rise. To succeed, resources for consumer education and

profit groups to promote the label and explain to consumers what the label means.") (emphasis added).

[12] *Id.* ¶ 137.

promotional support for the program should not be dependent on program participants. Rather, we strongly encourage the FCC to work with other government stakeholders to ensure these efforts are federally funded.

The Energy Star program provides a good example of how federal funding can ensure an effective program with strong industry uptake. Both the FCC and the Administration have pointed to Energy Star as a model when discussing how to structure the Mark program.[13] The Energy Star program was sponsored by the Environmental Protection Agency ("EPA") and the Department of Energy ("DOE") under Congressional mandate with federal funding.[14] As the program grew over the past thirty years, various consumer product categories were included.[15] Over this same period, the federal government has placed significant emphasis on education and allocated tax dollars to encourage the use of Energy Star program standards, tasking a federal agency with managing the program and the associated brand in the consumer marketplace. [16]

[13] The White House, *FACT SHEET: President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks* (May 12, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/ (The Executive Order "creates a pilot program to create an 'energy star' type of label."); FCC, *Fact Sheet: Securing Smart Devices*, at 1 (rel. Aug. 10, 2023), https://docs.fcc.gov/public/attachments/DOC-395909A1.pdf ("Just like the "Energy Star" logo helps consumers know what devices are energy efficient, the Cyber Trust Mark will help consumers make more informed purchasing decisions about device privacy and security.")

[14] *See, e.g.*, 10 C.F.R. pt. 430; 42 U.S.C. §§ 6291-6309.

[15] EPA Energy Star, *Joint EPA and DOE Report to Congress on the 2009 ENERGY STAR Memorandum of Understanding with a Focus on Home Appliances*, at 7 (Mar. 2022), https://www.energystar.gov/sites/default/files/asset/document/EPA%20Energy%20Star%20Report%20to%20Congress_FINAL_3-30-2022.pdf ("2022 Joint Energy Star Report to Congress").

[16] *Id*. at 7 n. 11 ("As brand manager, EPA is responsible for protecting the ENERGY STAR trademark and enhancing its effectiveness in the consumer market. Activities are undertaken to increase awareness, understanding, loyalty, and its effect on behavior change.")

With the benefit of federal government coordination and funding, the Energy Star program helps partners participate in national campaigns with coordinated messaging and materials, and it provides partners with toolkits to foster participation in promotions which include information about how to participate, sample media posts, social graphics, and web banners.[17] Energy Star provides toolkits to help partners with their consumer outreach on certified products[18] with substantial and sophisticated materials such as brochures and videos, as well as online resources for consumers to find eligible products. EPA and DOE explain the agencies' investment in consumer awareness: they "[l]aunched a sophisticated, consumer-oriented ENERGY STAR Product Finder tool that leveraged a single, integrated database of product testing results; and [i]mproved ENERGY STAR brand management by introducing a more effective consumer education strategy integrated across all product categories and coordinated nationally throughout the year."[19]

A federal funding model like that for the Energy Star program is the best approach for addressing costs related to consumer education under the Cyber IoT Labeling Program. Federal funding has also been used for education and outreach about FCC and FCC-related programs. For example, the Commission recognized the critical need for consumer education in implementing the Affordable Connectivity Program ("ACP"), noting that "to achieve the

[17] EPA Energy Star, *Marketing Toolkit*, https://www.energystar.gov/saveathome/improvements/professionals/marketing-toolkit (last visited Aug. 19, 2024); EPA Energy Star, *Marketing Tools and Campaigns*, https://www.energystar.gov/partner-resources/utilities-eeps/market-tools-camps (last visited Aug. 19, 2024).

[18] *See* EPA Energy Star, *ENERGY STAR Marketing Materials for Products*, https://www.energystar.gov/products/tools_resources (last visited Aug. 19, 2024).

[19] 2022 Joint Energy Star Report to Congress at 4.

program's full potential and reach as many eligible households as possible, households must be clearly informed of the program's existence, benefits, and eligibility qualifications, and how to apply."[20] To accomplish that objective, the FCC used federal funds to set up an Outreach Grant Program, which sought "to enlist partners around the country to help inform ACP-eligible households about the program in their local communities, and to provide those partners with the funding and resources needed to increase participation among those Americans most in need of affordable connectivity."[21] The digital television transition also benefitted from federal funding for education efforts, and from federal coordination of messaging for consumer education.[22]

Of course, Congressional authorization may be required in order to secure adequate federal funding. But other potential sources of federal funding are available, like the Department of Homeland Security Cybersecurity and Infrastructure Security Agency ("DHS/CISA"). For example, DHS/CISA's "Secure Our World" program could be a natural funding source for the IoT Cyber Labeling program.[23] Secure Our World has relevant subject matter expertise and experience providing resources for consumer education and could be expanded to include information about the Mark and the IoT Cyber Labeling program.

[20] *In the Matter of Affordable Connectivity Program,* Second Report and Order, 39 FCC Rcd 9928, ¶ 2 (rel. Aug. 8, 2022).

[21] *Ibid.*

[22] *See, e.g., Outside the Box: The Digital TV Converter Coupon Program*, National Telecommunications and Information Administration, at 14-15 (Dec. 2009), https://www.ntia.gov/sites/default/files/publications/dtvreport_outsidethebox_0.pdf.

[23] CISA, *Secure Our World,* https://www.cisa.gov/secure-our-world (last visited Aug. 19, 2024).

B. The Bureau Should Clarify the Costs of Creating and Maintaining the IoT Registry to Minimize Regulatory Burdens.

The Order envisions that there will be a single registry of products that have received approval to use the FCC IoT Label.[24] While this registry will increase consumer access to information, it also will impose operational burdens and costs. The Bureau should clarify that CLAs will not be responsible for bearing those costs and refrain from including data fields in the registry that go beyond the focus of IoT security and NIST Internal Report ("NISTIR") 8425, to which the program is designed to align.[25]

The Order states that as part of the program, the FCC will "require information about how to operate the device securely, including information about how to change the password, as it would help consumers understand the cybersecurity features of the products, how those products are updated or otherwise maintained by the manufacturer, and the consumer's role in maintaining the cybersecurity of the product."[26] The Commission heeded commenters' concerns about complexity and decided prudently to pursue a "modest," "decentralized, API-driven registry," while leaving open options to expand in the future.[27]

[24] Order ¶ 111.

[25] *Id* ¶ 9 ("NIST's essential work . . . provide[s] the building blocks for our development and adoption of this IoT Labeling Program.")

[26] *Id*. ¶ 115.

[27] *Id*. ¶ 116 ("[T]he decentralized, API-driven registry we adopt today addresses the complexity concerns raised in the record. We cabin our initial vision of the registry and direct the Bureau, as described further below, to consider ways to make the initial design of the registry modest, with potential to scale the registry as the IoT Labeling Program grows.").

The Order determined that "the Lead Administrator is in the best position to interface with manufacturers to ensure the smooth operation of the registry."[28] The Commission agreed that it should use a third party to host and manage the registry due to the resources required to establish the registry.[29] It "direct[ed] the Lead Administrator to receive and address any technical issues that arise in connection with" the registry's API and displaying information from the registry to the consumer when they present the QR Code.[30] Details about obligations and costs to establish and maintain the registry were left open in the Order, which "direct[ed] the Bureau to seek comment and consider, as part of a public process, the technical details involved with the operation of the registry."[31]

Accordingly, Section J of the Notice asks a variety of questions about the "publicly available registry containing information supplied by entities authorized to use the FCC IoT Label."[32] Among other things, the Notice seeks comment on the Order's conclusion that "the 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 design" and would be aggregated into a landing page with a .gov domain.[33] The Notice then asks about who "should be responsible for

[28] *Id.* ¶ 120.

[29] *Ibid.*

[30] *Ibid.*

[31] *Id.* ¶ 121.

[32] Notice ¶¶ 20-24.

[33] *Id.* ¶ 22.

hosting this landing page. Is the Lead Administrator in the best position to host the landing page? What additional costs are involved with this responsibility?"[34]

CTIA offers the following suggestions:

- If the FCC is planning to build a registry with a .gov domain, it should consult with industry to specify the interface, tools, and approaches to maintain integrity and security of the registry and maximize its ease of use for consumers.
- The role of CLAs in the maintenance and operation of the registry is not clear, but logically, a CLA's role should be minimal compared to the Lead Administrator and manufacturers. For example, to the extent the .gov registry is treated as an information system operated on behalf of the government to which Federal Information Security Management Act ("FISMA") requirements might apply, an issue raised in the Notice,[35] no such obligations should apply to private parties providing data to the registry or to CLAs that may be able to validate registry data. CLAs should have no FISMA obligations.
- The Lead Administrator should be responsible for selecting the registry that it will develop and maintain.
- Manufacturers should remain responsible for and bear the costs of populating the registry and updating or expanding the information contained in it.

In response to the Notice, the Bureau should clarify the limited role of CLAs with respect to the creation, population and maintenance of the registry and make clear that CLAs will not be responsible for or expected to bear possible additional costs that may be involved in developing and maintaining the registry, either initially or as the program develops.

The Notice also asks about data fields that should be included in the registry, such as whether manufacturers should "be required to list the sensors contained in the complying product, such as cameras, microphones, and location tracking devices? Should manufacturers be required to disclose what data is collected by those sensors, and whether that data is shared with third

[34] *Id.* ¶ 24.

[35] *Id.* ¶ 19.

parties?"[36] In order to help ensure the success of the program, the Bureau should take care that the data included in the registry stays focused on security issues directly relevant to the Cyber Trust Mark, rather than adding information that may be relevant to other policy objectives. The Bureau should not mandate that information of this type be included in the registry, because doing so is outside the scope of issues being addressed by the Cyber Trust Mark and is not aligned with NISTIR 8425.

C. Post-Market Surveillance Obligations Should be Clear and Tailored to Avoid Extensive Additional Costs that May Discourage Participation by CLAs or Manufacturers.

The Order directs the Lead Administrator to "identify or develop, and recommend to the Commission for approval, the . . . activities and procedures that CLAs will use for performing post-market surveillance."[37] That includes "specific requirements such as the number and types of samples that a CLA must test and the requirement that grantees submit, upon request by PSHSB or a CLA, a sample directly to the CLA to be evaluated for compliance at random or as needed."[38] As a result, the Notice does not ask specific questions about post-market surveillance, because the Order left it to the Lead Administrator to specify post-market surveillance expectations**.**

CTIA believes that clearly defining the post-market surveillance program is critical to ensuring the program's success, because the costs of post-market surveillance obligations may be substantial obstacles to broad participation by CLAs. As the Bureau proceeds, it should emphasize and clarify that the Lead Administrator's approach should provide clarity and use a

[36] *Id.* ¶ 21.

[37] Order ¶ 128.

[38] *Ibid.*

tailored approach that minimizes operational costs for CLAs for post-market surveillance. If post-market surveillance costs are significant or uncertain, this will increase the costs that CLAs must pass on to participating manufacturers. Doing so could make the costs of obtaining the Mark unattractive, thereby dampening participation in the program, in the same way that imposing education costs on participants could jeopardize the program's success.

Thus, the Bureau should recommit to the idea that the Lead Administrator should set clear guidelines for post-market surveillance, which expressly set the number of samples and frequency of tests. That includes both the periodicity and thresholds for any surveillance actions. These requirements should balance the need for surveillance with minimizing operational costs on CLAs.

Moreover, post-market surveillance costs cannot be determined with specificity until the Commission approves the Lead Administrator and CLAs, and these organizations are able to collaborate to develop the post-market surveillance process. Therefore, the Commission should encourage the Lead Administrator to impose modest obligations that do not increase up-front application costs. One option would be to have manufacturers of products pay for the testing for post-market surveillance separately from any application fees. This would keep application costs lower and reduce potential barriers to program participation—a matter of particular importance to smaller manufacturers for whom the costs of initial and follow-up testing can be substantial.

Whether or not a manufacturer pays for post-market surveillance separate from application fees, CLA obligations should be minimal and clearly described. The complaint process described in the Notice[39] should not impose ongoing obligations on CLAs generally to police compliance with the criteria for use of the Mark, and the Commission should clearly state

[39] Notice ¶ 16.

that CLAs cannot be held responsible for a manufacturer's misuse of the Mark, including by virtue of a product that qualified for the Mark but then became ineligible or had a product fall out of compliance. Clarifying these points would remove potential cost and liability concerns that may limit organizations' interest in serving as a CLA.

III. THE COMMISSION SHOULD ESTABLISH CLA SELECTION CRITERIA THAT PRIORITIZE EXPERIENCE AND EFFICIENCY AND REFRAIN FROM ADOPTING UNNECESSARY REQUIREMENTS THAT MAY LIMIT THE POOL OF CLA APPLICATIONS

The Bureau "seeks comment on whether there are additional areas of expertise or specific requirements a CLA applicant should be required to demonstrate in addition to those listed in the Order."[40] The Notice lays out detailed requirements for the review of CLA applications and the fees associated with the application,[41] including a requirement for CLAs to obtain ISO/IEC 17065 accreditation.[42] To help ensure the success of the Cyber IoT Labeling program and avoid implementation delays, CTIA encourages the FCC to focus on organizations with a proven track record of certification when selecting CLAs, and adopt a flexible approach if it proceeds with an ISO/IEC 17065 accreditation requirement.

Based on CTIA's own experience with establishing and running certification programs,[43] CTIA proposes the following criteria to allow CLAs to begin issuing certifications quickly and competently:

[40] Notice ¶ 11.

[41] *Id.* ¶¶ 2-10.

[42] *Id.* ¶ 6.

[43] *See* CTIA Certification, *Device Certification Programs*, https://ctiacertification.org/device-certification-programs/ (last visited Aug. 19, 2024).

First, a prospective CLA should have a minimum of five to ten years of experience managing a cyber certification program. Approving CLAs that do not have such experience administering an existing certification program could delay the Mark program, while requiring at least five to ten years provides a sufficient period for an entity to demonstrate the capability to execute a successful program.

Second, a prospective CLA should have proven experience in running or participating in a working group on cybersecurity standards. This experience will be essential in interfacing with and supporting the Lead Administrator in defining requirements and testing procedures.

Third, for entities with at least five to ten years of experience running certification programs, the ISO/IEC 17065 accreditation should be optional. The purpose of ISO/IEC 17065 accreditation is to ensure competence, consistent operation, and impartiality of a certification body in performing compliance verification for products, processes, and services. CLA candidates that have substantial experience—e.g., at least five to ten years—managing successful certification programs will have already demonstrated these attributes and should not be required to go through the process of obtaining ISO/IEC 17065 accreditation, which can be costly and time-consuming.

Requiring all CLA candidates to go through the ISO/IEC 17065 accreditation process would unnecessarily increase costs and introduce potential new burdens. For example, obtaining ISO/IEC 17065 accreditation could require CLA applicants to amend foundational documents, adopt new or amended operating policies and procedures, produce new or revised documents, and undergo audits—all of which could introduce costs beyond the application fee. There is no reason to impose these costs and burdens on entities that have a proven a track record running certification programs. However, to the extent the Commission wants extra assurance about the capabilities of an organization with less experience running its own program, it may be reasonable to require ISO/IEC 17065 accreditation if the organization has less than five to ten years of experience in managing a certification program. To the extent the Commission believes ISO/IEC 17065 accreditation remains important for all CLAs, an 18-month grace period should be available to entities that have a proven track record of successfully managing a certification program.

Separately, CTIA agrees that a different accreditation, ISO/IEC 17025, "General Requirements for the Competence of Testing and Calibration Laboratories,"[44] is appropriate for the Cybersecurity Testing Laboratories ("CyberLABs"). The Commission is right to expect that the CyberLABs that will themselves be conducting testing and review of products should have this accreditation.[45] CTIA's own certification program, for example, requires CTIA Certification Authorized Test Labs to have accreditation under ISO/IEC 17025, with the scope of accreditation matching the scope of certification testing the test lab is authorized to conduct.[46]

Finally, CTIA agrees with the Bureau's tentative conclusion that manufacturer applications submitted to the CLA should be confidential, and that CLAs should maintain this confidentiality.[47] The Bureau is correct that these applications will contain a variety of

[44] International Organization for Standardization, ISO/IEC 17025:2017(E), General requirements for the competence of testing and calibration laboratories (3d ed. 2017).

[45] Order ¶ 67 ("[W]e are persuaded that it is appropriate to recognize testing labs that have been accredited to ISO/IEC 17025 standards to conduct compliance testing that would support an application for authority to affix the FCC IoT Label.").

[46] CTIA Certification, Policies and Procedures for Authorized Test Lab Version 1.16, at 6 (May 2024), https://ctiacertification.org/wp-content/uploads/2024/05/CTIA-Certification-Policies-and-Procedures-for-ATLs-Ver-1.16.pdf.

[47] Notice ¶ 17.

information that is customarily treated as proprietary and confidential. It would discourage participation in the Cyber Trust Mark program if these applications were publicly available, and there is no countervailing reason to make them public.

IV. CONCLUSION

As the Commission moves to implement the operational details of this important program, CTIA encourages the Commission to seek federal funding for promoting the Mark, limit the burden on potential CLAs by reducing unnecessary costs and tailoring post-market surveillance responsibilities, and prioritize experience in determining CLA selection criteria. CTIA welcomes further engagement with the Commission as we support next steps to operationalize the program.

/s/ David Valdez
David Valdez
Vice President, Privacy and Cybersecurity

Umair Javed
Senior Vice President and General Counsel

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

Justin Perkins
Director, Cybersecurity and Policy

Mike Beirne
Director, Regulatory Affairs

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200