**Before the Department of Commerce**
**National Institute of Standards and Technology**
**Washington, D.C.**

In The Matter of

| | | |
|---|---|---|
| *Draft Baseline Security Criteria for Consumer Software Cybersecurity Labeling* | ) | Draft NIST Cybersecurity White Paper |
| *Consumer Cybersecurity Labeling for IoT Products: Discussion Draft on the Path Forward* | ) | NIST Cybersecurity Discussion Draft |

# COMMENTS OF CTIA


Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

Melanie K. Tiano
Assistant Vice President, Cybersecurity and Privacy

Avonne S. Bell
Director, Connected Life

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


December 16, 2021

## TABLE OF CONTENTS

## I. INTRODUCTION AND SUMMARY.

CTIA[1] welcomes the opportunity to provide feedback to the National Institute of Standards and Technology ("NIST") as it implements President Biden's Executive Order, *Improving the Nation's Cybersecurity* ("Cyber EO"),[2] specifically to initiate a consumer software security labeling pilot program ("Software Pilot Program") and a consumer Internet of Things ("IoT") device security labeling pilot program ("IoT Pilot Program," and, together with the Software Pilot Program, "Pilot Programs").[3] CTIA has engaged with NIST on workstreams under the Cyber EO, including NIST's White Paper on Draft Baseline Security Criteria for Consumer IoT Devices ("Draft IoT Security Criteria")[4] and the second draft of NIST's publication on Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations,[5] and is pleased to continue to collaborate with NIST.

The Cyber EO directs NIST—in consultation with other agencies as appropriate—to initiate Pilot Programs to educate the public on IoT device security and software development

[1] CTIA® (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st-century connected life. The association's members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry, and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[2] Exec. Order No. 14,028, 86 Fed. Reg. 26,633 (May 17, 2021) ("*Cyber EO*").

[3] *Id.* at 26,640.

[4] Comments of CTIA, NIST's Draft Baseline Security Criteria for Consumer IoT Devices (Oct. 18, 2021), https://www.nist.gov/system/files/documents/2021/10/29/28-20211018%20-%20Comments%20re%20NIST%20IoT%20Baseline%20Security%20Criteria%20for%20IoT%20Labeling%20Pilot%20Program.pdf.

[5] Comments of CTIA, NIST's Draft (2nd) NIST SP 800-161 Rev. 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (Dec. 10, 2021).

security.[6] As part of the Software Pilot Program, NIST is directed to "identify secure software development practices or criteria," "examine all relevant information, labeling, and incentive programs, employ best practices," and, importantly, "focus on ease of use for consumers and a determination of what measures can be taken to maximize manufacturer participation."[7]

CTIA appreciates NIST's collaboration with stakeholders, including the workshops in September ("September Labeling Workshop")[8] and December ("December Labeling Workshop," and together with the September Labeling Workshop, "Labeling Workshops").[9] By releasing the White Paper on Draft Baseline Criteria for Consumer Software Cybersecurity Labeling ("Draft" or "White Paper"),[10] NIST is continuing to work with industry on the Software Pilot Program. In addition, NIST also recently released a discussion draft related to the IoT Pilot Program, *Consumer Cybersecurity Labeling for IoT Products: Discussion Draft on the Path Forward* ("IoT Discussion Draft").[11] Developing both Pilot Programs will be challenging, and

---

[6] *Cyber EO*, at 26,640.

[7] *Id.* at 26,640-41.

[8] *Workshop on Cybersecurity Labeling Programs for Consumers: Internet of Things (IoT) Devices and Software*, NIST (Sept. 14-15, 2021), https://www.nist.gov/news-events/events/2021/09/workshop-cybersecurity-labeling-programs-consumers-internet-things-iot ("*September Labeling Workshop*").

[9] *Cybersecurity Labeling for Consumer IoT and Software: Executive Order Update and Discussion*, NIST (Dec. 9, 2021), https://www.nist.gov/news-events/events/2021/12/cybersecurity-labeling-consumer-iot-and-software-executive-order-update ("*December Labeling Workshop*").

[10] DRAFT Baseline Security Criteria for Consumer Software Cybersecurity Labeling, NIST (Nov. 1, 2021), https://www.nist.gov/system/files/documents/2021/11/01/Draft%20Consumer%20Software%20Labeling.pdf ("*Draft*").

[11] *See* Consumer Cybersecurity Labeling for IoT Products: Discussion Draft on the Path Forward, at 2, NIST (Dec. 3, 2021) https://www.nist.gov/system/files/documents/2021/12/03/FINAL_Consumer_IoT_Label_Discussion_Paper_20211202.pdf ("*IoT Discussion Draft*"). CTIA discusses aspects of the IoT

NIST's experience and continued outreach to industry stakeholders will be critical.

Here, CTIA does not make specific suggestions about baseline technical criteria for consumer software labeling, but rather, CTIA files comments on the Draft because aspects of NIST's approach to consumer software labeling are similar to NIST's recently released IoT Discussion Draft.[12] For example, in both the White Paper and the IoT Discussion Draft, NIST proposes that a binary label is likely the most appropriate labeling approach for its Pilot Programs.[13] To that end, CTIA makes three primary recommendations for NIST to consider for its Pilot Programs.

*First*, NIST should not prematurely embrace a single conceptual approach to labeling—like "binary labels"—without more extensive research on consumer effectiveness and understanding of any particular kind of label. NIST has appropriately determined that its approach should avoid creating unnecessary consumer confusion and be based on thorough consumer testing of labels. Consistent with that determination, NIST should not presume that "binary labels" are the best approach without a rigorous evaluation of evidence—including substantial evidence developed in the specific context of cybersecurity labeling. Instead, NIST should design its Pilot Programs with the explicit goal of promoting and testing a variety of labeling approaches, which will help stakeholders better understand the benefits and risks of

---

Discussion Draft with these comments, and will additionally separately provide feedback to NIST on other aspects of the IoT Discussion Draft.

[12] *See IoT Discussion Draft*, at 2 (proposing that "[a] single binary label (a 'seal of approval' type of label indicating a product has met a baseline standard) is likely most appropriate, coupled with a layered approach that leads interested consumers to additional detail online.") CTIA's comments urging NIST to reconsider its proposal to endorse a binary label approach for the Software Pilot Program apply equally to NIST's more recent proposal to endorse a binary label approach for the IoT Pilot Program.

[13] *See Draft*, at 16-17("NIST proposes that a binary label is likely most appropriate."); *IoT Discussion Draft*, at 11 ("NIST proposes that a single binary label is likely most appropriate.").

various approaches and will encourage further innovation with respect to labeling across the software and IoT ecosystems. Indeed, NIST's Pilot Programs, which are voluntary and non-regulatory, are an ideal place to test different approaches and promote innovation generally in labeling without risk of creating a confusing patchwork of expectations that would result, for example, from a more regulatory approach across various jurisdictions.

*Second*, NIST should avoid suggesting that the same label design should apply to both Pilot Programs, as important differences between consumer software and consumer IoT devices may warrant different labeling approaches.

*Third*, NIST should revise the White Paper and other publications related to the Pilot Programs to discuss the significant litigation risk that is likely to result from industry participation in the labeling programs, and consider whether safe harbors that promote industry participation and predictable industry standards could be implemented.

## II. NIST SHOULD NOT PREJUDGE ONE LABELING APPROACH FOR ANY PILOT PROGRAMS.

### A. Cybersecurity Is Complex, Requiring Any Cybersecurity Labels to Be Rooted in Robust Testing and Research.

IoT security and software development security are both highly technical topics, and consumers have widely varying levels of cybersecurity sophistication. As a result, many if not most consumers are unfamiliar with detailed security information that may be provided about consumer IoT devices and consumer software. Robust consumer testing of any labeling program is therefore critical, including testing to determine what labeling *approaches* may be most appropriate, in addition to testing specific *design* and *consumer education materials*. While NIST's Draft has correctly highlighted the importance of consumer testing of label design and consumer education materials, it should also recognize and emphasize the importance of testing to inform labeling *approaches*.

NIST is right to recognize the importance of testing label design and consumer education materials, as consumer understanding is the key element of any labeling approach. The White Paper establishes as one of its Labeling Criteria that "the software provider is using a label that has undergone rigorous consumer testing to ensure its usability."[14] NIST also includes guidance about consumer testing, explaining that "selected label designs and consumer education materials should undergo rigorous consumer testing prior to launching a labeling program."[15] CTIA agrees that extensive consumer testing must be an integral element of the Pilot Programs, as the consumer IoT device and consumer software labels will attempt to convey highly technical and complex information to consumers that have varying levels of cybersecurity knowledge and sophistication.

This focus on consumer testing is also consistent with FTC guidance. An FTC representative at the September Labeling Workshop noted that the FTC has determined that the most effective consumer labels are those that have been tested on consumers.[16] Indeed, the FTC regularly emphasizes the importance of consumer testing and has made clear that it will hold companies liable for making claims that it views as misleading about security.[17] Moreover, according to the FTC, "[a]dvertisers are responsible for ensuring that all express and implied claims that an ad conveys to reasonable consumers are truthful and substantiated."[18] As a result,

---

[14] *Draft*, at 11.

[15] *Id*. at 21.

[16] *September Labeling Workshop.*

[17] *See., e.g.*, D-Link Agrees to Make Security Enhancements to Settle FTC Litigation, Press Release, FTC (July 2, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/d-link-agrees-make-security-enhancements-settle-ftc-litigation.

[18] .com Disclosures: How to Make Effective Disclosures in Digital Advertising, at 5, FTC (Mar. 2013), https://www.ftc.gov/system/files/documents/plain-language/bus41-dot-com-disclosures-information-about-online-advertising.pdf.

"[c]opy tests or other evidence of how consumers actually interpret an ad can be valuable."[19]

However, CTIA is concerned that NIST's White Paper and recent IoT Discussion Draft do not apply this perceptive analysis of the importance of testing to overall labeling approaches. Just as rigorous consumer testing of label designs and education materials is integral to "determin[ing] a label's appropriateness,"[20] so too is testing of an earlier, fundamental decision in any labeling program: the general labeling approach. NIST recognizes that there are multiple label "types," including descriptive labels, binary labels, and graded labels,[21] and recognizes that "[a]ll labeling approaches have their strengths and weaknesses."[22] Nevertheless, NIST "proposes that a *binary label* is likely most appropriate" for the Software Pilot Program, and puts forward a similar proposal for the IoT Pilot Program; under both proposals, NIST also suggests that binary labels may be coupled with a layered approach.[23] As discussed further below, given the lack of cybersecurity-specific consumer testing on this point, CTIA believes these proposals should be reconsidered and the Pilot Programs should test labeling approaches more broadly.

In particular, NIST should encourage consumer testing at every stage of development of a labeling program, not just the design phase. Given the value of consumer understanding as a touchstone for effective labeling, it is important for NIST to recognize the critical role that consumer testing plays during the approach phase. Instead of its current focus on binary labels, NIST should design its Pilot Programs with the goal of promoting and testing a variety of labeling approaches across the software and IoT ecosystems. This will allow the Pilot Programs

---

[19] *Id*. at 5, n.14.

[20] *Draft*, at 21.

[21] *Id.* at 16.

[22] *Id.* NIST makes a similar statement in the IoT Discussion Draft. *IoT Discussion Draft*, at 11.

[23] *See Draft*, at 16-17. *IoT Discussion Draft*, at 2, 11.

themselves to contribute to the robust testing that is needed for a meaningful and effective labeling program, and it will ultimately help stakeholders better understand the benefits and risks of various labeling approaches. What is more, it will provide these benefits under the voluntary and non-regulatory Pilot Programs, which will avoid the risk of a confusing patchwork of different approaches across various state, federal, and international jurisdictions that would result from a more regulatory approach. A broader focus on all labeling approaches is also consistent with NIST's well-established position that it is not designing its own label nor establishing its own labeling program,[24] and would help ensure that the Pilot Programs will "focus on ease of use for consumers," as directed by the Cyber EO.[25]

In any case, NIST should clearly state its goals for the Pilot Programs, clarifying that neither Pilot Program is intended to establish a standard for consumer software or IoT labeling outside of the Pilot Programs and that the Pilot Programs can serve to accelerate innovation across the software and IoT markets with respect to labeling. CTIA is encouraged by language in the IoT Discussion Draft describing that the IoT Pilot Program "will specify desired outcomes, allowing providers and customers to choose best solutions for their devices and environments."[26] NIST notes that one benefit of an outcome-based approach is that it "[a]llows for a vibrant IoT product conformity and labeling landscape because the outcome-based criteria can be mapped to existing conformity assessment approaches. They also can be used in the final implementation of new, and potentially broader, labeling schemes."[27] CTIA agrees with the laudable goals of the IoT Pilot Program that NIST seeks to achieve by establishing outcome-based baseline security

[24] *Draft*, at 3; *IoT Discussion Draft*, at 1.

[25] *Cyber EO*, at 26,640-41.

[26] *IoT Discussion Draft*, at 1.

[27] *Id.* at 18.

criteria and urges NIST to apply this same approach, driven by the same goals, in establishing the parameters of the labeling approach to be used under the Pilot Programs.

### B. NIST Should Not Endorse Binary Labels as a One-Size-Fits-All Approach for Its Pilot Programs.

Given the diversity of the consumer software and consumer IoT ecosystems, there is not one label type that is universally most appropriate for *all* consumer software or consumer IoT labeling programs. NIST already recognizes that "[t]here is no one-size-fits-all definition for cybersecurity that can be applied to all types of consumer software. The risk associated with software is tightly bound to that software's intended use (both in function and operating environment), as well as its post deployment configuration. The cybersecurity considerations appropriate for a mobile game will differ from those applied to an online banking app or to run the media station on an automobile."[28] This same concept applies equally to a label that conveys cybersecurity information about software or IoT devices. Given the complexity and diversity in the software and IoT ecosystems, it may be the case that different label types are most appropriate in different contexts. To that end, NIST should promote a more flexible and risk-based approach to labeling under its Pilot Programs instead of endorsing a binary label.

Even assuming that one labeling approach can eventually be found to be most appropriate for software or IoT labeling, extensive consumer testing—beyond the limited studies that NIST briefly summarizes in the White Paper[29] and the IoT Discussion Draft[30]—is required to support such a determination. However, NIST's current proposal is based on a view of labeling approach options that is overly simplified for purposes of the Pilot Programs. For example, the

[28] *Draft*, at 2.

[29] *Id.* at 17-18.

[30] *IoT Discussion Draft*, at 21-24.

White Paper weighs its proposed binary approach against two alternatives (descriptive labels and graded labels) and concludes that the binary approach is preferable.[31] In the IoT Discussion Draft, NIST draws a similar high-level conclusion.[32] At this stage, however, NIST does not need to lock the Pilot Programs into a certain approach for communicating information to consumers. While the other approaches certainly have potential downsides, there may be creative and effective solutions that are not so easily categorized. Informed market-based analysis—fueled by consumer research and creative solutions that NIST and others have not yet evaluated—should drive decisions. As noted above, the Pilot Programs can encourage innovation in labeling approaches rather than endorse a single approach.

Moreover, there are legitimate concerns about using binary labels to convey complex cybersecurity information that is inherently fluid or variable, and fundamentally different from measurable outputs like energy efficiency. NIST is right to discuss the potential limitations of binary labels, including that they can create a false sense of security in consumers.[33] While NIST cites some evidence that consumers understand that labeled products are not entirely secure,[34] this evidence is too premature to reach a conclusion about consumer understanding of these types of labels. For example, NIST cites two studies for the proposition that consumers understand that labeled products are not entirely secure.[35] Participation in both of these studies

---

[31] *Draft*, at 16-17.

[32] *IoT Discussion Draft*, at 2, 11.

[33] *Draft*, at 18.

[34] *Id.*

[35] Consumer Internet of Things Security Labelling Survey Research Findings, Harris Interactive, at 4, (2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950429/Harris_Interactive_Consumer_IoT_Security_Labelling_Survey_Report_V2.pdf (*"Harris Interactive Study*"); Shane D. Johnson *et al.*, The Impact of IoT Security Labelling on

was limited to residents of the United Kingdom, so they may not be predictive of consumer behavior in the United States.[36] Moreover, neither of these studies' findings rebut the notion that consumers may still overestimate the security profile of a product based on the label. [37]

In proposing a binary label as the preferred approach, NIST's White Paper states that the ENERGY STAR program, which is a binary label, is "generally regarded as one of the most successful and recognizable government-administered programs."[38] However, the ENERGY STAR program's binary approach is not necessarily a good fit for conveying complex cybersecurity information.[39] Cybersecurity is a multi-faceted, nuanced concept that cannot be easily simplified to a binary, on-or-off label, unlike the quantitative nature of energy efficiency. Additionally, appliances with energy ratings are used in a more predictable and limited range of use cases, whereas IoT devices can be configured and deployed in a range of contexts that could potentially affect device security. Cybersecurity is also not static; rather, it is context-specific and is constantly evolving, requiring security vulnerabilities to be addressed over time through updates long after the device is manufactured.

The conclusion that a binary approach is most appropriate for all labeling oversimplifies the issue at this stage and creates a risk that consumers will be confused, as opposed to being

---

Consumer Product Choice and Willingness to Pay, PLoS ONE, at 8 (Jan. 24, 2020), https://journals.plos.org/plosone/article/file?id=10.1371/journal.pone.0227800&type=printable ("*Johnson Study*").

[36] *See Harris Interactive Study*, at 9; *Johnson Study*, at 13-15.

[37] *See Harris Interactive Study*, at 9; *Johnson Study*, at 13-15.

[38] *Draft*, at 15.

[39] In the IoT Discussion Draft, NIST acknowledges that "the cybersecurity context may differ from other common label contexts (e.g., food or energy), such as the unclear return on investment for cybersecurity and cybersecurity concepts typically being poorly understood and not easily relatable among the general public." This should counsel against recommending a binary approach without further study. *IoT Discussion Draft*, at 21.

assisted by an appropriate labeling approach. The Cyber EO directs NIST to "focus on ease of use for consumers" in carrying out both Pilot Programs.[40] As a result, NIST should ensure that the criteria are simple and digestible to the average consumer. But striking the right balance when trying to design a label is difficult, and it can be dependent on the context of the labeled product. An overly simplistic label can contribute to consumer misunderstanding that devices are 100% secure.[41] This has an impact not only on consumer choices, but also liability considerations for manufacturers that will face lawsuits and potential liability if consumers claim that labels inaccurately convey that devices are completely secure.

Given the stakes, this approach should be studied more and subjected to rigorous consumer testing. In short, NIST should not prejudge that a binary approach is the right approach or that it should be rigidly followed in the Pilot Programs.

## III. THERE ARE IMPORTANT DISTINCTIONS BETWEEN CONSUMER SOFTWARE AND CONSUMER IOT DEVICES, WHICH MAY CALL FOR DIFFERENT LABELING APPROACHES.

NIST asks "[w]hether the software label approach and design should be unique or extended to the IoT product label (also directed in the EO) to facilitate brand recognition, even though the technical criteria will be different."[42] Subsequently, as discussed above, the IoT Discussion Draft extended NIST's analysis and proposal with respect to a labeling approach

[40] *Cyber EO*, at 26,640-41.

[41] NIST concludes in the IoT Discussion Draft that "multiple variations of labeling approaches likely would cause confusion among consumers and limit the effectiveness of such efforts." *IoT Discussion Draft*, at 1. CTIA agrees that the Pilot Programs should actively work to avoid consumer confusion, and it encourages NIST to consider the risk of confusion associated with prematurely applying a binary label across the board under its Pilot Programs, without more robust research and testing.

[42] *Draft*, at 1.

under the Software Pilot Program to the IoT Pilot Program.[43] NIST should not automatically extend its work and approach with respect to software labeling to apply to IoT labeling, as these are two very different product markets.

NIST notes that the White Paper complements the Draft IoT Security Criteria,[44] and indeed, the principles and considerations that should drive NIST's work under the Software Pilot Program should apply equally to the IoT Pilot Program. For example, it is critical that both programs be voluntary, as established under the Cyber EO.[45] Both programs involve similar challenges in communicating complex and highly technical cybersecurity information in a digestible format to a wide range of consumers. Additionally, it is critical for both programs that NIST focuses on general criteria and desired outcomes. And NIST has made clear time and again—in this White Paper,[46] the Draft IoT Security Criteria,[47] and at the Labeling Workshops[48]—that it is neither establishing its own labeling programs nor designing its own labels, and is instead focusing on identifying desired outcomes. This is the right approach.

---

[43] *See IoT Discussion Draft*, at 2, 11.

[44] *Draft*, at 1.

[45] *See Cyber EO*, at 26,640-41 (directing NIST to make "a determination of what measures can be taken to maximize manufacturer participation" for both the Software Pilot Program and the IoT Pilot Program).

[46] *Draft*, at 3 ("NIST is not designing a particular label – nor is NIST establishing its own labeling program for consumer software. Rather, these criteria set out desired outcomes, allowing and enabling the marketplace of providers and consumers to make informed choices.").

[47] DRAFT Baseline Security Criteria for Consumer IoT Devices, NIST, at 1 (Aug. 31, 2021), https://www.nist.gov/system/files/documents/2021/08/31/IoT%20White%20Paper%20-%20Final%202021-08-31.pdf ("NIST will identify key elements of labeling programs in terms of minimum requirements and desirable attributes. Rather than establishing its own programs, NIST will specify desired outcomes, allowing providers and customers to choose the best solutions for their devices and environments. One size may not fit all, and multiple solutions might be offered by label providers.").

[48] *September Labeling Workshop*; *December Labeling Workshop*.

However, NIST should avoid extending the substantive approach for any consumer software label to any consumer IoT device label without independent testing showing that this is the right approach for these two product categories. Despite similarities between the Pilot Programs, there are important differences between consumer software and consumer IoT devices that may warrant approaching those labels differently. For example, consumer software and consumer IoT devices are two completely different categories of products that are marketed to different categories of consumers. NIST should not assume, without empirical evidence, that a particular label approach will effectively communicate cybersecurity information to consumers of software products as it will to consumers of IoT devices. The ecosystem of IoT devices is vast and diverse, ranging from low-cost and higher-risk consumer devices to devices with stronger security profiles. As NIST has noted, many IoT devices do not or cannot support a wide range of cybersecurity and privacy capabilities commonly found in other technological products.[49]

NIST should also not assume, without any evidence, that labels across software and IoT use cases are more effective if they appear to be visually similar—for "brand recognition"[50] or otherwise. The Draft implies that extending the same label approach and design to the Pilot Programs could "facilitate brand recognition."[51] This assessment is far too premature, and it does not recognize the difference in product markets for software and IoT devices. Additionally, NIST is not in a position at this point to objectively evaluate whether "brand recognition" of

[49] *See* NISTIR 8228, Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks, at 9, NIST (June 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf.

[50] *Draft*, at 1.

[51] *See id.*

labeling approaches across very different kinds of consumer products would be helpful or contribute to the overall effectiveness of the Pilot Programs. Any such assessment should be subject to consumer testing, while recognizing that the customer base for software and IoT may be so disparate that this is not a useful priority.

## IV. GIVEN THE WHITE PAPER'S RECOGNITION OF COMPLEXITIES WITH CONSUMER UNDERSTANDING, THERE ARE COMPELLING ARGUMENTS FOR SAFE HABORS TO PROMOTE INDUSTRY PARTICIPATION AND DEVELOP WORKABLE INDUSTRY STANDARDS.

The Cyber EO requires NIST, in evaluating consumer software and consumer IoT labeling proposals, to "consider ways to incentivize manufacturers and developers to participate in" the Pilot Programs.[52] NIST, in coordination with the FTC, is also directed to "focus on ease of use for consumers and a determination of what measures can be taken to maximize manufacturer participation."[53]

Cybersecurity labels can create significant liability risks for various stakeholders. For example, labeling creates litigation risks to manufacturers, developers, and certification bodies, flowing from the unique challenges in communicating complex cybersecurity information to consumers with varying levels of sophistication and cybersecurity knowledge. Indeed, the ENERGY STAR program and its labels have generated litigation, including private class actions.[54] This record deserves scrutiny for lessons learned that may inform liability risks and mitigations in the software and IoT labeling context. In the absence of liability protections, organizations may not want to assume the risk that consumers could misinterpret a label and

[52] *Cyber EO*, at 26,640.

[53] *Id.* at 26,640-41.

[54] *See, e.g., Dzielak v. Whirlpool Corp.*, 120 F. Supp. 3d 409 (D.N.J. 2015); *Pargett v. Wal-Mart Stores, Inc.*, 2020 WL 5028317 (C.D. Cal. Apr. 10, 2020).

bring a lawsuit.

To fulfill its mandate under the Cyber EO to incentivize participation from manufacturers and developers, NIST should revise its White Paper and other publications related to the Pilot Programs to acknowledge the significant litigation risk that is created through participation in the Pilot Programs. NIST can acknowledge that these concerns are not merely hypothetical—and that they could pose a significant barrier to robust industry participation in the Pilot Programs—without taking a position on the propriety or legitimacy of consumer litigation over product labeling.

Liability protections such as safe harbors would provide significant value to the Pilot Programs by driving greater industry participation and helping to establish predictability in practices throughout industry. In other contexts, safe harbors have been shown to encourage activities like carrier blocking of illegal and unwanted automated calls.[55] NIST should evaluate these examples and other models to see whether they could be applied to the Pilot Programs. In the IoT labeling context, CTIA has urged that at a minimum, helpful liability protections should apply to: (1) a manufacturer or developer that displays a label on its product; and (2) an organization that performs third-party certifications. Similar safe harbors should be considered for any software labeling.

In evaluating ways to encourage stakeholder participation in Pilot Programs, NIST should also consider encouraging the use of regulatory sandbox policies that other agencies have

[55] *See, e.g., Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Report and Order, and Notice of Proposed Rulemaking, 35 FCC Rcd. 7614, ¶ 3 (2020) (establishing a safe harbor from liability for the unintended or inadvertent blocking of wanted calls); *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Report and Order, 35 FCC Rcd. 15221, ¶ 13 (2020) (expanding the call blocking safe harbor to include network-based blocking).

successfully implemented to promote pro-consumer innovation while providing liability protections and greater regulatory certainty to industry. The Consumer Financial Protection Bureau, for example, has administered several programs designed to facilitate innovation in this manner, including a regulatory sandbox program.[56]

## V. CONCLUSION.

CTIA is pleased to continue its work with NIST to initiate the Pilot Programs pursuant to the Cyber EO. As NIST moves forward with both Pilot Programs, CTIA recommends that NIST: (1) avoid prematurely embracing a single conceptual approach to labeling without more extensive research on consumer effectiveness and understanding of the different types of labels; (2) recognize the differences between the two Pilot Programs and avoid suggesting that the same label approach and design should apply to both; and (3) revise the White Paper and other publications related to the Pilot Programs to discuss the significant litigation risk that is likely to result from participation in the Pilot Programs and consider implementing safe harbors that promote industry participation and predictable industry standards.

Respectfully submitted,

*/s/ Melanie K. Tiano*
Melanie K. Tiano
Assistant Vice President, Cybersecurity and Privacy

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

Avonne S. Bell
Director, Connected Life

[56] *Innovation at the Bureau*, Consumer Financial Protection Bureau, https://www.consumerfinance.gov/rules-policy/innovation/ (last visited Nov. 12, 2021).

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

www.ctia.org