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

In The Matter of

Draft Baseline Security Criteria for Consumer IoT Devices	)))	Draft NIST Cybersecurity White Paper

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

October 18, 2021

TABLE OF CONTENTS

I. INTRODUCTION AND SUMMARY

CTIA[1] welcomes the opportunity to continue working with the National Institute of Standards and Technology ("NIST") on Internet of Things ("IoT") cybersecurity as NIST begins fulfilling its charge under President Biden's Executive Order, *Improving the Nation's Cybersecurity* ("Cyber EO")[2] to explore a consumer IoT device security labeling pilot program ("Pilot Program"). NIST has been leading across the federal government and with industry on IoT security. CTIA has been proud to partner with NIST on the IoT Device Cybersecurity Capability Core Baseline ("NISTIR 8259A")[3] and the IoT Non-Technical Supporting Capability Core Baseline ("NISTIR 8259B"),[4] as well as NIST's study of IoT confidence mechanisms.[5]

President Biden was right to look to NIST to lead the Pilot Program**,** given NIST's work on IoT cybersecurity and its experience convening stakeholders from government and industry. The Cyber EO directs NIST—in consultation with other agencies as appropriate—to lead development of a Pilot Program to educate the public on IoT device security.[6] As part of the Pilot Program, NIST must "identify IoT cybersecurity criteria," "examine all relevant information, labeling, and incentive programs and employ best practices," and, importantly,

---

[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] NISTIR 8259A, IoT Device Cybersecurity Capability Core Baseline, NIST (May 2020), https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259A.pdf ("*NISTIR 8259A*").

[4] NISTIR 8259B, IoT Non-Technical Supporting Capability Core Baseline, NIST (Dec. 2020), https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259b-draft.pdf. ("*NISTIR 8259B*").

[5] *E.g.*, Draft NIST Cybersecurity White Paper, Establishing Confidence in IoT Security: How Do We Get There?, NIST (May 14, 2021), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.05142021-draft.pdf.

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

"focus on ease of use for consumers and a determination of what measures can be taken to maximize manufacturer participation."[7] Developing a Pilot Program will be difficult, and NIST's experience will be critical. NIST's White Paper on Draft Baseline Security Criteria for Consumer IoT Devices ("Draft Baseline Security Criteria" or "Draft")[8] starts a multi-step process to explore a Pilot Program, which will include baseline security criteria proposed in this Draft, as well as criteria for conformity assessments and labeling. Each step of this process must be rooted in risk management and flexibility and coordinated with industry.

CTIA has four primary suggestions for NIST to improve the baseline security criteria. It should: (1) clarify in the baseline security criteria that the Pilot Program is voluntary and focused on higher-risk consumer IoT devices, not conventional IT devices like smartphones, laptops, and tablets; (2) make clear that all criteria are not suitable for all devices, and consider tiers for baseline security criteria based on a range of devices with varying risk profiles and existing consensus-based approaches; (3) encourage voluntary use of flexible consensus baselines; and (4) simplify the baseline security criteria to provide more clarity and avoid consumer confusion**.**

Beyond baseline security criteria**,** as NIST considers conformity assessments and labeling, CTIA offers two suggestions. NIST should: (1) prioritize tools that are clear and helpful to consumers, supported by robust consumer testing to ensure that any label or information will avoid confusion; and (2) encourage policymakers to consider liability protections and safe harbors to encourage participation and promote predictable standards. Federal Trade Commission ("FTC") expertise and industry experience with consumer

---

[7] *Id.*

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

communications and labeling suggest these considerations will be important to any labeling program's success.

II. IOT SECURITY SHOULD BE PROMOTED THROUGH A VOLUNTARY, FLEXIBLE, AND RISK-BASED FEDERAL APPROACH, WHERE EACH PART OF THE COMPLEX ECOSYSTEM PLAYS A PART.

A. As Innovation Drives Explosive IoT Growth, Varied Government Efforts on Security Highlight the Need for a Unified, Federal Approach.

The IoT device market is growing rapidly, driving economic growth and providing substantial benefits to consumers. As NIST recognizes,[9] IoT innovation is affecting diverse sectors and improving the lives of consumers. As just a few examples, health IoT technology has facilitated the development of smart medication dispensers[10] and monitoring devices that help alleviate the need for opioids,[11] while in the vehicle space IoT is being facilitated by in-vehicle connectivity, resulting in the swift development of self-driving cars.[12] Not surprisingly, the IoT market is projected to reach $10B by 2025.[13]

In recent years, government agencies have shown interest in IoT security. In 2019, the Consumer Product Safety Commission ("CPSC") created an Interagency Working Group on

[9] Draft NISTIR 8259C, Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline, at 1, NIST (Dec. 2020), https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259c-draft.pdf ("[IoT] devices offer new functionality that can enhance the operations of government, commercial, and other enterprises and provide benefits to consumers and the general public").

[10] *E.g.*, Suganya G. et al., *IoT Based Automated Medicine Dispenser for Online Health Community Using Cloud*, 7 Int'l J Recent Tech & Eng'r 759 (Feb. 2019), https://www.ijrte.org/wp-content/uploads/papers/v7i5s4/E11570275S419.pdf.

[11] *E.g.*, Chris Penrose, *Technology Helps Battle the Opioid Crisis*, AT&T (Jan. 6, 2020), https://about.att.com/innovationblog/2020/01/technology_opioid.html (last visited Oct. 7, 2021).

[12] *See* Vivek Kumar, *Augmented Mobility: IoT is Redefining Autonomous Vehicles Landscape*, Analytics Insight (Feb. 14, 2021), https://www.analyticsinsight.net/augmented-mobility-iot-is-redefining-autonomous-vehicles-landscape (last visited Oct. 7, 2021).

[13] Adroit Market Research, *Internet of Things (IoT) Connectivity Market to Hit USD 10 Billion by 2025*, Yahoo Finance (May 25, 2021), https://finance.yahoo.com/news/internet-things-iot-connectivity-market-100400185.html (last visited Oct. 7, 2021).

Consumer Product Safety of Internet-Connected Products, which consists of the CPSC, the NIST National Cybersecurity Center of Excellence, and the FTC, among others.[14] The FTC has been active in oversight of IoT device security, bringing enforcement actions under Section 5 of the FTC Act,[15] publishing guidance,[16] and hosting workshops.[17] The Food and Drug Administration ("FDA") has engaged in efforts to address the security of connected medical devices.[18] The National Highway Traffic Safety Administration ("NHTSA") has published guidance detailing cybersecurity best practices for modern vehicles.[19] This year, the Federal Communications Commission ("FCC") has increased activity in security, releasing a Notice of Inquiry[20] seeking comment on its role in promoting IoT device security.

---

[14] Status Report on the Internet of Things (IoT) and Consumer Product Safety, at 17, CPSC (Sept. 25, 2019), https://www.cpsc.gov/s3fs-public/Status-Report-to-the-Commission-on-the-Internet-of-Things-and-Consumer-Product-Safety.pdf?6sv9HwTXKHrkdmAyAkQ0_TsKCkpl1lR2. The other agencies include the Food and Drug Administration, the Federal Communications Commission, the Department of Energy, and the Department of Homeland Security.

[15] *See* Privacy and Security Enforcement, FTC https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited Oct. 7, 2021).

[16] *See*, *e.g.*, Careful Connections: Keeping the Internet of Things Secure, FTC (Sept. 2020), https://www.ftc.gov/system/files/documents/plain-language/913a_careful_connections.pdf.

[17] *See*, *e.g.*, *Connected Cars: Privacy, Security Issues Related to Connected, Automated Vehicles*, FTC (June 28, 2017), https://www.ftc.gov/news-events/events-calendar/2017/06/connected-cars-privacy-security-issues-related-connected.

[18] *See*, *e.g.*, FDA Report on the Quality, Safety, and Effectiveness of Servicing of Medical Devices, FDA (May 2018), https://www.fda.gov/media/113431/download; Strengthening Cybersecurity Practices Associated with Servicing of Medical Devices: Challenges and Opportunities, FDA (June 2021), https://www.fda.gov/media/150144/download.

[19] Cybersecurity Best Practices for Modern Vehicles, NHTSA (Oct. 2016), https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/812333_cybersecurityformodernvehicles.pdf; Cybersecurity Best Practices for the Safety of Modern Vehicles: Draft 2020 Update, NHTSA (2020), https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/vehicle_cybersecurity_best_practices_01072021.pdf.

[20] *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program; Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program*, Notice of Proposed Rulemaking and Notice of Inquiry, 86 Fed. Reg. 46,644, 46,641 (June 17, 2021), https://docs.fcc.gov/public/attachments/fcc-21-73a1.pdf.

Moving forward, a coordinated federal approach for IoT is critical. Fragmentation, with agencies pursuing overlapping and perhaps inconsistent approaches, risks creating uncertainty and wasting resources. NIST—as a non-regulatory agency with deep experience in IoT—is suited to lead a comprehensive and unified approach that is voluntary, flexible, and risk-based.

B. The IoT Ecosystem Is Complex with Many Stakeholders Playing Important Roles in Security.

CTIA members prioritize IoT security. Given the massive growth in the IoT market, the private sector has a strong interest in securing IoT devices and protecting consumers. To that end, CTIA and other associations, standards development organizations, alliances, and coalitions that make up the Council to Secure the Digital Economy published the C2 Consensus on IoT Device Security Baseline Capabilities ("C2 Consensus").[21] This document established a set of recognized "device security capabilities that can be applied to all new IoT devices that connect to the internet" to aid industry's ongoing efforts to secure IoT devices.[22] Looking ahead, to better secure the IoT ecosystem, the full range of stakeholders (manufacturers, network operators, software and application developments, enterprise device managers, and consumers) must play a role. Any unified, federal approach to IoT security should not look to one set of actors in the ecosystem, but to the ecosystem as a whole.

[21] The C2 Consensus on IoT Device Security Baseline Capabilities, Council to Secure the Digital Economy (Sept. 2019), https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf.

[22] *Id.*

III. ANY PILOT PROGRAM SHOULD ALIGN WITH THE CYBER EO BY PROMOTING A VOLUNTARY AND RISK-BASED APPROACH THAT FOCUSES ON CONSUMER IOT DEVICES MOST IN NEED OF ENHANCED SECURITY.

The Cyber EO looks to develop a voluntary Pilot Program focused on critical cybersecurity risks. As a threshold matter, the Cyber EO tasks NIST to make "a determination of what measures can be taken to maximize manufacturer participation."[23] To promote effective industry participation in any future program, NIST at a minimum should clarify in its final baseline security criteria and all other work related to the Pilot Program that participation is purely voluntary.

Proper scoping can also increase the likelihood of private sector participation. *First,* NIST should focus on relatively less secure and higher-risk consumer devices, where increasing consumer awareness and security options may have the most impact. This means that NIST should not try to advance a labeling program that applies to all or even most IoT use cases. The Communications Sector for years has called for work to increase security of less-secure (often lower-cost) consumer devices, which can be used in distributed denial-of-service attacks. In the National Security Telecommunications Advisory Committee's ("NSTAC") 2017 Report to the President on Internet and Communications Resilience, industry made clear that "[d]evice manufacturers, particularly IoT device development kit manufacturers, need to assure good tools are included and use secure default configuration, automated patching, and the ability to recover from malware infections."[24] NSTAC also emphasized the importance of consumer awareness of

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

[24] NSTAC Report to the President on Internet and Communications Resilience, at 21, NSTAC (Nov. 16, 2017), https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20ICR%20FINAL%20%2810-12-17%29%20%281%29-%20508%20compliant_0.pdf.

basic security for connected devices, "including about the importance of completing updates."[25] NIST should scope a pilot program to focus on helping consumers manage inherently less-secure and unmanaged devices in order to have the most impact.

Second, NIST should not include in the scope of the Pilot Program conventional IT devices, like smartphones, laptops, or tablets. NIST has long treated consumer IoT devices as distinct from smartphones and other conventional IT devices. For example, NISTIR 8259 differentiates "IT devices," such as smartphones, laptops, and tablets, from IoT devices.[26] Similarly, the IoT Cybersecurity Improvement Act of 2020 excludes conventional IT devices from its definition of an IoT device.[27] The bill's legislative history makes clear that: "[w]e traditionally think of computing devices such as *computers, smartphones, and tablets* as our primary interface with the internet. These computing devices have securely designed, mature, and powerful operating systems. However, IoT devices normally have less computing power and, therefore, security capabilities than traditional computing devices."[28] This is sensible, because security protocols for smartphones and other IT devices are well-established, whereas many consumer IoT devices face challenges. For example, NIST has noted that "[m]any IoT devices do not or cannot support the range of cybersecurity and privacy capabilities typically built into conventional IT devices."[29] The scope of any Pilot Program should build on NIST's

[25] *Id.*

[26] NISTIR 8259, Foundational Cybersecurity Activities for IoT Device Manufacturers, at iv, NIST (May 2020), https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf.

[27] IoT Cybersecurity Improvement Act of 2020, Pub. L. No. 116-207, § 2(4)(A), 134 Stat. 1001 (2020).

[28] 166 Cong. Rec. H4353 (daily ed. Sept. 14, 2020) (statement of Rep. Keller) (emphasis added). *See also* H.R. Rep No. 116-501, at 13 (2020) ("Generally, IoT devices have lower computing power and lack mature security architecture found in widely used general purpose computing devices and network infrastructure, such as personal laptops, tablets, and routers.").

[29] 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. NIST has also identified that built-in cybersecurity capabilities for IoT devices are often "inadequate in terms of strength or performance" while "[p]ost-

approach and the IoT Cybersecurity Improvement Act, which NIST should make explicit in the final baseline security criteria and all other publications related to the Pilot Program.

IV. RISK MANAGEMENT MUST BE THE TOUCHSTONE OF ANY CONSUMER IOT LABELING PILOT PROGRAM.

A. In Order for the Pilot Program to Be Flexible and Risk-Based, NIST Should Adjust Some of its Criteria.

There is no one-size-fits-all cybersecurity solution in the vast and diverse IoT ecosystem—even within the consumer IoT device category. NIST should adjust some of its criteria to account for IoT diversity and to better promote a risk-based approach.

With respect to the Draft Baseline Security Criteria, NIST was right to leverage NISTIR 8259A and NISTIR 8259B as starting points. Those documents highlight the importance of flexibility and tailoring security to context. NIST establishes in NISTIR 8259A that its core baseline of security capabilities "does not specify how the device cybersecurity capabilities are to be achieved, so organizations . . . have considerable flexibility in implementing it to effectively address need" and that these capabilities "will often need to be added or removed from an IoT device's design, integration, or acquisition to best address an organization's common cybersecurity risks."[30] NIST explains in NISTIR 8259B that "[t]he individual non-technical supporting capabilities in the baseline may be implemented in full, in part, or not at all."[31]

---

market security capabilities cannot be installed onto many IoT devices" and that an IoT device may require "additional capabilities that most conventional IT devices do not use, especially if the IoT device enables new interactions with the physical world." *Id.* at 9-10.

[30] *NISTIR 8259A,* at 3.

[31] *NISTIR 8259B,* at 2.

However, some baseline security criteria in NIST's Draft appear to be prescriptive or are presented in a way that obscures how they may apply to consumer devices with diverse risk profiles. NIST's Draft states that "[t]hese are core baselines and need to be tailored (or profiled) for specific use cases or sectors. This profiling can involve editing the capabilities to address specific concerns as well as extensions or additions to the baseline capabilities and sub-capabilities"[32] NIST should bolster language about flexibility in the use of the baseline criteria and should structure the baseline tables to show how they may be applied flexibly in practice. This will show manufacturers that they can take a risk-based approach to IoT security design and still work within the pilot program.

First, NIST should explain that *all* of the criteria will not be appropriate for *all* consumer IoT devices. For example, encryption[33] is not appropriate—and would be overly burdensome—for many consumer IoT devices, as it hinders processor and battery performance in small and low-to-medium-complexity devices. Such devices, such as smart toasters, sprinkler systems, or GPS dog collars, would require complex capabilities if required to encrypt data at rest. There are more lightweight[34] ways to protect data, but NIST's explicit reference to "encryption with authentication" as part of the potential criteria for the data protection capability fails to account for the importance of these lightweight options for simpler, lower-risk devices.[35]

---

[32] *Draft,* at 1.

[33] *Id.* at 4 (listing as a potential criteria "[t]he ability to use demonstrably secure cryptography (e.g., modules consistent with FIPS 140-3) for cryptographic algorithms (e.g., encryption with authentication, cryptographic hashes, digital signature validation) to protect the confidentiality and integrity of all the product component's stored (e.g., collected and received data, internal software) and transmitted data. Note: available cryptographic modules maybe dependent on or limited by the *product component host*").

[34] *See NIST Issues First Call for 'Lightweight Cryptography' to Protect Small Electronics*, NIST (Apr. 18, 2018), https://www.nist.gov/news-events/news/2018/04/nist-issues-first-call-lightweight-cryptography-protect-small-electronics.

[35] *Draft,* at 4.

Similarly, event logging[36] is not an appropriate baseline for all IoT devices. The importance of event logging capabilities depends on context. While event logging is an important security element for a connected security camera, for example, it is unlikely to serve its intended purpose in a connected light bulb because the average consumer is unlikely to ever need to access security event data in that context. This comparison highlights the need for NIST to apply its flexible and risk-based approach throughout its baseline security criteria.

Second, NIST should consider structuring its baseline security guidance in tiers, to provide examples of how criteria under each capability may vary depending on the type of device (e.g., simple or complex), the context in which it is deployed (e.g., managed or unmanaged), and its general risk profile. Such tiering would help to align with the Cyber EO's instruction that the IoT cybersecurity criteria "shall reflect increasingly comprehensive levels of testing and assessment that a product may have undergone," and will help to provide clearer guidance for all stakeholders, including both manufacturers and consumers.

B. A Pilot Program Should Encourage Voluntary Use of Flexible Consensus Baselines.

Importantly, NIST has made clear that in exploring the Pilot Program it is not attempting to mandate baselines against which devices are measured. The Draft states that:

> "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."[37]

[36] *Id.* at 5 (listing as a potential criterion "[t]he ability to log cybersecurity-related state information (e.g., software update installations, failed log in attempts, configuration changes)").

[37] *Draft,* at 1.

During NIST's Workshop on Cybersecurity Labeling Programs for Consumers ("Labeling Workshop"), a NIST representative emphasized this, explaining that NIST is not establishing its own labeling program and is instead working to identify minimum requirements and desirable attributes for a labeling program.[38] This is the right approach, as it will help stakeholders develop approaches that can be adapted by industry participants as appropriate.

As NIST continues to develop the baseline security criteria, it should encourage voluntary and flexible use of industry best practices and consensus baselines, as appropriate. This is consistent with the Cyber EO's directive that NIST "shall examine all relevant information, labeling, and incentive programs and employ best practices."[39] Examples of industry best practices and consensus baselines that may be appropriate for stakeholders to consider include: CTIA's IoT Cybersecurity Certification Program; the Internet of Secure Things (ioXt) Certification Program; and CSDE's C2 Consensus on IoT Device Security Baseline Capabilities. NIST should also account for innovation and experimentation, allowing for the baseline security criteria to evolve and accommodating further development of industry best practices and consensus baselines.

[38] *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 ("*Labeling Workshop*").

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

V. NIST MUST PRIORITIZE TOOLS THAT ARE CLEAR AND HELPFUL TO CONSUMERS AND AVOID CONFUSION.

A. NIST Should Simplify the Baseline Security Criteria as an Initial Step to Developing an Approach That Is Clear and Helpful to Consumers.

A critical directive from the Cyber EO in standing up any Pilot Program is to "focus on ease of use for consumers."[40] Although NIST recognizes that the criteria that will form the basis of a label must "be understood by largely non-technical purchasers of the product,"[41] several portions of the Draft are highly complicated and will be difficult to incorporate into a label that is not confusing, and that provides value to the average consumer.

For example, a potential criterion under the "Documentation" capability is documentation of the "[l]aws and regulations with which the IoT product and related support activities comply."[42] This could be confusing or misleading to consumers that do not understand the applicable legal frameworks or the implications of various laws and regulations, and it may be impractical to the extent that overlapping laws and regulations apply to a product. Furthermore, the criterion requiring documentation of "product design and support considerations related to the IoT product, such as [] [a]ll hardware and software components, from all sources (e.g., open source, propriety third-party, internally developed) used to create the IoT product (i.e., used to create each product component)" is complex and should be streamlined (or dispensed with) because software development process and provenance considerations are far beyond the need of all but the most tech-literate consumers.[43]

---

[40] *Id.*

[41] *Draft*, at 11.

[42] *Id.* at 5.

[43] *Id.* at 6.

More generally, the structure of NIST's Draft Security Baseline Criteria should be simplified, which will result in clearer guidance for manufacturers and a better starting point for a labeling approach that will not confuse consumers. *First,* it is unclear how the criteria listed in Table 3 would be applied in the Pilot Program. NIST states that these criteria "may apply, particularly to IoT products that include multiple components" but the Table does not make clear how these criteria interact with the criteria in Table 1.[44] Further clarification is needed to explain why these additional criteria may be needed and to what devices they could apply.

Second, the Draft should align more closely with NIST's existing core baseline—NISTIR 8259A. Although NIST states that Table 1 is "[d]eveloped from NISTIR 8259A,"[45] the capabilities listed in Table 1 stray from NISTIR 8259A. In multiple instances, the Draft expands the capabilities beyond "devices." For example, instead of "Device Identification," which is a capability defined by NISTIR 8259A,[46] the Draft lists "Asset Identification."[47] And the Draft adds a seventh capability (in addition to the six in NISTIR 8259A) called "Product Security," which is defined as "[t]he IoT product can perform other features and functions across some or all of its components to make IoT products minimally securable for the sector."[48] Given the robust stakeholder engagement process that NIST undertook to build NISTIR 8259A, NIST should more closely adhere to the capabilities in NISTIR 8259A and refrain from deviating from those well-established capabilities or adding new capabilities that have not been vetted by

[44] *Id.* at 3.

[45] *Id.*

[46] *NISTIR 8259A*, at 5.

[47] *Draft*, at 3.

[48] *Id.* at 5.

relevant stakeholders. Straying from the existing baseline will be confusing and unnecessary in the context of this Pilot Program.

Overall, simplifying and clarifying the criteria—and ensuring they remain consistent with NIST's existing work— is more likely to support labeling that can achieve the consumer-focused goals set out in the Cyber EO.

B. Any Pilot Program That Promotes Consumer Labels Must Emphasize Clarity and Thorough Consumer Research, to Avoid Confusion.

NIST recognizes that any consumer IoT product cybersecurity labels must be "[u]nderstandable by the consumer," "[a]ctionable by the consumer," and "[e]ffective in conveying the product's value."[49] The challenges in designing a non-confusing labeling approach are significant, as the design must be sufficiently simple for consumers to readily understand, while oversimplification of complex matters like security can be confusing or misleading. The panelists during the Consumer Perspectives panel of the Labeling Workshop noted that effective labels must be digestible across various consumer groups, including by incorporating user-friendly design and consistent symbols and language.[50] At the same time, as NIST's own technical criteria illustrate, cybersecurity is a complex topic that is difficult to convey to consumers.

NIST's recommendations about labeling must account for challenges in effectively conveying cybersecurity information to consumers. For example, while the Cyber EO contemplates criteria that "reflect increasingly comprehensive levels of testing and assessment"[51]—which is consistent with a risk-based approach to IoT device security in the first

[49] *Id.* at 11.

[50] *Labeling Workshop*.

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

instance—a label that tries to convey such a tiered approach may be confusing to consumers and may not be the most effective way to convey information in many circumstances. NIST should make clear that a lower security tier does not necessarily mean that a device is less secure but rather that the device has a lower risk profile, and any labels should not inadvertently mislead consumers to believe that such devices have inadequate security based on a risk assessment. Thus, different options may be appropriate across the range of risk profiles in consumer IoT.

NIST also should emphasize that any labeling or related consumer-focused communications must be based on thorough consumer research and testing. As noted by an FTC representative at the Labeling Workshop, the most effective consumer labels are those that have actually been tested on consumers.[52] The highly technical nature of cybersecurity necessitates testing and research of label prototypes to ensure that the ultimate label will provide value to the average consumer and will not be misleading. Indeed, the FTC regularly emphasizes the importance of claim substantiation and consumer testing in many settings, as well as its willingness to hold companies liable for making claims that it views as misleading in the security context.[53] Likewise, in the context of environmental certifications, it has warned companies that "seals and certifications can inadvertently deceive consumers by conveying more than a marketer intends."[54] And more generally, the FTC has noted that "[a]dvertisers are responsible for ensuring that all express and implied claims that an ad conveys to reasonable consumers are

[52] *Labeling Workshop*.

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

[54] *FTC Sends Warning Letters about Green Certification Seals*, FTC (Sept. 14, 2015), https://www.ftc.gov/news-events/press-releases/2015/09/ftc-sends-warning-letters-about-green-certification-seals.

truthful and substantiated."[55] To that end, "[c]opy tests or other evidence of how consumers actually interpret an ad can be valuable."[56] These realities and risks must remain top of mind for NIST and any other agencies promoting consumer communications or labeling.

VI. TO PROMOTE MANUFACTURER PARTICIPATION, NIST SHOULD IDENTIFY LIABILITY RISKS AND SAFE HARBORS, AND PROMOTE PREDICTABLE INDUSTRY STANDARDS.

The Cyber EO requires NIST, in evaluating IoT labeling proposals, to "consider ways to incentivize manufacturers and developers to participate in these programs."[57] 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."[58] The use of a consumer IoT device label can create significant liability risk; without liability protection, manufacturers and certification bodies may not want to assume the risk that some consumers will misinterpret a label and bring a lawsuit.

NIST need not take a position on the propriety or legitimacy of consumer litigation over labeling to acknowledge that the concerns are real and may be an impediment to participation in product labeling. To discharge its mandate under the Cyber EO, NIST should identify for policymakers the litigation risk to manufacturers and certification bodies, flowing from unique challenges in communicating complex cybersecurity information to consumers with varying levels of sophistication and cybersecurity knowledge. As a result, liability protections such as legal safe harbors are likely to provide substantial value to the Pilot Program. Safe harbors

---

[55] .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.

[56] *Id*. n.14.

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

[58] *Id.*

would drive greater industry participation and may help achieve predictability in practices. Safe harbors and regulatory certainty have been important to encourage activities like carrier blocking of illegal and unwanted automated calls, so NIST should explore analogies and other models.[59] At a minimum, helpful liability protections should apply to: (1) a manufacturer that displays a label on its device; and (2) an organization that performs third-party certifications. Both groups face significant liability risks and are essential to the success of the Pilot Program, so NIST should address their risks in its evaluation of Pilot Program feasibility.

As part of its evaluation of how to encourage stakeholder participation, NIST should also consider encouraging the use of regulatory sandbox policies that have been employed successfully in other environments to promote pro-consumer innovation while providing liability protections and greater regulatory certainty to industry. The Consumer Financial Protection Bureau has administered several programs to facilitate innovation in this manner, including a regulatory sandbox program.[60]

VII. CONCLUSION

CTIA appreciates the opportunity to continue its work with NIST on IoT security. As NIST looks to refine and finalize the Draft Baseline Security Criteria, CTIA encourages NIST to: (1) clarify that the Pilot Program is voluntary and focused on higher-risk consumer IoT devices; (2) further promote both flexibility and a risk-based approach to consumer IoT device security; (3) encourage voluntary use of flexible consensus baselines; and (4) simplify the criteria to

[59] *See, e.g.*, *Advanced Methods to Target and Eliminate Unlawful Robocalls*, 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*, Report and Order, 35 FCC Rcd. 15221, ¶ 13 (2020) (expanding the call blocking safe harbor to include network-based blocking).

[60] *Innovation at the Bureau*, Consumer Financial Protection Bureau, https://www.consumerfinance.gov/rules-policy/innovation/ (last visited Oct. 7, 2021).

provide more clarity and avoid consumer confusion**.** Moreover, CTIA recommends that NIST's overall work on the Pilot Program prioritizes consideration of tools that are clear and helpful to consumers and contemplates the benefits that liability protections and safe harbors would provide for industry participation and uniformity.

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

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

October 18, 2021