September 19, 2023
Via barbara.cuthill@nist.gov
Barbara Cuthill
National Institute of Standards and Technology
Internet of Things Advisory Board
barbara.cuthill@nist.gov

Re: Internet of Things Advisory Board Updated Pre-Read Draft; Comments of CTIA

Dear IoT Advisory Board,

CTIA[1] appreciates the opportunity to comment on the Internet of Things ("IoT") Advisory Board's ("Advisory Board") August 18, 2023 Updated Pre-Read Draft Report ("Draft Report"),[2] which the Advisory Board is finalizing into a report ("Final Report") that will be delivered to the Internet of Things Federal Working Group ("Federal Working Group") by December 2023. The Federal Working Group will integrate the Final Report into its IoT policy recommendations to Congress in June 2024 regarding actions the federal government should take to overcome barriers to IoT adoption and support IoT development. We understand that the Advisory Board's goal is to finalize the substance of the Draft Report at its upcoming September meeting, so we appreciate the opportunity to provide feedback at this critical juncture. The Advisory Board is right to welcome public comments as it develops the Final Report, as meaningful collaboration will help the Final Report reflect a broad range of stakeholder perspectives.

The Draft Report proposes "Key Recommendations," which are broken down into fourteen categories.[3] While some of the categories are industry-specific, several categories—including cybersecurity and privacy—are "horizontal," meaning that they apply broadly across specific industries and beyond the IoT ecosystem. CTIA supports the Draft Report's categories, which generally reflect the Advisory Board's Charter.[4] With this letter, CTIA (1) encourages the Advisory Board to apply voluntary, flexible, and

[1] CTIA – The Wireless Association® (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] Work-in-Progress Draft Report of the Internet of Things Advisory Board, NIST (Aug. 18, 2023), https://www.nist.gov/system/files/documents/2023/08/18/Draft%20IoTAB%20Report%2020230816%20v2.pdf, ("Draft Report").

[3] The Key Recommendation categories are: (1) National Data Protection Framework; (2) Standardize IoT Implementation; (3) IoT Cybersecurity; (4) IoT Connectivity Improvement and Expansion; (5) Address Privacy Considerations; (6) Sustainable Infrastructure; (7) Workforce; (8) Smart Traffic and Transit; (9) Augmented Logistics and Supply Chains; (10) Precision Agriculture; (11) Environmental Monitoring; (12) Public Safety; (13) Health Care; (14) International Considerations.

[4] U.S. Department of Commerce National Institute of Standards and Technology Internet of Things Advisory Board Charter, NIST, § 4 (Dec. 15, 2021), https://www.nist.gov/system/files/documents/noindex/2021/12/20/IOT-Board-Charter-20211215.pdf.

consensus-based approaches to all recommendations in the Final Report; (2) urges the Advisory Board to support uniform and technology-agnostic standards or frameworks for any "horizontal" recommendations; (3) supports a number of the Key Recommendations that promote interoperability, support improved connectivity, encourage security of IoT devices; and (4) identifies other recommendations that should be modified to be more voluntary, flexible, and consensus-based.

IoT Promises Enormous Benefits for Consumers, Businesses, and Society, and the Wireless Industry Is Committed To Continuing Its Efforts To Advance IoT.

While the Draft Report provides a good starting point to discuss the benefits of IoT, it should be expanded to incorporate additional language elaborating on a number of critical topics.

IoT Benefits. IoT will bring immense positive change, from devices that make life easier (like smart appliances)[5] to life-saving health management tools (such as wireless infusion pumps, health trackers)[6] to revolutionary business efficiencies (like enhanced asset and productivity monitoring).[7] As the Draft Report correctly articulates, "the Internet of Things is likely to deliver significant and scalable economic and societal benefits to the United States."[8] Fundamentally, IoT offers the potential to solve some of the greatest social challenges of our time, including a wide variety of public health and environmental challenges.

CTIA applauds the Draft Report's recognition of the benefits emerging from the IoT ecosystem.[9] Building from this, CTIA urges the Advisory Board to bolster its discussion of the benefits likely to flow from IoT, so that the full potential of IoT can more highlighted more explicitly. The Advisory Board has been clear during its meetings about some of the seismic benefits that may come from the IoT, and it would be helpful to have more of this perspective included in the Draft Report. Without a clearly articulated vision of the potential benefits from IoT, it will be harder for policymakers to understand the potential costs of failing to take key enabling steps. And because the Final Report represents the best chance for industry to make these benefits known to the Federal Working Group, it is critical that the Advisory Board include as much perspective on the positive impacts of IoT in the Final Report as possible.

Connectivity. The Draft Report correctly recognizes connectivity as a significant factor in increasing IoT adoption. The wireless industry plays a key role in America's technology ecosystem, and will continue to be an integral part of new and emerging technology areas, as this connectivity helps to accelerate the development of emerging technologies, and CTIA and its members are committed to enabling wireless

[5] *See, e.g., Smart Cities Working Groups*, CTIA, https://www.ctia.org/smart-cities-working-group (last visited Sept. 18, 2023); *see also* Smart Cities Playbook: Building Your Connected Community, CTIA (2019), https://api.ctia.org/wp-content/uploads/2020/02/CTIA-Smart-Cities-Playbook.pdf.

[6] The 5G Innovators: Entrepreneurs Leveraging the 5G Platform, CTIA (Feb. 2023), https://api.ctia.org/wp-content/uploads/2023/02/2023-CTIA-Industry-Case-Studies.pdf.

[7] *NIST Cybersecurity for IoT Program*, NIST, https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program (last visited Sept. 18, 2023). (The rapid proliferation of Internet-connected devices and rise of the IoT "bring the promise of enhanced business efficiencies and increased customer satisfaction."); *see also Wireless Empowers America's Seniors*, CTIA Blog (Aug. 21, 2020), https://www.ctia.org/news/wireless-empowers-americas-seniors.

[8] Draft Report at 28.

[9] *See e.g.*, Draft Report at 38, 42, 53.

connectivity to support additional IoT deployment. With the wireless industry's significant investments in the further deployment of the 5G network, which is the most secure generation of wireless technology to date, wireless providers continue enhancing next-generation wireless services and providing further fuel for the IoT ecosystem and U.S. economy. Wireless connectivity is critical to providing connectivity to all Americans, including those in more rural and remote areas, and enabling all to have access to the benefits from IoT.

Wireless networks, particularly 5G, provide unprecedented reliability, robust security, extremely low latency, widespread coverage, and seamless mobility, which can support technological innovation in numerous contexts including various IoT use cases. With wireless connectivity, individuals and businesses can use the diverse landscape of IoT offerings to stay connected and reap transformative benefits. Wireless networks will support lightning-fast connections between sensors and artificial intelligence ("AI") data processing. Thus, while IoT is clearly not limited to 5G applications, the growth of 5G will inevitably allow for the expansion of new IoT applications and further IoT adoption. Comprehensive national policies that support access to licensed spectrum, particularly low- and mid-band, are critical for the next generation wireless that will enable the continued growth of IoT innovation. **Key Recommendation 4.0** correctly identifies the importance of connectivity and key spectrum resources to the future of IoT.

IoT Security. The Draft Report correctly incorporates multiple recommendations to improve the security of IoT. CTIA and the wireless industry are leaders in developing and deploying innovative approaches to enhance cybersecurity, including IoT. As CTIA noted in a recent white paper, the wireless industry has long deployed "mutual authentication protocols between devices and networks," using "Zero Trust principles" to "help advance security."[10] **Key Recommendation 3.0** correctly promotes NIST's role in cybersecurity. CTIA and its members have collaborated with the National Institute for Standards and Technology ("NIST") over the years on a plethora of cybersecurity topics, including NIST's IoT cybersecurity efforts[11] as well as its broader cybersecurity efforts.[12] CTIA applauds the Advisory Board's

[10] Defining Zero Trust: Industry Approaches and Policy Frameworks for Strong Wireless Network Security, CTIA, at 11 (Jan. 9, 2023), https://api.ctia.org/wp-content/uploads/2023/01/Defining-Zero-Trust-White-Paper-2023.pdf.

[11] Earlier this year, CTIA provided comments on Draft SP 1800-38A: Executive Summary (See Letter Comments of CTIA, Preliminary Draft, NIST SP 1800-36A: Executive Summary, Enhancing Internet Protocol-Based IoT Device and Network Security (Feb. 3, 2023)). Additionally, CTIA has contributed to NIST's prior work on IoT security (See, e.g., Comments of CTIA, NIST CSWP 18 (Initial Public Draft), Establishing Confidence in IoT Security: How Do We Get There? (filed June 14, 2021); Comments of CTIA, Draft NISTIR 8259, Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers (filed Sept. 30, 2019); Comments of CTIA, Draft Project Description, Security for IoT Sensor Networks: Building Management Systems Case Study (filed Mar. 28, 2019); Comments of CTIA, Draft NISTIR 8228, Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks (filed Oct. 24, 2018)).

[12] CTIA also provided input in the development of the NIST Cybersecurity Framework and SP 800-53 to which Draft SP 1800-36E maps components of the reference design. See, e.g., Comments of CTIA, Views on the Framework for Improving Critical Infrastructure Cybersecurity, Docket No. 151103999-5999-01(Feb. 23, 2016); Comments of CTIA, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (Draft) Request for Comments (Apr. 10, 2017); Comments of CTIA, Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management, Docket No. 220210-0045 Request for Information (Apr. 25, 2022); Comments of CTIA, NIST SP 800-53 Rev. 5 (Draft), Security and Privacy Controls for Information Systems and Organizations (Final Public Draft), NIST SP 800-53 Rev. 5 (Draft) (May 29, 2020). CTIA Letter Comments of CTIA, Preliminary Draft, NIST SP 1800-36B-E: Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management: Enhancing Internet Protocol-Based IoT Device and Network Security, Volume E at 9-34 (filed June 20, 2023).

recognition of the leading role that NIST has played—and should continue to play—in IoT security.

The Final Report's Recommendations Should Promote Voluntary, Flexible, and Consensus-Based Approaches, as well as Uniform and Technology-Agnostic Approaches on Issues that Span Across Sectors.

Principles for All Recommendations. As the Advisory Board moves ahead to draft its Final Report, it should reiterate the importance of voluntary, flexible, consensus-based approaches, and offer support for NIST's continued involvement in creating and updating guidance and standards that are rooted in these core principles, such as the NISTIR 8259 Series.[13] A voluntary, flexible approach, without unnecessary regulatory barriers or overly prescriptive, one-size-fits-all standards, will help industry innovate, deploy new technologies, deliver societal benefits, bolster the national economy, and maintain America's leadership in technology matters. In contrast, prescriptive regulations can be burdensome and drive businesses to abandon promising ideas or cede leadership to other countries due to the potential costs of compliance. The IoT landscape is vast and diverse, and products are deployed in a wide variety of use cases and have varying risk profiles. Rather than static regulations, the Final Report should recognize that the government can and should embrace strategies such as developing flexible policies and frameworks, promoting industry standards and best practices, and supporting crucial public-private partnerships.

Recommendations for federal government action should further emphasize the need for a light-touch regulatory approach for emerging technologies generally. The Advisory Board should highlight the various successes of a light-touch regulatory approach to emerging tech, and advise Congress that such an approach will best "foster or enhance the adoption of technology or help expand economic opportunities within the emerging technology areas."[14]

Principles for Horizontal Recommendations. Additionally, the Advisory Board should expand the Draft Report's recommendations to emphasize the benefits of and need for technology-agnostic, uniform, and risk-based horizontal standards. National frameworks, standards, or legislation that address horizontal issues, such as privacy and cybersecurity, should be uniform and apply across industries in the internet ecosystem, rather than narrowly tied to certain products or sectors. In the world of constantly-emerging technologies and rapidly-changing industries, uniform, technology-agnostic standards help future-proof efforts to, for example, improve security or sustainability.

While the Final Report will correctly focus on IoT applications and enabling technologies, any horizontal recommendations it adopts should be technology-agnostic. Technology-agnostic approaches allow for the principles of privacy and security to be applied uniformly as new technologies are created or are expanded beyond their current definitions. NIST has implemented this principle in its creation and development of the Cybersecurity Framework and Privacy Framework.[15] Existing broad legal frameworks, when properly applied, may provide better protection against potential harms than a reactive, technology-specific approach, particularly as many such laws and regulations have stood the test of time. Further, existing

[13] *NIST Cybersecurity for IoT Program: NISTIR 8259 Series*, NIST, https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/nistir-8259-series (last updated Nov. 16 2021).

[14] *Study To Advance a More Productive Tech Economy*, Notice; Request for Information, 86 Fed. Reg. 66,287, 66,287 (Nov. 22, 2021), https://www.govinfo.gov/content/pkg/FR-2021-11-22/pdf/2021-25428.pdf.

[15] *See Cybersecurity Framework*, NIST, https://www.nist.gov/cyberframework (last visited Sept. 18, 2023); *Privacy Framework*, NIST, https://www.nist.gov/privacy-framework (last visited Sept. 18, 2023).

frameworks can apply without needing to resolve challenges caused by technology-specific definitions, particularly if the frameworks apply to conduct regardless of the technology used.

CTIA Applauds a Number of the Advisory Board's Key Recommendations.

Key Recommendation 2.0: Standardize IoT Implementation.[16] CTIA supports the Draft Report's dedication to improve "Standardization in IoT Implementation" to increase interoperability.[17] The Advisory Board can further promote this interoperability by encouraging technology-agnostic standards and frameworks.

Key Recommendation 3.0: IoT Cybersecurity.[18] CTIA supports the Draft Report's focus on NIST's role in "develop[ing] recommended baselines and outcomes for the entire IoT ecosystem. . . ." and agrees that "[b]y tasking NIST with developing required outcomes, and industry with specific requirements to meet those outcomes, each side works in an area of strength. These roles are working and should continue."[19] CTIA also agrees that NIST should continue to guide IoT security. As a non-regulatory agency with extensive expertise on cybersecurity risk management, NIST is the right agency to develop and promote flexible, risk-based approaches that will best lead to a securable IoT ecosystem, thereby helping to protect consumers. NIST has continually demonstrated its effectiveness in these efforts, with its voluntary consensus guidance for IoT security being a seminal baseline across the IoT ecosystem. Further, CTIA supports **Supporting Recommendation 3.4**, which specifically recommends that "the federal government should continue to support NIST as the developer of outcome-based requirements that inform industry consensus standards, and industry as the developer of those standards."[20]

CTIA encourages the Advisory Board to expand on its support of NIST's collaboration with industry throughout the Final Report. Similarly, CTIA also supports the Advisory Board's continued discussion of cybersecurity throughout the Draft Report. Cybersecurity must be a top priority for IoT implementation because it is key critical to establishing and keeping consumer trust.

Key Recommendation 4.0: IoT Connectivity Improvement and Expansion.[21] CTIA supports the Draft Report's recommendation to "promote accelerated innovation to ensure improved communications by ensuring the availability of suitable and sufficient spectrum resources, the development of wide-area

[16] Draft Report at 37 ("The Federal Government should establish methods to foster interoperability for IoT technology, including through the use of consistent models, protocols, and schemas.").

[17] *Id.*

[18] *Id.* at 43 ("The Federal Government should provide specific and consistent guidance for providers and adopters to ensure secure operations. While not the exclusive source of cybersecurity guidance, federal entities should continue to support NIST as a developer of outcome-based requirements that inform industry consensus standards, and industry as the developer of those standards.").

[19] *Id.*

[20] *Id.* at 45.

[21] *Id.* at 51 ("The federal government should expand and improve programs that ensure reliable and sufficient connectivity among and between IoT devices in all areas of the country. The government should further promote accelerated innovation to ensure improved communications by ensuring the availability of suitable and sufficient spectrum resources, the development of wide-area networking technologies, and enhancing interoperability.").

networking technologies, and enhancing interoperability."[22] In particular, CTIA strongly supports taking action to make additional spectrum available. Exclusive-use, licensed spectrum is the lifeblood of secure wireless connectivity, and the federal government should take steps to ensure more of this critical resource is available. Specifically, CTIA encourages the Advisory Board to include recommendations to advance mid-band spectrum priorities. Globally, the U.S. has fallen behind other countries that have increased access to mid-band spectrum for exclusively licensed, flexible uses, risking the nation's ability to be a global leader for next-generation services. Low- and mid-band spectrum availability has increased only moderately since 2012, and existing licensed spectrum allocations are insufficient to meet continuing consumer demand. Replenishing the pipeline of mid-band spectrum for licensed operations is critical for development of the 5G economy and maintaining US. Global competitiveness in the wireless and broader IoT ecosystem.

CTIA also supports additional funding and acceleration of broadband deployment in rural America, so long as this is done on a technology-neutral basis. Wireless networks present a cost-effective solution for closing the digital divide in many circumstances, and the Advisory Board should recommend that broadband provided by wireless receive the same consideration in funding as other broadband solutions.

While CTIA and its members have done and are doing a tremendous amount of work on their own to encourage IoT adoption, there is more that can and should be done at the federal government level. The Draft Report correctly recognizes this need, and CTIA supports its recommendations that address the need for increased "connectivity among and between IoT devices in all areas of the country."[23]

Section 6.2: AI Considerations.[24] CTIA supports the Advisory Board's plan to incorporate a broad discussion about the intersection of IoT and AI.[25] In doing so, it is important for the Advisory Board to recognize that AI, as a concept, is not monolithic, and there are many AI implementations that can operate in already-regulated industries without needing any additional regulations. For example, wireless providers have already seen benefits in utilizing AI to:

- Improve accessibility through applications like voice-enabled calling, auto-captioning, and natural language understanding—all powered by AI or machine learning—promise life-altering benefits for individuals with disabilities. This helps to increase independence, connectivity, and communications for and among individuals with a variety of accessibility needs.
- Strengthen national security and cybersecurity, for example, by using AI to supplement the industry's already robust cybersecurity posture to engage in real-time network threat detection, helping facilitate zero trust approaches to cybersecurity, and supplementing identity and access management tools.
- Manage wireless networks to improve network speeds, efficiency of operations, network interoperability, and network resiliency. For example, AI and machine learning models help providers anticipate natural disasters, monitor planned and unplanned antenna changes, and detect device performance anomalies.

[22] *Id.*

[23] *Id.*

[24] *Id.* at 23.

[25] *See e.g., Id.* at 108, 112.

Any AI recommendation should highlight and encourage the beneficial uses of AI and innovation.

Further, with respect to any recommendations regarding AI, the Advisory Board should call for a reasonable and balanced federal approach to AI that encourages development of trustworthy AI; promotes innovation that will continue to deliver benefits to consumers, the economy, and society; and ensures American leadership in AI development and standards. Any federal framework should, among other things, (1) account for existing laws and regulatory protections, to avoid needless and burdensome duplication given that there are already laws and regulations that protect against many of the concerns posed by AI; (2) be uniform across sectors and harmonized, to avoid the harmful impacts of state- and federal-level fragmentation; (3) be risk-based, focusing on high-risk applications of AI, rather than trying to address AI as a technology more broadly or treat all applications of AI the same; and (4) be flexible, consistent with NIST's AI Risk Management Framework.[26]

CTIA Encourages the Advisory Board To Modify a Number of Other Key Recommendations To Be More Focused on Voluntary, Consistent, and Consensus-Based Approaches.

The Draft Report represents a strong effort to address necessary steps that should be taken to promote IoT adoption. At the same time, there are a number of areas in the Draft Report where it would be beneficial to revisit the existing conclusions and recommendations.

Key Recommendation 1.0: National Data Protection Framework.[27] CTIA cautions the Advisory Board against proposing a new "data protection" framework for IoT. **Key Recommendation 1.0** calls for "a framework or model by which data related to the Internet of Things may be protected and used to benefit all."[28] **Supporting Recommendation 1.1** promotes the delineation of frameworks based on the types of data.[29] **Supporting Recommendation 1.2** encourages an IoT specific privacy framework and points to California Consumer Privacy Act ("CCPA") and General Data Protection Regulation ("GDPR") as models for the guidance.[30]

The Advisory Board should reconsider this recommendation, and should not encourage data- or technology-specific privacy frameworks. NIST has already developed a voluntary Privacy Framework with heavy input from industry stakeholders,[31] including CTIA; the Privacy Framework can be applied as needed in IoT implementations. Creation of new frameworks that are narrowly focused on certain types of data or technologies limits the longevity and future-applicability of the principles embodied in the frameworks, as discussed above. Rather, specific topics—like IoT—can be better addressed in profiles or other separate modules under the existing, general Privacy Framework. And not only is there no need for additional, technology-specific frameworks, but the adoption of such frameworks could also be harmful to the

[26] NIST AI 100-1, Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST (Jan. 2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

[27] Draft Report at 32 ("The U.S. should establish a framework or model by which data related to the Internet of Things may be protected and used to benefit all. The model would consider a schema for describing IoT-related data and methods for both use and protection.").

[28] *Id.* at 33.

[29] *Id.* at 33-34.

[30] *Id.* at 34-35.

[31] *Privacy Framework*, NIST, https://www.nist.gov/privacy-framework (last visited Sept. 18, 2023).

deployment of IoT by creating confusion and fragmentation.[32] In addition, the Draft Report should avoid suggesting the use of the GDPR and CCPA as guides for any federal framework.[33] These laws and resulting regulations have proven difficult and costly to implement and are developing from different jurisdictions and authorities. Instead, the Advisory Board should put forward recommendations that rely on uniform, consistent privacy principles.

Indeed, rather than its current **Key Recommendation 1.0**, CTIA encourages the Advisory Board to articulate support for national privacy legislation that is uniform and comprehensive, which CTIA and the wireless industry have long supported. CTIA and the wireless industry are committed to protecting consumer privacy. Unfortunately, the current status of privacy laws in the United States—which is heavily fragmented at both the state and federal levels—works against this goal. Fragmentation leads to consumer confusion about how data is treated and what rights they may have, as consumers may be unaware that the same data can be regulated differently depending on the jurisdiction or business designation. This consumer confusion is compounded by over-notification and warning fatigue that can result from such a complex regulatory landscape. Fragmentation also puts a significant strain on private sector resources by requiring compliance with numerous different standards that vary across jurisdictions. This strain can divert resources from meaningful practices that promote privacy. The harmful impacts of fragmentation are only growing worse in the absence of federal action, with multiple states adopting differing approaches and even more on the horizon.

Comprehensive federal privacy legislation that preempts the growing patchwork of state privacy laws is the only way to combat fragmentation and achieve a uniform national approach to privacy. For many years, CTIA has supported federal privacy legislation that would establish a uniform, comprehensive, and technology-neutral national law and provide consistent protections across states and industry sectors.[34] By enacting such legislation, the federal government would provide needed clarity and certainty to consumers and businesses and ensure that consumers are protected equally no matter where they reside. A single national approach would provide guidance for both consumers and companies seeking clarity on what the expectations are for data privacy and security. This would ultimately lead to more complete and widespread compliance and would also offer strong protections for consumers across the nation, regardless of their location or how they interact with the digital economy. This would be positive for consumers and businesses alike.

[32] *See* Draft Report at 34 ("Supporting Recommendation 1.2: The government should develop an IoT Privacy Framework for Innovation and Data Protection specifically tailored to the unique challenges posed by IoT devices.").

[33] *Id.*

[34] *See* Kelly Cole & Tom Power, *Protecting Consumers with Federal Privacy Legislation*, CTIA Blog (Nov. 9, 2018), https://www.ctia.org/news/protecting-consumers-with-federal-privacy-legislation.

Supporting Recommendations 3.3,[35] 3.5,[36] and 5.1[37]: IoT Labeling Initiatives. CTIA encourages the Advisory Board to expand its three supporting recommendations on IoT labeling to include (1) requirements that any program remain voluntary, flexible, clearly-scoped, and industry-led and (2) specific protections for participants to encourage adoption of any voluntary, federal labeling program.

First, consistent with the general principles outlined in Section III, recommendations for any cybersecurity labeling program, such as FCC's proceeding to implement a voluntary labeling program called the "U.S. Cyber Trust Mark,"[38] or other similar labeling scheme contained in the Final Report should include clear direction for these programs to remain voluntary, flexible, clearly-scoped, and industry-led.

- For any labeling program to be successful, participation must be voluntary. A voluntary program enables stakeholders to test different approaches and promote innovative solutions that can be adapted by industry participants as appropriate.
- Cybersecurity labeling programs must also be flexible since "device cybersecurity capabilities will often need to be added or removed from an IoT device's design, integration, or acquisition to best address an organization's common cybersecurity risks."[39]
- The scope of a cybersecurity labeling program should also be clear, have defined objectives, and be easily understandable. Expanding a cybersecurity labeling program to provide consumers information outside of the core function of the label takes away from the effectiveness of providing consumer with clear, straightforward information about a device's security. Federal government agencies involved in developing labeling initiatives should thus avoid the temptation to turn these labels into a grab-bag of information, because doing so will inevitably dilute the label's message.
- Finally, labeling programs must be industry-led because industry remains best able to understand the ways in which labels can be designed to inform customers without overwhelming them with extraneous information.

While CTIA agrees that a labeling program should "prioritize broad and active industry engagement when developing and maintaining the government-sponsored portion of the U.S. national cybersecurity label for connected devices,"[40] as put forth in **Supporting Recommendation 3.3**, CTIA also encourages the Advisory Board to expand this recommendation to highlight the importance of keeping such a program voluntary and flexible as well.

CTIA also urges the Advisory Board to modify **Supporting Recommendation 5.1**'s proposal to combine or couple a privacy labeling with the U.S. Cyber Trust Mark for two reasons: (1) The U.S. Cyber Trust

---

[35] Draft Report at 45 ("The government should prioritize broad and active industry engagement when developing and maintaining the government-sponsored portion of the U.S. national cybersecurity label for connected devices.").

[36] *Id.* at 46 ("The Administration should encourage Congressional support to deploy IoT cybersecurity labeling initiatives, including establishing incentives for manufacturers to participate.").

[37] *Id.* at 55 ("Develop and implement a privacy transparency system for IoT devices, using the 'U.S. Cyber Trust Mark' for business, government, and consumer data for Connected Devices and other transparency programs as a guide.").

[38] *Cybersecurity Labeling for Internet of Things*, PS Docket No. 23-239, Notice of Proposed Rulemaking, FCC 23-65 (rel. Aug. 10, 2023).

[39] NISTIR 8259A, IoT Device Cybersecurity Capability Core Baseline, NIST, at 3 (May 2020), https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259A.pdf.

[40] Draft Report at 45.

Mark is still in its early formation stage and linking a recommendation to a program that has not been developed is premature, and (2) expanding the scope of the Trust Mark or linking another label with the Trust Mark runs the risk of overwhelming consumers with too much information, making all labels less effective.

Any labeling program needs to remain industry-led, with NIST continuing to play the key role of defining standards. The private sector has already developed best practices, certification programs, and consensus baselines, and it is critical to leverage this experience. NIST should retain its role as the developer of any technical specifications for implementation of a labeling program. NIST has the expertise and capability to draw from existing industry work and design flexible, effective standards. NIST has already been charged with these obligations under the IoT Cybersecurity Improvement Act of 2020 and President Biden's Executive Order, *Improving the Nation's Cybersecurity*,[41] and has developed several workstreams to develop these standards. The Advisory Board should also recognize that prescriptive requirements established by other government agencies with specific regulatory mandates could lead to overly rigid, fragmented security requirements that could have the unintended effect of reducing trust, rather than improving it.

Second, there are three critical types of protections that should be included in any recommendations for a federal labeling program. While **Supporting Recommendation 3.5** helpfully proposes that the "Administration should encourage Congressional support to deploy IoT cybersecurity labeling initiatives, including establishing incentives for manufacturers to participate,"[42] CTIA encourages the Advisory Board to include the specific incentives outlined below. Each of the following is necessary to properly incentivize participation.

- Treating participation in the program as a safe harbor means giving companies confidence that their voluntary, good faith use of the IoT cybersecurity label will serve as a means of compliance with applicable federal law and will not expose them to additional risk of litigation and regulation by the federal government. Accordingly, a safe harbor is essential to encourage participation in the program and use of the label.
- Absent federal preemption, state laws (in the form of legislation, regulation, or common law) could impose conflicting or differing obligations on companies that participate or could elect to participate in the program. Without preemption, participation in the program itself could lead to unpredictable liability from other state laws. Without clear guidelines, companies eligible for the program could be subject to different determinations of liability in different states, or even determinations that the label itself conveys a message that establishes some form of obligation under state law.
- International harmonization of labeling standards will help augment the security of products being used around the world and coming into the U.S. and will give consumers and other users greater confidence in the security levels for IoT devices. Global consistency will also reduce barriers to other markets for U.S.-based firms by eliminating the inefficiencies of divergent labeling rules in multiple markets, which can create costly and unnecessary duplication of product design and delays. Finally, international technical standards are generally preferred over national standards in commercial and international trade contexts because such international standards are less likely to be questioned and challenged as non-tariff market access barriers.

[41] Exec. Order No. 14,028, 86 Fed. Reg. 26,633 (May 17, 2021).

[42] Draft Report at 46.

Supporting Recommendations 6.3[43] and 6.4[44]: Creation of Federal Agencies/Offices Focused on Emerging Technologies. CTIA encourages the Advisory Board to reconsider including recommendations to create federal agencies and offices focused on emerging technologies. The principles of uniform, technology-agnostic frameworks and standards, discussed in Section III, cannot be reconciled with the creation of additional government agencies or offices devoted to emerging technologies, and the Advisory Board should avoid calling for the creation of such ad hoc entities. Additionally, "emerging technologies" is a broad, vague and impossible to define term that encompasses a vast array of technologies, including IoT. Without any guideposts around what constitutes an "emerging technology," new regulatory bodies with this mission could end up capturing vastly more regulatory authority than intended, putting them at odds with existing regulatory structures. In fact, as "emerging technologies" become mainstream, it is difficult to see how and when regulatory authority over these technologies could be shifted from new "emerging" technology regulation to existing structures. At what point, for example, would the Internet itself have been transitioned away from an agency or other body focused on "emerging technology"? Therefore, it has been and continues to be more effective to have subject-matter-specific agencies address the technologies that fall within their purview, even when those technologies represent a new approach to solving already-extant problems.

Calling for specialty bodies would also be counterproductive to the Advisory Board's desire[45] to future-proof the final report. The best way to ensure the long-term success of IoT and adoption of the cybersecurity and privacy principles advocated by the Draft Report is to keep standards consistent and uniform across all technologies and all industries, allowing the smooth integration of new technologies into existing structures and regulatory frameworks. To the extent any regulatory bodies institutes new regulations to this effect, the authority should remain with the existing agencies and not allow for additional regulatory bodies to further fragment the regulatory landscape.

* * *

CTIA appreciates the opportunity to provide feedback on the Draft Report as the Advisory Board finalizes recommendations that encourage the advancement of IoT. As the Advisory Board starts to finalize the Final Report, CTIA encourages the Advisory Board to continue to provide meaningful opportunity for input and to (1) call for voluntary, flexible, and consensus-based approaches under all of its recommendations, and for uniform and technology-agnostic frameworks under its "horizontal" recommendations; (2) continue to include recommendations that promote interoperability, support improved connectivity, encourage security of IoT devices, and incorporate AI; and (3) modify a few specific recommendations to be more focused on voluntary, consistent, and consensus-based approaches.

[43] *Id.* at 58 ("The Federal Government should establish an Emerging Technology (EmT) office within each of the federal agencies.").

[44] *Id.* ("The Federal Government should establish a national Emerging Technologies Program Office within the Executive office of the President to ensure that the federal government, state, and local government entities can effectively plan, implement, and manage emerging technology initiatives across the United States.").

[45] Internet of Things Advisory Board (IoTAB) Committee Meeting Minutes, NIST (Jan. 18-19, 2023), https://www.nist.gov/system/files/documents/2023/02/28/January_2023_IoTAB%20Meeting%20Minutes_v3.pdf.

Respectfully submitted,

/s/ Thomas K. Sawanobori
Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

David Valdez
Vice President, Privacy and Cybersecurity

Avonne S. Bell
Director, Connected Life

Justin Perkins
Manager, Cybersecurity & Policy

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