Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

Cybersecurity Labeling for	**)**	
the Internet of Things	**)**	**Docket No. 23-239**

Reply Comments of

NTCA–THE RURAL BROADBAND ASSOCIATION

To the Commission:

I. INTRODUCTION

NTCA–The Rural Broadband Association (NTCA) hereby submits reply comments in the above-captioned proceeding. In initial comments, NTCA expressed support for collaborative efforts among private and public sector bodies to promote security in the IoT environment. NTCA explained that this approach enables an ecosystem that can respond rapidly to evolving technology and threat environments while encouraging broad industry participation. NTCA identified National Institutes of Standards and Technology (NIST) programs as an example of public and private sector collaboration that creates achievable standards, encourages industry acceptance, and facilitates a platform that can adapt rapidly to change. NTCA also surfaced questions relating to the Commission's statutory authority to implement an IoT labels program. Finally, NTCA urged that to the extent a program is implemented, the Commission affirm its voluntary nature to ensure that it does not become a *de facto* requirement through attachment to other regulations.

II. DISCUSSION

Commenters Favor Collaborative Public/Private Sector Efforts that are Informed by NIST Standards

In initial comments, many commenters stated positions similar to those raised by NTCA. Parties from different sectors agreed with the continuing, evolutionary need for IoT security, and generally supported an approach that would encourage industry action by fostering consumer awareness through a labels regime. Many industry commenters acknowledged the role the Commission can play in a joint public and private sector effort. By way of example, the Connectivity Standards Alliance and USTelecom supported Commission leadership in oversight and management of an IoT label program.[1] The Cybersecurity Coalition also supported Commission administration of an IoT labels program,[2] and NCTA recommended the Commission as the "pertinent legal authority" in such an approach.[3] However, NCTA was clear that the technical standards governing the process should be reviewed and implemented through NIST-led collaborations.[4]

In fact, NIST guidelines were repeatedly cited as foundational standards. NIST has published several defining documents that define baseline standards for IoT security, including NIST IR 8529 (Foundational Cybersecurity Activities for IoT Device Manufacturers)[5] and NIST

[1] Connectivity Standards Alliance at 5; USTelecom at 10.

[2] Cybersecurity Coalition at 5.

[3] NCTA at 12.

[4] NCTA at 6.

[5] Michael Fagan (NIST), Katerina Megas (NIST), Karen Scarfone (Scarfone Cybersecurity), Matthew Smith (G2), "Foundational Cybersecurity Activities for IoT Device Manufacturers," NIST 8529, National Institutes of Standards and Technology (May 2020) (https://csrc.nist.gov/pubs/ir/8259/final) (accessed Nov. 10, 2023).

IR 8425 (Profile of the Core IoT Baseline for Consumer IoT Products).[6] These were recognized by many commenters. Consumer Technology Association identified NIST as the proper central authority for developing the baseline cybersecurity capabilities, labeling criteria, and related IoT security guidance.[7] Likewise, Underwriters Laboratories cited NIST IR 8425 as a baseline standard to enable "consistent and replicable product testing."[8] Samsung echoed this sentiment, noting that conformance with NIST criteria enables consistency. and recommended that NIST continue to lead private and public sector collaborative efforts for standard-setting.[9]

The widespread support among an array of industry participants including manufacturers, trade associations, and independent assessors[10] to use NIST standards as a basis for IoT label standards demonstrates several points: (1) The collaborative private/public sector approach is embraced across the industry; (2) NIST is a respected Federal partner in developing cybersecurity and IoT standards; (3) There is no need for the Commission to, as it were, "reinvent the wheel." NTCA supports an approach that conforms to these principles. As an active participant in numerous public and private sector cybersecurity efforts, NTCA affirms the value of collaborative, iterative efforts that update and refine preemptive and responsive actions.[11]

---

[6] Michael Fagan (NIST), Katerina Megas (NIST), Paul Watrobski (NIST), Jeffrey Marron (NIST), Barbara Cuthill (NIST), "Profile of the IoT Core Baseline for Consumer IoT Products," NIST 8425, National Institutes of Standards and Technology (Sep. 2022) (https://csrc.nist.gov/pubs/ir/8425/final) (accessed Nov. 10, 2023).

[7] Consumer Technology Association at 11-12.

[8] UL Solutions at 4. *See, also,* TechNet at 2 (Commission should align technical standards to NIST IR 8425).

[9] Samsung at 3.

[10] *See, i.e.,* Association of Home Appliance Manufacturers at 4.Comcast at 11; Consumer Reports at 11, 12; ioXt Alliance at 6; UL Solutions at 4.

[11] NTCA is a member of the Communications Sector Coordinating Council (CSCC) Executive Committee, for which NTCA staff counsel chairs the CSCC Small and Medium Sized Business Committee. Additionally, NTCA prepares informative resources to help members enhance their cybersecurity posture, including a National Institute of Standards and Technology (NIST) Framework Evaluation Tool that was developed by member companies to help small broadband providers to implement the NIST Cybersecurity Framework. NTCA also administers CyberShare, a small broadband provider ISAC (Information Sharing and Analysis Center. Finally, NTCA has participated actively

Connectivity Standards Alliance explains that technological development over time, including the emergence of higher-risk IoT devices, will demand different criteria for the program.[12] Samsung articulates similar points, urging industry-led standards that are risk-based and updated regularly to keep pace with evolving threats, technologies, and techniques.[13] This position is championed by others, including Consumer Reports which recommends the Commission to assign standards-setting to NIST or other standards bodies, leaving the Commission to focus on implementation and enforcement.[14] In similar vein, CTIA as well recommends the Commission to demur from taking the reins of standards setting and to leave those responsibilities within the hands of NIST. In this approach, the Commission would serve as program administrator and establish programmatic boundaries, while NIST would develop baseline cybersecurity standards and desired outcomes.[15] At bottom, commenters affirm the value of industry-led efforts to fortify the security of IoT devices.

An IoT Labels Program Must Accommodate Other Federal Agencies with Subject Matter Jurisdiction and Should Contemplate Currently Accepted Industry Standards

Even as commenters may generally support the Commission as the "scheme owner" to administer an IoT labels program, several commenters surface critical issues relating to regulatory overlap or potential conflict with other agency practices. For example, the Food and Drug Administration (FDA) explains that it has express statutory authority to regulate medical

in numerous docketed Federal proceedings aimed at enhancing data security and privacy.

[12] Connectivity Standards Alliance at 8-10.

[13] Samsung at 3.

[14] Consumer Reports at 11, 15, 16.

[15] CTA 1t 16-18. *See, also,* Connectivity Standards Alliance at 3 (the Commission should not modify NIST definitions).

device cybersecurity, and accordingly advises the Commission to exclude FDA-regulated medical devices from the Program.[16] In similar vein, albeit without the strict potential for cross-agency conflict, Pearl TV notes that the Commission's proposed definition could include Smart TVs, which are already subject to the ATSC 3.0 cybersecurity standard.[17] The U.S. Chamber of Commerce lists numerous industry standards groups, including the Telecommunications Industry Association's C2 Consensus on IoT Device Security Baseline Capabilities (C2 Consensus); CTIA's cybersecurity certification program for IoT devices; American National Standards Institute (ANSI)/CTA 2088; and various European programs.[18] NTCA submits that the proliferation of standards from different bodies supports Commission reliance on collective industry-driven NIST benchmarks. Such reliance need not obviate the work of the individual industry-specific bodies, as those groups would presumably be active in the formation of NIST standards upon which the Commission would rely and in whose development industry participates. At the same time, coordination with other Federal agencies would be necessary to ensure, as the FDA urges, that participants in a Commission program meet FDA or other requirements for medical device cybersecurity.[19]

The need for coordination with the Federal Trade Commission (FTC) was noted, as well. CTIA recommends the Commission to enter into a Memorandum of Understanding with the FTC to preempt unfair and deceptive trade practices actions (i) based on messages conveyed in a label; (ii) premised on alleged lack of device security where the device is labeled and is

[16] FDA at 1-4, 8, 9.

[17] Pearl TV at 5, 6. The Advanced Television Standards Committee is an international standards-setting body for digital TV.

[18] U.S. Chamber of Commerce at 2, 6.

[19] *See,* FDA at 5, 6.

compliant with the labeling requirements; and (iii) against a third-party standards or certification body.[20] Similarly, Telecommunications Industry Association urges the Commission to affirm that IoT devices obtaining a label have met any "reasonable security" requirements under state or Federal law, which would provide a safe-harbor presumption of reasonableness for devices that display the label.[21] TechNet, as well, argues for a "safe harbor" against Federal and state enforcement actions and/or private civil litigation for alleged damages resulting from a cyber incident.[22] NTCA agrees that reliance on labels should create a presumption of care and attention to cybersecurity needs, and that, as expressed in its initial comments, firms who rely on devices bearing a label can enjoy reasonable reliance on equipment manufacturer or vendor representations, and that firms that use these products "midstream" are not required to "unpack" equipment to determine the suitability of internal IoT devices or components.

Uncertainty Regarding Statutory Authority to Implement a Labels Program Can be Obviated by Ensuring that Participation Remains Wholly Voluntary

In initial comments, NTCA observed that the Communications Act does not provide a clear jurisdictional path toward IoT management. NTCA explained that whether Sections 302 and 332 extend reasonably to the further, broader field of IoT device security requires clarification, and it is not clear from the prior decisions cited in the NPRM that IoT labels are a logical follow-on to the authority to protect communications from spectrum interference. Comments submitted in the instant proceeding reflect diverse opinions on the ability of the Commission to draw authority from those provisions. Some industry associations offer support

[20] CTIA at 34.

[21] Samsung at 5-6.

[22] TechNet at 2, 3.

to the Commission's interest in relying on these sections.[23] Other organizations took a more cautious approach, suggesting that the provisions offer the Commission sufficient authority to establish a voluntary labeling program, but that a program *requiring* IoT devices to include the mark as a prerequisite for equipment authorization would be beyond the Commission's authority.[24] CTIA explained that notwithstanding Executive support for this foray, both Congress and the Executive branch have historically relied on NIST, the Department of Homeland Security, and the FTC to address cybersecurity.[25] In similar vein, the U.S. Chamber of Commerce advised the Commission to not "overinterpret its harmful interference authority under sections 302(a) and 333 to regulate the cybersecurity of IoT." The Chamber also noted that Congress did not look to the Commission when passed legislation to improve IoT cybersecurity.[26] USTelecom asserted the Commission cannot adopt a label program based on Sections 302 and 333, arguing those sections focus on wireless interference and neither addresses nor authorizes jurisdiction over cybersecurity and IoT security risk management.[27]

Commenters also discussed the need to ensure that an IoT labels protocol would be a voluntary program, only. Numerous commenters echoed NTCA concerns that voluntary standards must not transform to *de facto* obligations. Telecommunications Industry Association (TIA) urged the Commission to refrain from any regulatory requirements that would make an IoT labels program voluntary "in name only," such as by requiring the mark for equipment

[23] *See,* Information Technology Industry Council at 4; NCTA at 12.

[24] CTA at 8-10.

[25] CTIA at 11, 12.

[26] U.S. Chamber of Commerce at 3.

[27] USTelecom at 11-12.

authorization.[28] In initial comments, NTCA explored the statutory sections cited by the Commission and identified gaps between the purposes of those sections, as demonstrated by adjudicated proceedings in which those sections were invoked, and the intentions of the instant proceeding, as evidenced by the NPRM and its adjoining documents.[29] CTIA advised the Commission that the regulation of IoT security falls far beyond the boundaries of Commission authority and that regulations to govern cybersecurity *beyond* a voluntary IoT labeling program "would be a novel and expansive understanding of the [Commission's] core authority . . ." CTIA accordingly advises that Commission comportment to a voluntary program would mitigate jurisdictional concerns.[30]

III. CONCLUSION

There is general support for a NIST-based, voluntary labels program. However, such a program would need to be coordinated with other Federal agencies holding jurisdiction over various device sectors. Additionally, there remain substantial questions regarding the Commission's authority to implement a labels program. Ensuring that the program remains fully voluntary may obviate those concerns.

Respectfully submitted,

s/*Joshua Seidemann*
Joshua Seidemann, VP Policy and Industry Innovation
NTCA–The Rural Broadband Association
4121 Wilson Blvd., Suite 1000
Arlington, VA 22203
301-351-2000
www.ntca.org

DATED: November 10, 2023

[28] Telecommunications Industry Association at 2.

[29] NTCA at 8-11.

[30] CTIA at 44, 45.