Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

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

Comments of

NTCA–THE RURAL BROADBAND ASSOCIATION

Joshua Seidemann
VP Policy and Industry Innovation
NTCA-The Rural Broadband Association
4121 Wilson Blvd., Suite 1000
Arlington, VA 22203
703-351-2000
www.ntca.org

October 6, 2023

CONTENTS

Executive Summary i

I. Introduction 1

II. Discussion 2

A. Industry Led Efforts are Critical to Fortifying the Security of Connected Devices 2

B. Attempts to Promulgate IoT Standards Must be Tethered to the Statute 3

C. Voluntary Standards Must Not Transform to *de facto* Obligations 11

III. Conclusion 13

EXECUTIVE SUMMARY

NTCA supports industry-led efforts to enhance security in the IoT ecosphere. NTCA participates actively in government and industry workgroups; has filed in numerous relevant Federal dockets; and leads an industry cybersecurity program. Industry-led efforts combined with voluntary best practices enable rapid responses to evolving technical and market conditions and encourage consensus-driven guidelines that promote participation and reflect competitive interests in providing enhanced security to users. Accordingly, NTCA urges a careful examination before IoT standards are developed within the construct of regulatory oversight. Toward this end, and without diminishing the importance of ensuring the integrity of end-user IoT devices, it is not clear that sections of the Communications Act relating to radio interference provide a clear path toward the promulgation of IoT standards. Moreover, NTCA cautions strongly against approaches that could result in the inclusion of voluntary standards within mandatory regulatory guidelines.

Before the

FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

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

Comments of

NTCA–THE RURAL BROADBAND ASSOCIATION

To the Commission:

I. INTRODUCTION

NTCA–The Rural Broadband Association (NTCA) hereby submits these comments in the above-captioned proceeding.[1] NTCA supports efforts to enhance cybersecurity, including steps to increase cybersecurity awareness among consumers. In the realm of emerging and rapidly evolving technologies, NTCA consistently advocates the benefits of industry-led voluntary standards. This approach enables rapid response to meet technological advancements, as well as consensus-driven processes that reflect diverse knowledge and expertise within the industry. In that vein, voluntary, industry-led cybersecurity labels can be a sound component in encouraging more rigorous security for Internet of Thing (IoT) devices. At the same time, NTCA submits that voluntary standards must not trigger unanticipated consequences, including *de facto* regulatory requirements that could emerge if *intentionally* voluntary standards are incorporated into other regulatory requirements.

[1] *In the Matter of Cybersecurity Labelling for Internet of Things: Notice of Proposed Rulemaking,* Docket No. 23-239 (2023) (NPRM).

II. DISCUSSION

A. INDUSTRY-LED EFFORTS ARE CRITICAL TO FORTIFYING THE SECURITY OF CONNECTED DEVICES.

The Commission's inquiry into IoT labels is timely. U.S. households are now home to, on average, 22 connected devices, and nearly one-third of users with 20 or more connected devices report feeling overwhelmed managing their devices and associated subscriptions. More compelling, however, are data indicating that nearly one-quarter of users with 20 or more devices in a household have experienced two or more data security breaches in the past year.[2] These data are consistent with (and support) industry and government interest in promoting the security of IoT devices. Although NTCA itself is not strictly part of the app industry *per se*, it has led the charge promoting broadband and IoT among its rural broadband provider members. These applications support sectors that are critical to daily life and industry in rural spaces, including agriculture and healthcare.[3]

NTCA is sensitive to cybersecurity risks that accrue through connected devices, and participates actively in industry cybersecurity working groups and advocacy before Federal agencies on cyber issues. 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

[2] Susanne Hupfer, Michael Steinhart, "Shiny New Devices May Bring Joy, But Who's Protecting Consumer Data?," Deloitte Insights (Jan. 23, 2023).

[3] NTCA has published extensively on the role of broadband in agriculture, education, healthcare, and other sectors. Papers on these and other topics can be found at www.smartruralcommunity.org.

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 in Federal proceedings aimed at enhancing data security and privacy.[4]

Through these avenues, NTCA champions industry-led standards that emerge from collaborative interaction among stakeholders. This approach strikes a reasonable balance that earns "buy-in" from all parties and enables voluntary adoption of those aspects of standards that are most relevant and applicable to a given firm's operations. By way of example, NIST has undertaken significant work with industry to address the security of IoT devices. In May 2021, NIST issued a report on a Manufacturer Usage Description (MUD) standard to "reduce both vulnerability of IoT devices to network-based attacks and the potential for harm from any IoT devices that become compromised."[5] MUD standards are aimed at ensuring that broadband networks will permit IoT devices to transmit and receive only traffic that is required for device performance, while the network will block all other types of communications with the device, "thereby increasing the device's resilience to network-based attacks." Similarly, the National

[4] *See, i.e., Advance Notice of Proposed Rulemaking for Trade Regulation Rule on Commercial Surveillance and Data Security: Comments of NTCA–The Rural Broadband Association,* Docket ID 2022-17752, Federal Trade Commission (Nov. 21, 2022); *Developing a Privacy Framework: Comments of NTCA–The Rural Broadband Association,* Docket No. 181101997-8897-01, National Institute of Standards and Technology (Jan. 15, 2019); *Developing the Administration's Approach to Consumer Privacy: Comments of NTCA–The Rural Broadband Association,* Docket No. 180821780-8780-01, RIN 0660-XCO43, National Telecommunications and Information Administration (Nov. 9, 2018).

[5] NIST Special Publication 1800-15, "Securing Small-Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD)" (May 2021) (https://www.nist.gov/publications/securing-small-business-and-home-internet-things-iot-devices-mitigating-network-based) (visited Sep. 18, 2023).

Telecommunications and Information Administration (NTIA) developed the Software Bill of Materials, which focuses on security for the software supply chain.[6] These outcomes represent the collaborative work of industry stakeholders with expert Federal offices. The Commission recognizes the benefits of collaboration among government and industry, explaining this type of approach can "allow for the swift establishment and maturity of the program with broad industry and consumer acceptance that could adapt to a rapidly evolving threat landscape."[7]

B. ATTEMPTS TO PROMULGATE IoT STANDARDS MUST BE TETHERED TO THE STATUTE.

The Commission declares a laudable goal to "help consumers make informed purchasing decisions, differentiate trustworthy products in the marketplace, and create incentives for manufacturers to meet higher cybersecurity standards."[8] And indeed, as noted above, this is an increasingly critical issue as connected devices proliferate and become increasingly interwoven with aspects of daily life. These include, of course, not only matters of convenience such as connected thermostats or home appliances, but devices that collect, monitor, and respond to personal health or financial information. Additionally, sweeping transformations in industrial and agricultural IoT applications demand close and significant industry attention to security, updating, and user awareness of these devices and attendant risks.

Cybersecurity cannot be measured easily. The susceptibility of a device to inadvertent or adversarial intrusion relies in part on the context in which it is deployed and the user's individual protective measures. And, as the Commission alludes in the NPRM, the dynamic environment in

[6] "NTIA Releases Minimum Elements for a Software Bill of Materials" (Jul. 2021) (https://www.ntia.gov/page/software-bill-materials) (visited Sep. 18, 2023).

[7] NPRM at para. 19.

[8] "FACT SHEET: Securing Smart Devices – The FCC's Proposed Voluntary Cybersecurity Labeling Program for Internet-Enabled Devices," at 1.

which IoT devices are deployed, including changing tactics of adversarial actors, can render risky today a device that was deemed secure only yesterday.[9] Moreover, the natural progression of technological development that produces devices with more built-in security will organically characterize older devices as less secure, particularly as support and updates for those devices expire. And yet as opportunities for vulnerabilities increase, industry and government are confronted with the question of which body (government, industry, or both), is best equipped to be, in the expression of NIST, the "Scheme Owner"?[10] This question transcends questions of expertise alone and enters discussions of jurisdiction.

The Commission tentatively concludes that it has authority to adopt the IoT labeling program, relying on Section 302(a) of the Act, which authorizes the Commission, "consistent with the public interest, convenience, and necessity, [to] make reasonable regulations (1) *governing the interference potential of devices* which in their operation are capable of emitting radio frequency energy by radiation, conduction, or other means in sufficient degree to cause *harmful interference to radio communications . . .*"[11] In support of its proposals, the Commission cites two prior proceedings in which it relied on Section 302(a). In a Citizens Broadband Radio Service (CBRS) proceeding, Section 302(a) was invoked to secure software and firmware in order to prevent compromising devices or the data that they transmit.[12] The Commission mandated that end user devices must "contain security features sufficient to protect against

[9] *See,* NPRM at paras. 47, 48.

[10] *See,* "Recommended Criteria for Cybersecurity Labelling for Consumer Internet of Things (IoT) Products," National Institute of Standards and Technology (Feb. 2, 2022) (https://doi.org/10.6028/NIST/CSWP.02042002-2).

[11] NPRM at para. 57, emphasis added (internal citation omitted).

[12] *See, Amendment of the Commission's Rules with Regard to Commercial Operations in the 3550-3650 Mhz Band: Report and Order and Second Further Notice of Proposed Rulemaking,* Docket No. 12-354, FCC 15-47, 30 FCC Rcd 3959 (2015) (CBRS Order).

modification of software or firmware by any unauthorized parties" and that those devices "be able to protect the communication data that are exchanged between these elements."[13] That proceeding, however was aimed at opening for consumer use spectrum that had been previously reserved for military applications. As an overarching approach, the Commission adopted a three-tier authorization model that protected military needs while relegating other users to protocols that are substantively similar to the standards that apply for unlicensed spectrum (to not interfere, and to accept interference).[14] The CBRS proceeding evinced a prevailing interest in protecting incumbent military operations, as the Commission explained that its actions would ensure that civilian end user devices would not interfere with and potentially compromise military applications.[15] In similar vein, the Commission adopted security measures in a 5G proceeding to prevent manufacturers from making software changes that could enable unlicensed national information infrastructure (U-NII) devices to operate outside of authorized device parameters.[16] The Commission established rules to require protocols to "ensure the integrity of transmission" between white spaces devices and databases.[17] But here, too, the focus was on ensuring that devices operate only within their authorized spectrum range in order to not interfere with others' communications. This proceeding, too, focused more on the traffic of communications – in

[13] NPRM at para. 58, *citing*, CBRS Order at para. 240 (2015).

[14] *See, i.e.,* FCC 15-47 at para. 36.

[15] FCC 15-46 at para. 241.

[16] NPRM at para. 58, *citing Revision of Part 15 of the Commission's Rules to Permit Unlicensed National Information Infrastructure (U-NII) Devices in the 5GHz Band: First Report and Order,* Docket No. 13-49, 29 FCC Rcd 4127, 4143, at para. 54 (2014).

[17] NPRM at para. 58.

essence, spectrum management – than the security or data privacy concerns that are at the heart of the instant inquiry.

In contrast, the instant proceeding is characterized as "similar to the Energy Star program, which was created to help consumers identify energy-efficient appliances and encourage more companies to produce them in the marketplace – but for more cybersecure smart devices."[18] Indeed, the NPRM opens with sweeping explanation about the need for IoT security. The NPRM explains,

> Consumers have come to rely on the functionality and convenience of their smart devices, which run the gamut from home office routers to personal digital assistants, Internet-connected home security cameras, voice-activated shopping devices, Internet-connected appliances, fitness trackers, GPS trackers, medical devices, garage door openers, and baby monitors . . . With more than 25 billion connected IoT devices predicted to be in operation by 2030, consumers need tools that allow them to understand the relative security risk that an IoT device or product may pose . . . and to have a level of confidence whether the IoT devices they ultimately purchase meet certain cybersecurity standards.[19]

This platform is echoed in the Fact Sheet and the separate statements of the Commissioners,[20] creating an impression that the intent of the instant proceeding is to protect the integrity of end-user IoT devices and products. This aim is evident in the NPRM discussions that seek comment on how internal IoT devices might be addressed as connected to or apart from the products in which they operate[21] (for example, the difference between an IoT component and the home appliance in which it is installed). These goals, then, must be squared with Section 302(a), which

[18] "FACT SHEET: Securing Smart Devices – The FCC's Proposed Voluntary Cybersecurity Labeling Program for Internet-Enabled Devices," at 1.

[19] NPRM at para. 1.

[20] *See,* NPRM at Separate Statements of Chairwoman Rosenworcel and Commissioners Starks and Simington.

[21] *See,* NPRM at para. 13.

addresses the potential of radio frequency (RF) devices to "cause harmful interference to radio communications" or to be susceptible to interference from RF energy.[22]

The Commission explains that "interference issues also could arise if security vulnerabilities were exploited to use a device as an interference generator, or to transmit at times and intervals selected by the attacker to interfere with other devices."[23] And were that the primary concern of the proceeding and the thrust of the proposals then made, then it could seem a reasonable application of Section 302(a) to address that narrow issue. But the instant proceeding contemplates a far broader impact than, and appears to arise from concerns distinctly different than, interference with devices. Rather, the instant proceeding reflects the Commission's interest in protecting consumer data and operation of IoT devices and connected products. This is evident not only from the Commission's Fact Sheet and the separate statements of the Commissioners, but also the NPRM, which introduces the instant proceeding with summaries of other government and industry efforts aimed at protecting IoT security, specifically, the security of user data and operational integrity of devices, as opposed to the security of the communications network. To be sure, the NPRM cites the hazard of Denial of Service (DoS) attacks, but the overwhelming tone of the discussion is consistent with the concerns expressed in the Fact Sheet and statements of the Commissioners, specifically, end-user

[22] 47 U.S.C. § 302(a). In full, the section reads:

> The Commission may, consistent with the public interest, convenience, and necessity, make reasonable regulations (1) governing the interference potential of devices which in their operation are capable of emitting radio frequency energy by radiation, conduction, or other means in sufficient degree to cause harmful interference to radio communications; and (2) establishing minimum performance standards for home electronic equipment and systems to reduce their susceptibility to interference from radio frequency energy. Such regulations shall be applicable to the manufacture, import, sale, offer for sale, or shipment of such devices and home electronic equipment and systems, and to the use of such devices.

[23] NPRM at para. 59.

impacts, including: spreading spam emails,[24] stealing sensitive data,[25] suppressing security alarm systems,[26] stopping unauthorized intruders from tampering with connected devices,[27] protecting consumer privacy,[28] minimizing security risks,[29] and cybersecurity.[30] These concerns, as critical as they are, speak more to data security and less to interference with radio communications themselves.

And yet it is not clear that the Act intends to reach those places. The Commission offers that section 302(a)(2) of the Act provides authority to adopt reasonable regulations "establishing minimum performance standards for home electronic equipment and systems to reduce their susceptibility to interference from radio frequency energy."[31] Whether that authority reasonably extends to the further, broader field of IoT device security begs 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.

The NPRM itself asks this question as it presents Section 333 as an additional proposed basis of jurisdictional authority. The section provides, "No person shall willfully or maliciously interfere with or cause interference to any radio communications of any station licensed or

[24] NPRM at fn.6.

[25] NPRM at fn.6.

[26] NPRM at fn.8.

[27] NPRM at fn.11.

[28] *Id.*

[29] *Id.*

[30] *Id.*

[31] NPRM at para. 59.

authorized by or under this chapter or operated by the United States Government."[32] "Station" is defined by the Commission as "[o]ne or more transmitters or receivers or a combination of transmitters or receivers, including the accessory equipment, necessary at one location for carrying on a radiocommunication service, or the radio astronomy service."[33] But here, too, the statute directs itself to the integrity of the communication, as opposed to the operation of a follow-on device; the statute has been invoked, for example, to address Wi-Fi blocking and unauthorized transmission on government frequencies.[34] The legislative history of Section 303 focuses on

> . . . intentional jamming, deliberate transmission on top of the transmissions of authorized users already using specific frequencies in order to obstruct their communications, repeated interruptions, and the use of transmissions of whistles, tapes, records, or other types of noisemaking devices to interfere with the communications or radio signals of other stations.[35]

It is not clear that the NPRM itself embraces Section 333 to capture IoT devices, asking whether that section, "possibly coupled with other provisions," provides authority, or whether the IoT labels proposal is "necessary or reasonably ancillary to the execution of [its] implementation of any or all of these statutory responsibilities."[36] The Commission also seeks comment on its broad authority under Titles II and III and section 4(i) to "perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with this chapter, as may be necessary in the

---

[32] 47 U.S.C. § 333.

[33] 47 C.F.R. § 2.1.

[34] *I/M/O M.C. Dean, Inc.: Notice of Apparent Liability for Forfeiture,* File No. EB-SED-15-00018428, NAL/Acct. No.: 201632100003, FRN: 0011134921, FCC 15-146 (2015); *I/M/O Jason M. Frawley, Licensee of Amateur Radio Station WA7CQ, Lewiston, Idaho: Notice of Apparent Liability and Forfeiture,* File No. EB-FIELDWR-21-00032537, NAL/Acct. No.: 202232030001, FRN: 0002984920, FCC 22-43 (2022).

[35] H.R. Rep. No. 101-316, at 8 (1989).

[36] NPRM at para. 60, *citing Comcast v. FCC,* 600 F.3d 642 (D.C. Cir. 2010).

execution of its functions," including "promoting safety of life and property."[37] The lack of clear jurisdiction suggests the usefulness of examining this issue through the lens of ancillary jurisdiction principles. This analytical construct can help focus the inquiry and refine approaches to the NPRM's questions about jurisdictional authority.

As a baseline, we look to the ancillary jurisdiction test as stated in *Verizon v. FCC,* which tested the Commission's reliance on ancillary jurisdiction to regulate broadband internet access services in the Open Internet proceeding.[38] The test permits the Commission to regulate "interstate or foreign communications by wire or radio" if (1) the exercise of ancillary authority can be linked to an express delegation of ancillary authority, as opposed to a "policy statement," and (2) the action does not conflict with other principles of the Act.[39] IoT concerns (compelling, important, and critical as they are) agitate far afield from RF interference issues with which Sections 302 and 333 address. It is not clear that a voluntary IoT label program intended to increase consumer confidence serves the explicit concerns of diminishing radio interference as contemplated in Sections 302(a) and 333. Likewise, the sweeping interest in "promoting safety of life and property"[40] emerges as more of a policy statement than a statutory directive; the promulgation of standards must be contained by the principle that agencies do not possess "unbounded" authority.[41] The promulgation of IoT standards that conceivably affect markets in

[37] NPRM at para. 64, *citing* 47 U.S.C. § 151.

[38] *See, Verizon v. FCC,* 740 F.3d 623 (D.C. Cir. 2014) (Verizon). In this case, Verizon challenged the "Net Neutrality Order," *Preserving the Open Internet,* 25 FCC Rcd. 17905 (2010), which imposed disclosure, anti-blocking, and anti-discrimination requirements on broadband internet access service providers.

[39] Verizon at 632, 634.

[40] 47 U.S.C. § 151.

[41] *See, American Library Association v. FCC,* 406 F.3d 689, 694 (D.C. Cir. 2005).

which the Commission does not currently engage raises bracing questions about the extent to which even voluntary standards might reach.

C. VOLUNTARY STANDARDS MUST NOT TRANSFORM TO *DE FACTO* OBLIGATIONS

To be sure, the basic approach set forth by the Commission is consistent with prior NTCA advocacy on similar issues: Flexible industry-led guidelines can respond quickly to evolving technological and market needs while preserving the power of consumer decisions without undue regulatory imprints. In a competitive market-based setting, participants will be inclined to ensure their products meet common security demands, and an IoT label or similar ranking device should encourage developers and manufacturers to reach for the "gold standard" of security in order to promote their product effectively in the marketplace. And the Commission articulates the broad range of this marketplace - personal digital assistants, Internet-connected home security cameras, voice-activated shopping devices, Internet-connected appliances, fitness trackers, GPS trackers, medical devices, garage door openers, and baby monitors.[42] An industry-led, voluntary standard to assist consumers that draws upon industry consensus and can respond rapidly to evolving technology is preferable to government-mandated guidelines. But these standards must remain voluntary and should not be attached to regulatory programs or other obligations.

While the Commission asserts that participation would be voluntary, it notes that participation would be governed "in accordance with the regulations the Commission adopts in this proceeding, including but not limited to IoT security standards, compliance requirements, and the labeling program's operating framework."[43] Setting aside the jurisdictional issues

[42] NPRM at para. 1.

[43] NPRM at para. 57.

discussed above, NTCA submits that any Commission action must contain a clear commitment that voluntary standards will not become *de facto* regulations by bootstrapping them to existing obligations or other rules. Moreover, any program should clarify that firms relying on devices bearing a label can enjoy reasonable reliance on equipment manufacturers 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. Further, to the extent that future actions could effectively eschew voluntary standards by incorporating them into regulatory obligations, a safe harbor for already-deployed devices must be implemented. At bottom, even if jurisdiction to act in this proceeding exists, voluntary standards should not be baked into mandatory compliance.

The Consumer Products Safety Commission (CPSC) offers a cogent example of how voluntary standards can fortify a backstop without inducing regulation. By design, the CPSC demurs from rulemaking and instead relies on industry-led standards for the prosecution of its consumer protection mandate. The Consumer Product Safety Act (CPSA)

> requires the [CPSC] to defer to 'voluntary consumer product safety standards' that are predominantly drafted and developed by private industry. In light of this mandate, the CPSC provides technical assistance and otherwise helps industry groups develop voluntary standards more frequently than it issues mandatory safety standards through rulemakings.[44]

Most products that fall beneath the CPSC's jurisdiction are governed by voluntary industry standards. Congress has expressly directed the CPSC to promulgate mandatory consumer safety rules in some instances, but the CPSC is generally required to "defer to industry-developed voluntary safety standards." However, these voluntary standards do

[44] David Carpenter, "The Consumer Product Safety Act: A Legal Analysis," Congressional Research Service, at 1 (Apr. 24, 2018) (CRS).

not equate to a lack of agency involvement. In the first instance, the CPSC issues regular reports on voluntary industry standards. The standards are usually developed by industry groups such as American National Standards Institute (ANSI), Underwriters Laboratory (UL), or other bodies that combine trade organizations, researchers, and consumer advocates.[45] NTCA submits that this approach offers a model for Commission involvement in IoT security should jurisdiction to act be more firmly established in the first instance. Much the way NIST has coordinated cybersecurity efforts with the industry, to the extent that its statutory authority indeed permits, the Commission could serve a similar role for the discrete purpose of developing an IoT label. The label would not be required, nor "bootstrapped" onto regulatory obligations, but could be indicative of a developer's overall posture in the marketplace.

III. CONCLUSION

NTCA supports industry-led efforts to enhance security in the IoT ecosphere. This approach enables rapid responses to evolving technical and market conditions, and encourages consensus-driven guidelines that promote participation and reflect competitive interests in providing enhanced security to users. NTCA notes that the Act does not provide a clear

[45] CRS at 12. To be sure, the process is not perfect. Certain cost-benefit analyses undertaken by the CPSC have resulted in what observers have defined as "paralysis by analysis." CRS at 9, fn. 94. The CPSC worked with the window covering industry for more than 20 years to develop voluntary standards for window blind cords. GAO report at 9, fn.96; *see also* "Updated Voluntary Window Covering Safety Standard Takes Effect: Go Cordless," Consumer Product Safety Commission (Dec. 18, 2018) (https://www.cpsc.gov/Newsroom/News-Releases/2019/Updated-Voluntary-Window-Covering-Safety-Standard-Takes-Effect-Go-Cordless) (visited Nov. 16, 2022). But that does not mean that in the intervening years industry was not culpable for death or injury. Rather, cases were in fact litigated and a body of case law provided instructive direction for manufacturers. But a uniform, industry-accepted standard did not exist.

jurisdictional path toward IoT management, and cautions against approaches that could result in the inclusion of voluntary standards in mandatory regulatory guidelines.

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
703-351-2000
www.ntca.org

DATED: October 6, 2023