Before the
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, DC 20230

In the Matter of	)	
	)	
Request for Comments on Proposals and Positions for the 2020 World Telecommunication Standardization Assembly	)	Docket No. 200504-0126 RIN 0660-XC04
	)	
	)	

COMMENTS OF THE CONSUMER TECHNOLOGY ASSOCIATION

Consumer Technology Association ("CTA")®[1] applauds NTIA for seeking input from stakeholders and interested parties to help develop its proposals and positions regarding matters that will be addressed at the upcoming 2020 World Telecommunication Standardization Assembly ("WTSA–2020") of the International Telecommunication Union ("ITU").[2] As NTIA notes, the WTSA, which occurs every four years, sets the agenda for the ITU Telecommunication Standardization Sector ("ITU–T") for the next four years as well as ITU–T Study Group leadership.

The WTSA–2020 is an important forum where the United States should reaffirm its commitment to voluntary global standards that are open and that facilitate the interoperability of communications and information devices and apps. CTA agrees with NTIA that the "ITU has a role within its limited scope and remit."[3] For example, "ITU should provide a consensus-driven,

[1] As North America's largest technology trade association, CTA® is the tech sector. Our members are the world's leading innovators—from startups to global brands—helping support more than 18 million American jobs. CTA owns and produces CES®—the largest, most influential tech event on the planet.

[2] *Request for Comments on Proposals and Positions for the 2020 World Telecommunication Standardization Assembly*, Docket No. 200504-0126, RIN 0660-XC04, 85 Fed. Reg. 27,390 (May 8, 2020) ("*RFC*").

[3] *Id.* at 27,391.

transparent forum for issues appropriate to its own mission (e.g., interconnection)."[4] The U.S. delegation to WTSA–2020 should be vigilant to keep the ITU–T from taking any action, inadvertent or otherwise, that would disrupt the present successful voluntary standards environment.

CTA is deeply interested in the outcome of the WTSA–2020 because CTA represents the U.S. consumer technology industry. The success of this industry and the people it serves depends on the continued availability of open, voluntary standards processes. Government actors should allow the private sector to take the lead on standards development, relying on consensus-based standards, not top-down regulatory frameworks, to ensure interoperability, reliability, and security.

I. INDUSTRY-LED, OPEN, AND VOLUNTARY GLOBAL STANDARDS FOR COMMUNICATIONS AND INFORMATION TECHNOLOGIES LEAD TO BETTER AND MORE INNOVATIVE OUTCOMES

The United States should reaffirm its commitment to voluntary global standards that are open and that facilitate the interoperability of communications and information devices and apps. CTA supports the NTIA's proposal "to advocate for standards from [Standards Developing Organizations ("SDOs")] developed using a consensus-based, industry-driven approach; that industry should lead international standards development processes, and that those processes should be transparent and open."[5] Specifically, NTIA should advocate for the ITU–T to encourage industry-led, open, and voluntary global standards for communications and information technologies. The ITU–T should not duplicate, replace, or interfere with existing efforts, particularly with respect to issues outside the ITU's core mission. For example, there

[4] *Id.*

[5] *Id.* at 27,393; *see also* Open Stand, Principles, https://open-stand.org/about-us/principles (last visited June 5, 2020).

may be a role for the ITU–T with respect to 5G—IMT-2020 with regard to radio access/interconnection. In contrast, as noted further below, ITU–T should not engage in 5G security or supply chain security issues. As in other areas of telecommunications, consensus-based technical standards and interoperability in 5G are most likely to reflect the most current technological developments and the most practical solutions available. For instance, many CTA members are engaged in promoting open and interoperable standards for Radio Access Networks and other aspects of advanced telecommunications networks through initiatives such as the O-RAN Alliance, the Open RAN Policy Coalition, and the Telecom Infra Project.

The consumer technology marketplace is both innovative and competitive in the United States and worldwide. The current voluntary global standards process reflects this competitive environment by promoting innovation and flexibility while providing for interoperability and security. ITU-T standards setting, in contrast, has historically focused on the evolution of telephony as a network service. The NTIA should prioritize ITU-T work within that core mission area and caution the ITU-T against efforts to compete in areas already being studied and standardized elsewhere. NTIA should prioritize ITU–T work in the ITU's core mission areas and caution ITU against "scope creep" into areas already being studied and standardized by other important organizations.

A wide range of industry led, multistakeholder SDOs are already leading the development of telecommunications and information standards with respect to artificial intelligence ("AI")/machine learning ("ML"), consumer protection, cybersecurity, digital economy, Internet of Things ("IoT"), healthcare tech, and unmanned aerial vehicles ("UAVs"). Standards studies for these emerging technologies are best left to the organizations

already working in these areas such as ISO ("International Organization for Standardization"),[6] International Electrotechnical Commission ("IEC"),[7] regional groups (*e.g.* ETSI) and industry groups (*e.g.* IEEE[8] and CTA[9]). For example:

- ***Artificial Intelligence/Machine Learning***. This past February, CTA announced the release of the first-ever ANSI-approved standard for the use of AI in healthcare.[10] CTA's AI Committee also published a separate ANSI-approved standard defining more than 30 terms relating to AI and ML, reflecting "the pervasiveness of AI-enabled technology across the entire consumer technology industry."[11] IEEE recently published a standard for measuring the impact of AI and related systems on humans, which is important to understand as AI and related systems are increasingly used.[12]

- ***Consumer Protection.*** Industry stakeholders work together to address myriad consumer protection issues. For example, to help protect consumers from illegal robocalls, the communications industry developed the STIR/SHAKEN authentication framework to provide end-to-end cryptographic authentication and verification of telephone identity

---

[6] *See* ISO, About Us, https://www.iso.org/about-us.html ("ISO is an independent, non-governmental international organization with a membership of 164 national standards bodies.").

[7] *See* International Electrotechnical Commission, About the IEC, https://www.iec.ch/about/?ref=menu ("The International Electrotechnical Commission (IEC) is the world's leading organization that prepares and publishes International Standards for all electrical, electronic, and related technologies. Close to 20,000 experts from industry, commerce, government, test and research labs, academia, and consumer groups participate in IEC Standardization work.").

[8] *See* Institute of Electrical and Electronics Engineers, About IEEE, http://www.ieee.org/about/index.html ("IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity. IEEE and its members inspire a global community to innovate for a better tomorrow through its more than 419,000 members in over 160 countries, and its highly-cited publications, conferences, technology standards, and professional and educational activities.").

[9] CTA has an extensive Technology and Standards program that includes more than 70 committees, subcommittees, and working groups; roughly 1,100 participants; and holds American National Standards Institute ("ANSI") accreditation.

[10] Riya Anandwala and Danielle Cassagnol, CTA, Press Release, *CTA Launches First-Ever Industry-Led Standard for AI in Health Care* (rel. Feb. 25, 2020), https://www.cta.tech/Resources/Newsroom/Media-Releases/2020/February/CTA-Launches-First-Ever-Industry-Led-Standard.

[11] *Id.*

[12] IEEE SA, 7010-2020 - IEEE Recommended Practice for Assessing the Impact of Autonomous and Intelligent Systems on Human Well-Being (published May 1, 2020), https://standards.ieee.org/standard/7010-2020.html.

and other information in voice calls.[13] In addition, the U.S. Consumer Product Safety Commission relies on collaboration with voluntary standard organizations, including ANSI, ASTM, CSA, and UL, to develop consensus-based consumer product safety practices.[14] In the communications and technology space, such standards address baby monitors, batteries, and smoke alarms, among many other products.[15]

- ***Cybersecurity.*** As discussed in the next section, CTA co-leads, with USTelecom, a major multistakeholder forum convening and supporting efforts to improve cybersecurity, the Council to Secure the Digital Economy ("CSDE"), a group of more than a dozen major information and communications technology and services ("ICTS") companies deeply invested in the security of our communications infrastructure and connected products ecosystem. Additionally, ISO and IEC, based on input from national bodies, have made significant progress on such standards.

- ***Internet Standards.*** Standards groups including the IETF, W3C, and ISO, as well as supporting organizations like ICANN, the regional Internet registries, and other international bodies are adequately managing the development and evolution of Internet protocols and ecosystems. Given that existing work, the ITU–T's efforts to produce non-interoperable competitive approaches, such as "New IP" are not needed and in fact are counter-productive.

- ***Internet of Things.*** Numerous groups are developing technical standards to speed the growth, adoption, and utility of the IoT. Along with CTA, these include groups like IEC, IEEE, IIC, W3C, Wi-Fi Alliance, OneM2M, the ZigBee Alliance, and many others.[16] A relatively nascent vertical, marketplace competition for IoT—including relevant standards—is successfully driving innovation.

- ***Over-the-Top Services.*** The technical standards for any over-the-top ("OTT") service provider to reach any viewer in the world are already in place. Industry bodies including MPEG (a working group of the ISO/IEC Joint Technical Committee 1) and W3C host numerous experts and standards on OTT. Other bodies including 3GPP, ATSC and

---

[13] *See* Alliance for Telecommunications Industry Solutions, ATIS-1000074, Signature-based Handling of Asserted information using toKENs (SHAKEN) (approved Jan. 5, 2017), https://www.atis.org/sti-ga/resources/docs/ATIS-1000074.pdf.

[14] *See* Consumer Product Safety Commission, Voluntary Standards, https://www.cpsc.gov/Regulations-Laws--Standards/Voluntary-Standards.

[15] *See id.*

[16] *See, e.g.*, Postscapes Tech, IoT Standards and Protocols (Jan 2, 2020), https://www.postscapes.com/internet-of-things-protocols; Federal Communications Commission Technological Advisory Committee, *FCC-TAC IOT Working Group Standards* (2014), https://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting12414/FCC-TAC-IOT-Working-Group-IOT-Standards-Filter-Final.xlsx (reviewing many IoT standardization efforts).

HbbTV are handling region and category-specific application of these standards. The WAVE Project at CTA is coordinating interoperability within the OTT ecosystem.[17]

- ***Personal Data Protection.*** The data protection landscape is becoming increasingly complicated with the emergence of new data protection regimes in this country and across the globe. Industry coordinating with government agencies already is working to develop interoperable frameworks, as well as best practices to address certain privacy issues. For example, earlier this year, after a process engaging public and private stakeholders, the National Institute of Standards and Technology ("NIST") released the *NIST Privacy Framework* to help organizations manage their privacy risk, regardless of the legal or regulatory standards that apply.[18] Separately, to address data issues associated with emerging health technologies, CTA has published the *Guiding Principles for the Privacy of Personal Health and Wellness Information*.[19]

- ***Unmanned Aerial Vehicles/Unmanned Aircraft Systems.*** SDOs specializing in both aviation and wireless communications have made substantial progress on standards for the manufacture, operation, and communication of UAVs.[20] Although the ITU has a role to play with respect to radio frequencies that UAVs may utilize, standardization is already underway and does not require the same effort at the ITU–T. Further, the operation of UAVs are typically regulated by domestic civil aviation authorities which

---

[17] *See* CTA, Web Application Video Ecosystem Project: Announcing the WAVE Project for Internet video interoperability, https://standards.cta.tech/kwspub/wave; Press Release, CTA, *Internet Video Leaders Announce Interoperability Effort* (Dec. 22, 2015) (explaining that the project "will develop 'profiles' or specifications referencing key features of industry standards from IETF, MPEG and the W3C for interoperable, commercial video delivery. These profiles will provide the basic common understanding of interoperability from the streaming content provider, through the content delivery networks to the edge, and at the device player"), http://www.cta.tech/News/News-Releases/Press-Releases/2015-Press-Releases/Internet-Video-Leaders-Announce-Interoperability-E.aspx.

[18] NIST, *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0* (rel. Jan. 16, 2020), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf.

[19] CTA, *Guiding Principles for the Privacy of Personal Health and Wellness Information* (2019), https://cdn.cta.tech/cta/media/media/membership/pdfs/final-cta-guiding-principles-for-the-privacy-of-personal-health-and-wellness-information.pdf.

[20] *See, e.g.*, ASTM International, Committee F38 on Unmanned Aircraft Systems, https://www.astm.org/COMMIT/SUBCOMMIT/F38.htm (listing four subcommittees developing standards with respect to airworthiness; flight operations; personnel training, qualification, and certification; and executive); Alliance for Telecommunications Industry Solutions, *Support of UAV Communications in 3GPP Cellular Standards* (Oct. 2018), https://access.atis.org/apps-/group_public/download.php/42855/ATIS-I-0000069.pdf; 3rd Generation Partnership Project, UAS – UAV (Nov. 18, 2019), https://www.3gpp.org/uas-uav (discussing 3GPP releases and studies related to UAS). CTA itself has developed a standard that outlines the elements and characteristics of a serial number to be used by small unmanned aerial systems. ASNI, CTA, CTA 2063-2017 (ANSI) Small Unmanned Aerial Systems Serial Numbers, https://webstore.ansi.org/Standards/ANSI/CTA20632017ANSI.

coordinate through intergovernmental bodies such as the International Civil Aviation Organization which, in turn, can seek the support they need from the ITU–T.

- ***Smart Cities.*** ETSI has published standards specifically tailored to the concerns of smart cities, including a standard to define key performance indicators ("KPI") to aid decisionmakers.[21] ETSI's KPI standard references two ITU-T recommendations in addition to an ISO standard, demonstrating that generalized ITU-T recommendations—here with respect to methodologies for measuring the environmental impact of information and technologies—can provide a foundation for more specialized consensus-standards with respect to emerging technologies.[22]

The ITU–T need not address these technologies, where the private sector and regional standards bodies are already coordinating successfully. Indeed, NTIA correctly proposes to oppose ITU–T action on the following topics, which CTA agrees are "completely outside the ITU–T remit:" consumer protection, personal data protection, healthcare technology, and unmanned aerial vehicles.[23]

Rather than independently developing standards, the ITU can be helpful by encouraging and adopting industry standards, as it has done with H.264 in video compression.[24] Recognition by the ITU was an important step in the widespread adoption of the technology, especially as it accepted industry-developed consensus standards as international standards.[25] Approving an industry standard, however, is far different from actively spending resources creating a standard and forcing entities to duplicate fees and resources at the ITU and ITU–T. Activities should be

[21] *See, e.g.*, ESTI, Operational energy Efficiency for Users (OEU); KPIs for Smart Cities DGS/OEU-0019 v1.1.1 (2017-08), https://www.etsi.org/deliver/etsi_gs/OEU/001_099/019/01.01.01_60/gs_OEU019v010101p.pdf.

[22] *Id.* at 6.

[23] *RFC* at 27,392.

[24] H.264 was the result of a joint effort between ITU-T and ISO/IEC JTC1 MPEG.

[25] *See RFC* at 27,392 (seeking comment on the importance of ITU-T recommendations and whether there is a wide implementation of ITU-T recommendations in the United States).

limited to either developing standards in an ITU core competency or recognizing a voluntary, industry-led, consensus standard.

II. CTA CO-LEADS A PROMINENT EXAMPLE OF A MULTISTAKEHOLDER FORUM ADVANCING CYBERSECURITY

CTA agrees with NTIA's intention to "further the multistakeholder approach to internet policy."[26] In addition to consensus-standards, multistakeholder fora allow the private, public, and international body sectors to collaborate. As noted above, CTA co-leads, with USTelecom, one prominent and influential example of such a multistakeholder forum, the CSDE, a group of more than a dozen major ICTS companies deeply invested in the security of our communications infrastructure and connected products ecosystem.[27] CSDE has convened important discussions and produced tools to aid companies and governments alike. Such an approach should also continue to be used for the development of IoT device security baselines.

In November 2018, CSDE released the International Anti-Botnet Guide ("Guide").[28] The Guide is a playbook that offers companies across the digital ecosystem a set of baseline tools, practices and processes they can adopt to help protect against the threat of botnets and other automated, distributed attacks. The Guide provides a flexible approach for IoT devices of varying processing capabilities and data types, providing companies with a range of options to appropriately address security risks. This past November, CSDE released updates to the Guide for 2020.[29]

---

[26] *See generally RFC* at 27,392 (Section V).

[27] *See* Council to Secure the Digital Economy, Member Companies, https://securingdigitaleconomy.org/member-profiles (last visited June 2, 2020).

[28] *See* CSDE, *International Botnet and IoT Security Guide 2018*, https://www.ustelecom.org/wp-content/uploads/2018/11/CSDE-Anti-Botnet-Report-final.pdf.

[29] CSDE, *International Botnet and IoT Security Guide 2020*, https://securingdigitaleconomy.org/wp-content/uploads/2019/11/CSDE_Botnet-Report_2020_FINAL.pdf.

In 2019, through CSDE, CTA convened 20 major cybersecurity and technology organizations, industry associations, consortia, and standards bodies—all groups that convene their own security-focused memberships. This unprecedented industry effort, known as "Convene the Conveners" or "C2," sought to identify baseline security capabilities for the rapidly growing IoT marketplace to address four challenges:

1. Promoting global harmonization to prevent fragmentation of security specifications and requirements.
2. Working with emerging global market forces that naturally favor secure devices and systems.
3. Developing a coherent common language on these issues that is compelling to various policy and technical audiences.
4. Assisting policy development internationally and in the United States, including at the state level.

The final version of this effort was released on September 17, 2019.[30] Through this effort and other avenues, CTA and many of its member companies have collaborated closely with leaders at NIST—in particular, assisting NIST in its thoughtful approach to developing a "Core Baseline for IoT Devices" recently finalized in NISTIR 8259A, *IoT Device Cybersecurity Capability Core Baseline*,[31]—as well as with NTIA, the Department of Homeland Security, and other government agencies.

The United States government's efforts in developing the Roadmap Toward Resilience Against Botnets and the work that has followed also represent how a multistakeholder process

[30] CSDE, *The C2 Consensus on IoT Device Security Baseline Capabilities*, *https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf*.

[31] Michael Fagan et al., *NISTIR 8259A, IoT Device Cybersecurity Capability Core Baseline* (May 2020), https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259A.pdf; *see also Michael Fagan et al., NISTIR 8259, Foundational Cybersecurity Activities for IoT Device Manufacturers* (May 2020), https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf.

can achieve results. CSDE worked closely with the Departments of Commerce and Homeland Security in their development of *A Roadmap Toward Resilience Against Botnets*.[32] The development of the C2 Consensus is one outcome of that multistakeholder process.

CTA has also convened a working group of cybersecurity experts to draft a voluntary industry consensus standard for IoT baseline security.[33] This document (draft CTA-2088) is in the final stages of approval and publication and is anticipated by manufacturers, retailers, and other stakeholders as an important element of the drive to secure the IoT.

CSDE's success in creating the Guide, C2 Consensus, and its recent work with the Departments of Commerce and Homeland Security represent the strengths of a multistakeholder process. The multistakeholder process is succeeding in the United States and it will continue working globally.

III. THE ITU SHOULD AVOID GOVERNMENT-CENTRIC APPROACHES TO 5G SUPPLY CHAIN SECURITY

CTA's technology security efforts have historically focused on technical standards activities pertinent to consumer technology, but in recent years—as consumer technology has itself become more pertinent to broader ICTS ecosystem security concerns—CTA has significantly broadened and deepened its security efforts. For instance, CTA is an active member of the Sector Coordinating Councils for both the Information Technology and the Communications sectors. Over the past several years, CTA's engagement with the government

---

[32] *See, e.g.*, U.S. Department of Homeland Security & U.S. Department of Commerce, *A Roadmap Toward Resilience Against Botnets* (Nov. 29, 2018), https://www.commerce.gov/sites/default/files/2018-11/Botnet%20Road%20Map%20112918%20for%20posting_1.pdf (noting that CSDE will be a contributor for numerous tasks described in the Road Map).

[33] *See generally* CTA, Status of Active Consumer Technology Association Projects, https://standards.cta.tech/kwspub/current_projects (noting that CTA's R14 Cybersecurity and Privacy Management Committee WG1 is working to turn the Guide's language of best practices into technical standard language) (last visited June 2, 2020).

promoted security approaches characterized by a focus on risk management and industry-government collaboration. Similarly, this model of government-facilitated industry leadership through partnership and collaboration across government is working to secure the 5G supply chain. For instance:

- The Communications Sector Coordinating Council contributed substantially to the first version of DHS's risk assessment required under Section 5(b) of EO 13873, and industry will continue to do so in the subsequent updates and improvements of this required annual assessment.

- The ICT Supply Chain Risk Management Task Force is a formally chartered industry-government partnership in which both the leadership and the membership of the Task Force is a 2-to-1 industry-to-government ratio. Among several other workstreams with substantive deliverables, Working Group 1 is developing legal and procedural recommendations for a regime to govern the sharing between industry and government of derogatory information or suspicions regarding certain suppliers.

- NIST Special Publication 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, is the federal government's primary guide to supply chain risk management; like other NIST risk management guidance, this publication both benefits from and promotes private sector expertise and experience.

These are models of private sector leadership and cross-sector collaboration that should be expanded globally. The ITU should recognize and promote private sector efforts, and government initiatives that facilitate such private sector efforts, advancing supply chain security throughout the global ICT market. The ITU should avoid—and discourage—government-centric approaches to 5G supply chain security.

IV. LIMITED RESOURCES SHOULD SUPPORT CORE MISSIONS

Both the U.S. Government's and ITU–T's limited resources are best prioritized in areas where they have the most expertise and can further core missions. Accordingly, CTA supports NTIA's proposals to restructure and merge ITU–T's study groups as well as "ensure the ITU–T refocuses its efforts on technical matters that are within its mandate and expertise and to

minimize and redirect any work on issues outside ITU–T's mandate."[34] As a first step, CTA recommends consolidating SG12 (Performance, QOS and QOE) and SG15 (Transport, access and home) given their overlapping subject matter, i.e., transport and measuring transport.

Streamlined study groups will reduce the burden on U.S. participants who are already engaged in numerous standards-setting activities. The cost of participating in an ITU sector is significant and, therefore, a barrier to involvement by U.S. entities.[35] Further, as noted above, U.S. companies are heavily involved with other international, regional, and industry standards efforts where the barrier to participation is lower.[36] Facing finite resources, American companies are participating where the barriers to participate are lower, limiting entities' participation in ITU efforts.

CTA also supports NTIA's plans to prioritize its participation in study groups because, as NTIA notes, "it is imperative that the United States facilitate U.S. industry's ability to influence standards for the next generation of communications."[37] In particular, NTIA should pursue the best opportunities to be vigilant of ITU–T involvement where other organizations are more effectively addressing the subject matter area.

[34] *See RFC* at 27,391.

[35] *See id*. at 27,392 (seeking comment on the factors that influence U.S. industry's participation in ITU activities).

[36] *See id*. at 27,392 (observing that "[w]hile the ITU–T has been widening its areas of interest in recent years, participation from U.S. firms in ITU–T standards work has declined in general").

[37] *Id*.

V. CONCLUSION

CTA urges NTIA to ensure that the U.S. delegation to WTSA–2020 advocates the continued use of voluntary global standards and a limited scope for the ITU–T.

Respectfully submitted,

CONSUMER TECHNOLOGY ASSOCIATION

By: */s/ Jamie Susskind*

Jamie Susskind
Vice President, Policy and Regulatory Affairs

/s/ Mike Bergman
Mike Bergman
Vice President, Technology and Standards

Consumer Technology Association
1919 S. Eads Street
Arlington, VA 22202
(703) 907-7644

June 8, 2020