The Internet & Television Association
25 Massachusetts Avenue, NW | Suite 100
Washington, DC 20001
(202) 222-2300

**Rick Chessen**
Chief Legal Officer
Senior Vice President, Legal & Regulatory Affairs
o (202) 222-2445 e rchessen@ncta.com

October 15, 2021

Dr. James Olthoff
Acting Under Secretary of Commerce for Standards and Technology
National Institute of Standards and Technology
U.S. Department of Commerce
100 Bureau Drive
Gaithersburg, MD 20899

Dear Dr. Olthoff:

NCTA – The Internet & Television Association (NCTA)[1] submits these comments in response to the National Institute of Standards and Technology's (NIST) request for comment on draft criteria for a labeling program on the cybersecurity capabilities of Internet of Things (IoT) devices.[2] NIST was directed by Executive Order 14,028, *Improving the Nation's Cybersecurity*, to "identify IoT cybersecurity criteria for a consumer labeling program," and to undertake pilot programs for IoT consumer labeling.[3] On August 31, NIST issued draft baseline security criteria for consumer IoT devices, and on September 14 and 15, hosted a virtual public workshop to discuss, among other things, industry's preliminary feedback on those potential IoT baseline security criteria.[4]

**Overview.** As the nation's largest providers of broadband service, cable companies have been leaders in deploying a diverse set of state-of-the-art network capabilities, security tools and measures, and customer support services aimed at preventing, detecting, and mitigating cybersecurity risks, including those posed by IoT devices. In addition, the cable industry has

---

1 NCTA is the principal trade association of the cable television industry in the United States, which is a leading provider of residential broadband service to U.S. households. Its members include owners and operators of cable television systems serving nearly 80% of the nation's cable television customers, as well as more than 200 cable program networks.

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

3 Exec. Order 14,028, 86 Fed. Reg. 26,633, 26,640 (May 17, 2021) (E.O. 14,028).

4 *Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software*, NIST, https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/cybersecurity-labeling-consumers-internet-things (last updated Sept. 21, 2021).

long sought to drive increased security of IoT and other connected devices.[5] For example, NCTA, along with other communications sector organizations such as the Alliance for Telecommunications Industry Solutions, CableLabs, CTIA, the Telecommunications Industry Association, and USTelecom, played key roles in the development and adoption of the IoT security recommendations set forth in the C2 Consensus on IoT Device Security Baseline Capabilities.[6] NCTA, CableLabs, and several member companies are all involved in the work of the Open Connectivity Foundation (OCF) on developing secure discovery and connectivity standards for IoT devices.[7] Cable and communications companies also participate in the ioXt Alliance device certification program, which provides guidelines for assessing and delineating the appropriate level of security for a particular device within a product category and utilizes authorized labs for testing and certification.[8] The communications sector also is working with Underwriters Laboratories (UL) in connection with the development and implementation of IoT security ratings, which are based on UL's IoT Security Top 20 Design Principles.[9]

NCTA shares the Administration's goal of improving cybersecurity, including through "educat[ing] the public on the security capabilities of [IoT] devices."[10] Labeling should remain an industry-driven, sector-specific effort, aligned with the industry efforts described above, and NCTA urges NIST to undertake pilot programs and further research before considering a government-centric approach to labeling.

**Underpinning any robust labeling effort is the development of verifiable security criteria or requirements for IoT devices. Ongoing cable industry efforts on the security of gateway networking devices make clear the need to develop security requirements at a use-case and context specific level to ensure applicability and efficacy.** NIST has provided critical thought leadership in developing guidance on the broad security capabilities of connected devices. Industry continues to translate that guidance to device-specific criteria that could underpin a labeling effort for particular devices. Cable operators deploy gateway devices (cable modems, integrated access points, and home routers) in customer homes that enable a consumer to attach to cable broadband networks. The cable industry continues to update security requirements for such gateway devices, informed by government and industry efforts around IoT security (although gateway devices are considered networking equipment, not IoT). Such efforts

---

5 *See e.g.*, CableLabs, *A Vision for Secure IoT* (2017) (CableLabs Secure IoT Paper), https://www-res.cablelabs.com/wp-content/uploads/2017/07/28093258/A_Vision_for_Secure_IoT_Informed_insights_summer_2017.pdf.

6 *See* Council to Secure the Digital Economy, *The C2 Consensus on IoT Device Security Baseline Capabilities*, https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf.

7 *See generally OCF Solving the IoT Standards Gap*, Open Connectivity Foundation, https://openconnectivity.org/ (last visited Oct. 8, 2021).

8 *See generally* The Global Standard for IoT Security, ioXt, https://www.ioxtalliance.org/ (last visited Oct.8, 2021).

9 *See IoT Security Rating: Security Testing to Support IoT Product Manufacturers*, Underwriters Laboratories, https://www.ul.com/services/iot-security-rating (last visited Sept. 8, 2021).

10 E.O. 14,028, 86 Fed. Reg. at 26,640.

effectively ensure that the industry's security practices take account of and keep pace with the evolution of these devices by taking into consideration the specific context and use of gateways.

As the result of a successful industry-based working group, CableLabs[11] recently released a set of best common practices (BCP) to secure gateway devices that are deployed in customer homes and businesses as part of cable broadband services.[12] This work builds on CableLabs' and the cable industry's longstanding leadership in cybersecurity to ensure a consistent and robust baseline for gateway device security, increased economies of scale, and simplified communication and procurement between network operators and device manufacturers.

The cable industry has long employed extensive network security practices to ensure the confidentiality, integrity, and availability of broadband services, including ensuring gateway device security.[13] The BCP[14] expands and standardizes these network security practices for gateway devices and complements cable operators' broader set of security practices. For instance, DOCSIS® Security testing is performed on all gateway devices to ensure DOCSIS[15] protocol conformance, including the verification of the correct implementation of public key infrastructure (PKI) authentication and identity management, BPI+ encryption, and EAE (Early Authentication and Encryption) secure provisioning requirements.

The BCP document also goes beyond DOCSIS Security requirements and provides a common framework for the full range of security considerations applicable to gateway devices, including hardware and manufacturing considerations, default security settings, configuration procedures, secure boot, roots of trust, software/firmware development and verification, encryption requirements for both data in transit and data at rest, and physical security, among others. To further ensure the robustness of the BCP and confirm its scope was fully comprehensive of applicable security considerations, the BCP was mapped to NISTIR 8259D that provides general guidance for connected devices used by the federal government.[16]

The BCP represents the cable industry and related manufacturers coalescing around a common baseline that furthers the following critical goals:

---

[11] CableLabs, a 501(c)(6) non-profit established in 1989 that presently consists of 65 members worldwide, is the technology consortium of the cable industry globally, based in Colorado. CableLabs convenes industry stakeholders to develop CableLabs specific specifications, such as DOCSIS® technology.

[12] Brian Scriber, et al., *Raising the Bar on Gateway Device Security*, CableLabs (Oct. 7, 2021), https://www.cablelabs.com/raising-the-bar-on-gateway-device-security.

[13] CableLabs, *Security Networks in the Broadband Age* (2017), https://www.cablelabs.com/securing-networks-broadband-age.

[14] Gateway Device Security Best Common Practices, Version V01 (newest version), CL-GL-GDS-BCP, (CableLabs 2021), https://www.cablelabs.com/specifications/CL-GL-GDS-BCP.

[15] DOCSIS is a technology that enables the delivery of broadband over cable networks. *See, e.g.*, *DOCSIS 3.1 Technology*, CableLabs, https://www.cablelabs.com/technologies/docsis-3-1 (last visited Oct. 14, 2021).

[16] Dep't of Commerce, NIST, NISTIR 8259D (Draft), *Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government* (2020), https://csrc.nist.gov/publications/detail/nistir/8259d/draft.

1. Provide a common framework for security elements and controls within gateway devices, including cable modems, integrated Wi-Fi access points, and home routers, to align the varied approaches to device security across the industry.
2. Create a community of manufacturers and network operators collaborating to enhance gateway device security.
3. Leverage well-established and well-vetted security controls and practices to minimize the risk of unknowingly introduced vulnerabilities or other security weaknesses.
4. Harmonize security requirements across network operators to drive increased economies of scale, lowering the cost of broadband deployment.
5. Further protect network resources and broadband service from malicious attacks.
6. Provide a framework for network operator assurance that enables verification of testable practices and configurations.
7. Enable alignment across standards, regulatory, and compliance regimes through a transparent and open set of best common practices.
8. Establish a security framework for gateway devices that builds in flexibility and agility, so that manufacturers and network operators can address and adapt to new threats and changes in the cyber risk landscape.

Critically, the development of the BCPs represented an effort by the cable industry and its vendors that was specific to the gateway device use case. Similar industry efforts will continue because the security field continuously evolves in the face of evolving threats. The BCP development process could be considered as a model for creating the use-case specific criteria that could then form the foundation for a robust consumer IoT label. Industry-led and sector-specific approaches, such as the BCP development process, lead to better investment, buy-in, and compliance with program criteria because the affected industries participated in developing a feasible, effective, and relevant set of guidelines.

**Although the criteria listed in NIST's IoT White Paper may be over or underinclusive for many devices and use cases, NCTA agrees as a general matter that criteria around unique identifiers and authentication are critical.**[17] As NIST notes, the security criteria outlined in the white paper "are core baselines and need to be tailored (or profiled) for specific use cases or sectors," which could involve "editing the capabilities to address specific concerns as well as extensions or additions to the baseline capabilities and sub-capabilities."[18] NCTA agrees that, because of the wide variety of IoT devices and use cases—both of which continue to expand—all the criteria listed may not be applicable in all instances and appropriate implementation may be device and use-case specific. In some cases (for example IoT devices used as smart locks or security cameras),[19] additional criteria could be

[17] *See* CableLabs Secure IoT Paper at 9-11 (addressing device identity and authentication).

[18] IoT White Paper at 1.

[19] *See id.* at 10.

considered.

Although NIST and industry should continue to discuss how to tailor the criteria for different use cases or sectors, there are two criteria in particular that NCTA strongly supports in the context of IoT devices capable of attaching to a broadband network. Third party users that attach to U.S. networks without authorization inhibit consumers' and network operators' ability to identify and mitigate security threats and pose a growing risk to U.S. networks. To help combat this problem and other security threats, NCTA supports the use of strong identifiers (as NIST suggests[20]) to identify specific devices, where the device identity is globally unique, immutable, and attestable.[21] Use of such identifiers enables an ISP and/or its customer to locate devices connected to the network and assists with targeting any necessary actions to disconnect or otherwise disable devices that pose a threat to network security. Such strong identifiers also minimize the risk of identity spoofing that would inhibit locating specific devices.[22] As the IoT cybersecurity guidelines set forth in NISTIR 8259 note, "[b]eing able to distinguish each IoT device from all others is needed for the other common risk mitigation areas—vulnerability management, access management, data protection and incident detection."[23]

NCTA also supports the use of strong authentication mechanisms for IoT devices that attach directly or indirectly to broadband networks. "Secure authentication, authorization, and accountability minimize the potential for compromising a device or other devices in the local IoT ecosystem during the onboarding process" when "a new device is connected and added to the network and the local IoT ecosystem."[24] Federal guidelines for IoT security suggest that consumers take steps to protect their networks, including by restricting access to authorized devices and using strong passwords.[25] NISTIR 8259 in particular—which the current IoT White Paper draws heavily from—emphasizes that access management is critical, including "[p]revent[ing] unauthorized and improper . . . access to, usage of, and administration of IoT devices throughout the devices' lifecycles by people, processes and other computing devices."[26] NCTA is therefore pleased to see included in Table 1 of the IoT White Paper "[t]he ability to logically restrict access to each network interface to only authorized persons or devices," and "[t]he ability to authenticate individuals and other IoT product components using appropriate

---

20 *Id.* at 3.

21 CableLabs Secure IoT Paper at 9-10.

22 *Id.*

23 Dep't of Commerce, NIST, NISTIR 8259, *Foundational Cybersecurity Activities for IoT Device Manufacturers*, at 4 (2020) (NISTIR 8259), https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf.

24 CableLabs Secure IoT Paper at 10-11.

25 Fed. Trade Comm'n, *Consumer Protection: How To Secure Your Home Wi-Fi Network*, Consumer Information (May 2021), https://www.consumer.ftc.gov/articles/how-secure-your-home-wi-fi-network#limit (advising consumers to change pre-set passwords on devices and use passwords that are "more complex"); *Security Tip (ST05-003) Securing Wireless Networks*, Cybersecurity & Infrastructure Security Agency, https://us-cert.cisa.gov/ncas/tips/ST05-003 (last revised May 8, 2020) (suggesting customers change default passwords, restrict access to only "authorized users" and install firewalls on the network and devices, among other things).

26 NISTIR 8259 at 4.

mechanism to technology, risk and use case," for example using digital certificates, biometrics, or strong passwords.[27] Strong non-default secure credentials are an important tool to protect both consumers and networks as IoT devices proliferate in the marketplace and IoT-fueled cyber attacks accelerate.

**One size will not fit all when it comes to criteria for labeling and potential solutions should be industry-driven and subject to further research and consideration.** In the IoT White Paper, NIST acknowledges that when it comes to consumer labeling, "[o]ne size may not fit all," and that multiple solutions may be required.[28] NCTA agrees. As described above, there are a host of different IoT devices in the marketplace used for many different purposes by a diverse set of end users with differing levels of sophistication. The criteria or labeling approach that works best for one device, use case, or consumer may not work well for another. This reality underscores that NIST is heading in the right direction in "allowing providers and customers to choose the best solutions for their devices and environments."[29] NCTA urges NIST to continue to collaborate with industry to understand the existing sources for consumer information on IoT security, including existing industry standards and associated labeling programs. An industry-driven approach will best be able to accommodate the needs of particular devices and users and to adapt to changing conditions in the marketplace and in the threat landscape.

As required by E.O. 14,028, NIST should proceed with pilot programs[30] to examine successful industry-driven labeling efforts. And given the lack of relevant examples with respect to government labeling programs, it would be prudent to analyze the results of those pilot programs and undertake further research on the numerous considerations of a consumer IoT security labeling program before any development of a government-led labeling initiative.

**Conclusion.** For the foregoing reasons, NCTA continues to support a flexible approach to providing consumers with security information for IoT devices that accounts for existing industry tools and continuing developments. The ongoing CableLabs gateway security effort is just one example of how broadband providers continually invest in upgrading network security and respond to security threats. Although NCTA supports two criteria in particular that are set forth in the IoT White Paper as best practices—including the use of strong identifiers and secure authentication mechanisms to mitigate the risk of unauthorized third-party device access to U.S. networks—we suggest that NIST complete the pilot programs contemplated by E.O. 14,028 and consider the results of such programs and further research before developing any government-run IoT security labeling program.

---

27 IoT White Paper at 4.

28 *Id.* at 1.

29 *Id.*

30 E.O. 14,028, 86 Fed. Reg. at 26,640.

Respectfully Submitted,

**/s/ Rick Chessen**

Matt Tooley

Vice President, Broadband Technology

Rick Chessen
Loretta Polk
Danielle Piñeres
NCTA – The Internet & Television Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, DC 20001-1431
(202) 222-2445

October 15, 2021