

1  
2

**IEEE P802.18**  
**Radio Regulatory Technical Advisory Group (RR-TAG)**

Proposed Comment to FCC NPRM: Cybersecurity Labeling for  
Internet of Things

Date: 2023-10-03

Author(s):

Name	Company	Address	Phone	Email
Hassan Yaghoobi	Intel Corp.			<a href="mailto:hassan.yaghoobi@intel.com">hassan.yaghoobi@intel.com</a>
Carol Ansley	Cox			<a href="mailto:carol@ansley.com">carol@ansley.com</a>
David Goodall	Morse Micro			<a href="mailto:dave@morsemicro.com">dave@morsemicro.com</a>
Mike Montemurro	Huawei			<a href="mailto:montemurro.michael@gmail.com">montemurro.michael@gmail.com</a>

3

4 This document drafts a proposed comment to FCC NPRM: Cybersecurity Labeling for Internet of Things.

**Notice:** This document has been prepared to assist IEEE 802.18. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.

5 Electronic filing

[October 3, 2023]

6  
7 Erika Olson  
8 Acting Chief Cybersecurity and Communications Reliability Division  
9 Public Safety and Homeland Security Bureau  
10 Federal Communications Commission  
11 Washington, DC

12  
13 Re: Comment to NPRM: Cybersecurity Labeling for Internet of Things  
14  
15

16 Dear Acting Chief Olson,

17  
18 IEEE 802 LAN/MAN Standards Committee (“IEEE 802 LMSC”) thanks the Federal  
19 Communications Commission (FCC) for issuing the consultation on the Notice of Proposed  
20 Rulemaking (“NPRM”): Cybersecurity Labeling for Internet of Things and for the opportunity to  
21 provide comments.  
22

23 IEEE 802 LAN/MAN Standards Committee (IEEE 802 LMSC) is a leading consensus-based open  
24 standards development committee for networking standards that are used by industry globally. It  
25 produces standards for networking devices, including wired and wireless local area networks  
26 (“LANs” and “WLANs”), wireless specialty networks (“WSNs”), wireless metropolitan area  
27 networks (“Wireless MANs”), and wireless regional area networks (“WRANs”). Technologies  
28 produced by implementers of our standards are a critical element for all networked applications  
29 today.  
30

31 IEEE 802 LMSC is a committee of the IEEE Standards Association and of Technical Activities,  
32 two of the Major Organizational Units of the IEEE. IEEE has about 400,000 members in over 160  
33 countries and its core purpose is to foster technological innovation and excellence for the benefit  
34 of humanity. IEEE is also a major accredited standards development organization whose standards  
35 are recognized world-wide. In submitting this document, IEEE 802 LMSC acknowledges and  
36 respects that other components of IEEE Organizational Units may have perspectives that differ  
37 from, or compete with, those of IEEE 802 LMSC. Therefore, this submission should not be  
38 construed as representing the views of IEEE as a whole<sup>1</sup>.  
39

40 IEEE 802 LMSC applauds the Commission’s NPRM that proposes a cybersecurity labeling  
41 program for Internet of Things (IoT). IEEE 802 LMSC recognizes the Commission’s goal of  
42 improving consumer confidence and understanding of the security of their connected devices and  
43 supports proposed voluntary cybersecurity labeling program for such devices.  
44

45 Please find below the IEEE 802 LMSC’s comments, which provides the Commission with the  
46 latest information on IEEE 802’s standards projects related to IoT devices operating in unlicensed  
47 bands, our support on selected comments about industry-led cybersecurity standards, scope of  
48 cybersecurity labeling, testing, and conformity.  
49

50 **IEEE 802 standards for Internet of Things devices**

---

<sup>1</sup> This document solely represents the views of IEEE 802 LMSC and does not necessarily represent a position of either the IEEE or the IEEE Standards Association.

51  
52 IEEE 802 wireless technologies such as IEEE 802.11 and IEEE 802.15 have been instrumental in  
53 enabling a rich diversity of IoT devices. This diversity includes, but is not restricted to, smart  
54 meters, smart lighting, smart plugs, switches and controls, sensor devices, locks, home appliances,  
55 and video cameras. In addition, many IoT devices combine sensors with cameras to support  
56 applications such as smart doorbells, security cameras with motion detection or smoke detection,  
57 etc.

58  
59 Of particulate note is the IEEE Std 802.11ah-2016 standard<sup>2</sup> and the IEEE Std 802.15.4-2020  
60 standard<sup>3</sup>. The former, known as Wi-Fi HaLow in the marketplace, was developed with long range,  
61 low power sensor and IoT networks and applications such as agriculture<sup>4</sup> in mind. The latter,  
62 known as Wi-SUN in the marketplace, was developed to support applications such as smart  
63 metering and includes features such as location discovery and device ranging. Some other  
64 examples of the IoT devices which implement IEEE 802.15.4 technologies are TV remote controls,  
65 lighting, window and door locks, heating and air conditioning systems, alarm systems, and remote  
66 medical monitoring.

67

### 68 **Standardized security mechanisms for IEEE 802.11 based IoT devices**

69 The same robust security mechanisms specified in IEEE Std 802.11-2020<sup>5</sup> that are found in  
70 consumer smartphone and PC products are available to IEEE 802.11 based IoT devices.

71

72 IEEE Std 802.11-2020 standard provides a security framework for wireless communications that  
73 includes access control through IEEE Std 802.1X-2020<sup>6</sup>, robust authentication, data  
74 confidentiality, and key management. The IEEE 802.1X-2020 protocols are specified to establish  
75 a secure link for communications between the IoT device and the network. For home networks,  
76 IEEE Std 802.11-2020 offers password-based authentication that is resistant to dictionary attacks.  
77 For managed networks, IoT devices can be authenticated using Authentication, Authorization, and  
78 Accounting (AAA) infrastructure.

79

80 IEEE Std 802.11-2020 provides two cryptographic encapsulation mechanisms to ensure data  
81 confidentiality and data origin authenticity. Counter Mode (CTR) with Cipher Block Chaining  
82 Message Authentication Code Protocol (CCMP) encapsulation provides Advanced Encryption  
83 Standard (AES) encryption with CTR for data confidentiality. Galois/Counter Mode Protocol  
84 (GCMP) provides AES encryption with GCM for integrity protection. Both mechanisms can be  
85 established with either 128 or 256 bit key sizes. IEEE Std 802.11-2020 also provides data integrity

---

<sup>2</sup> “IEEE Standard for Information technology—Telecommunications and information exchange between systems - Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 2: Sub 1 GHz License Exempt Operation,” IEEE Std 802.11ah-2016 (Amendment to IEEE Std 802.11-2016, as amended by IEEE Std 802.11ai-2016), vol., no., pp.1-594, 5 May 2017, doi: 10.1109/IEEESTD.2017.7920364.

<sup>3</sup> “IEEE Standard for Low-Rate Wireless Networks,” IEEE Std 802.15.4-2020 (Revision of IEEE Std 802.15.4-2015), vol., no., pp.1-800, 23 July 2020, doi: 10.1109/IEEESTD.2020.9144691.

<sup>4</sup> Wi-Fi Alliance: The future of farming: Testing the rural range of Wi-Fi CERTIFIED HaLow™. [Available online](#) [accessed: 28 September 2023]

<sup>5</sup> “IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks--Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,” IEEE Std 802.11-2020 (Revision of IEEE Std 802.11-2016), vol., no., pp.1-4379, 26 Feb. 2021, doi: 10.1109/IEEESTD.2021.9363693.

<sup>6</sup> “IEEE Standard for Local and metropolitan area networks--Port-Based Network Access Control,” IEEE Std 802.1X-2010 (Revision of IEEE Std 802.1X-2004), vol., no., pp.1-205, 5 Feb. 2010, doi: 10.1109/IEEESTD.2010.5409813.

86 and replay protection for broadcast/multicast management frames using AES in CMAC and  
87 GMAC modes with either 128 or 256 bit key sizes. All security protocols specified in the IEEE  
88 Std 802.11-2020 standard require fresh cryptographic keys and corresponding security  
89 associations. The standard provides procedures to establish fresh keys for both establishing a new  
90 communication link as well as refreshing keys on an existing link.

## 92 **Industry-led Cybersecurity Standards**

93  
94 IEEE 802 LMSC supports the Commission’s recognition of industry-led development,  
95 implementation, and testing of cybersecurity standards.

96  
97 IEEE 802 LMSC believes that there is no need to convene a Commission-sponsored group to  
98 develop standards and this would replicate the work already completed or projects underway in  
99 industry-led standards bodies, in particular the NIST publications<sup>7,8</sup> that form the basis of the  
100 proposed voluntary requirement. Security protocols specified in the IEEE Std 802.11-2020, using  
101 the IEEE Std 802.1X-2020 standard, are also certified as part of the Wi-Fi Alliance’s Wi-Fi  
102 CERTIFIED WPA3 program<sup>9</sup>.

103  
104 IEEE 802 LMSC recommends the Commission evaluate cybersecurity standards developed by  
105 approved or accredited industry organizations for adoption under the IoT Cybersecurity Labeling  
106 Program. Having said that, we recommend the Commission also consider ongoing industry work  
107 (e.g., IEEE 802.15 Working Group Task Group 4ac in IEEE 802 LMSC) in its evaluation.

## 109 **Scope of Cybersecurity Labeling**

110 IEEE 802 LMSC believes that the scope of the proposed cybersecurity labeling program should  
111 be carefully studied and limited to IoT consumer products. More specifically, IEEE 802 LMSC  
112 proposes adoption of NIST Recommended Criteria for Cybersecurity Labeling for Consumer  
113 Internet of Things (IoT) Products<sup>10</sup> and excluding common general purpose computing equipment  
114 (e.g., personal computers, smartphones) as well as general internet and networking infrastructure  
115 (e.g., internet routers and switches).

116  
117 In addition, to meet the goal of improving consumer confidence and understanding of the security  
118 of connected devices, IEEE 802 LMSC recommends considering a focus on labeling IoT end  
119 products and excluding other components such as modules, gateways, backends, or applications.

## 121 **Cybersecurity Testing and Conformity**

122  
123 IEEE 802 LMSC supports providing options for device manufacturer testing and self-assessment  
124 as well as testing by FCC-approved, industry accredited labs (e.g., Wi-Fi Alliance authorized test  
125 labs<sup>11</sup>) or by an FCC-approved CyberLAB. IEEE 802 LMSC believes that availability of these

---

<sup>7</sup> M. Fagan, *et al.*, “Profile of the IoT Core Baseline for Consumer IoT Products,” NIST IR 8425, September 2022.  
[Available online](#) [accessed: 28 September 2023]

<sup>8</sup> M. Fagan, *et al.*, “Foundational Cybersecurity Activities for IoT Device Manufacturers,” NIST IR 8259, May 2020.  
[Available online](#) [accessed: 28 September 2023]. This paper defines “transducer” as an element of the definition of an  
IoT device.

<sup>9</sup> Wi-Fi Alliance: Security. [Available online](#) [accessed: 28 September 2023]

<sup>10</sup> Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products, Section 2.1  
Scope of an IoT Product, February 2022. [Available online](#) [accessed: 28 September 2023]

<sup>11</sup> Wi-Fi Alliance: Certification, Authorized Test Labs. [Available online](#) [accessed: 28 September 2023]

126 options for conformity is key in the efficiency of compliance programs and hence critical in  
127 successful adoption of such a voluntary program. Details of such options and the specific scope of  
128 such testing is a subject of further study.

129

### 130 **Conclusion**

131

132 IEEE 802 LMSC thanks the Commission for the opportunity to comment on this important NPRM  
133 on cybersecurity labeling program for IoT and supports initiating the voluntary labeling program.  
134 We respectfully request the Commission to consider our comments listed in this response.

135

136

137 Respectfully submitted

138

139 By: /s/.

140 Paul Nikolich

141 IEEE 802 LAN/MAN Standards Committee Chairman

142 em: [p.nikolich@ieee.org](mailto:p.nikolich@ieee.org)