PUBLIC NOTICE

Federal Communications Commission
45 L Street NE
Washington, DC 20554

News Media Information 202-418-0500
Internet: www.fcc.gov
TTY: 888-835-5322

DA 25-33
January 10, 2025

PUBLIC SAFETY AND HOMELAND SECURITY BUREAU REMINDS ACCREDITATION BODIES TO REQUEST RECOGNITION FOR THE INTERNET OF THINGS CYBERSECURITY LABELING PROGRAM

PS Docket No. 24-714

By this Public Notice, the Public Safety and Homeland Security Bureau (Bureau) reminds organizations seeking authority to accredit Cybersecurity Label Administrators (CLAs) and/or laboratories under the Federal Communications Commission's (FCC or Commission) Internet of Things (IoT) Cybersecurity Labeling Program, which includes the U.S. government certification mark (U.S. Cyber Trust Mark), that they must be recognized by the Bureau to perform such accreditation.[1]

Accreditation bodies seeking recognition must submit a letter addressed to the Chief, Public Safety and Homeland Security Bureau, requesting recognition to accredit CLAs and/or requesting recognition to accredit CyberLABs under the Commission's IoT Labeling Program. The letter must include the following information as evidence of the accreditation body's credentials and qualifications to accredit CLAs and/or laboratories:

1. Name of entity and contact information.
2. A general description of the organization.
3. Successful completion of an ISO/IEC 17011 peer review, such as being a signatory to an accreditation agreement that is acceptable to the Commission.[2]

[1] *Cybersecurity Labeling for Internet of Things*, PS Docket No. 23-239, Report and Order and Further Notice of Proposed Rulemaking, 39 FCC Rcd 2497 (March 15, 2024) (*IoT Labeling Order*).

[2] *IoT Labeling Order* 39 FCC Rcd at 2521, para. 45 & n.178 ("The organization(s) accrediting the prospective Label Administrators and testing labs must meet the requirements and conditions in ISO/IEC 17011. *See* 47 CFR § 8.218(b)(1); ISO/IEC 17011:2017(E), *Conformity assessment—Requirements for accreditation bodies accrediting conformity assessment bodies*, Second Edition, November 2017; IBR approved for § 8.217."). We note that peer evaluations ensure that accreditation bodies operate to the same standards around the world and assess the competence, consistent operation, and impartiality of the accreditation bodies. The accrediting body may further detail in its request, relevant competences, and processes it has in place to ensure the impartiality and objectivity of its activities required by ISO/IEC 17011.

4. In the case of accreditation bodies seeking recognition to accredit laboratories, demonstrated experience with the accreditation of conformity assessment testing laboratories to ISO/IEC 17025.[3]
5. In the case of accreditation bodies seeking recognition to accredit CLAs, demonstrated experience with the accreditation of conformity assessment bodies certifying products, processes, and services to ISO/IEC 17065.[4]
6. Accreditation personnel/assessors with specific technical experience on the Commission cybersecurity certification rules and requirements.[5]
7. Procedures and policies developed for the accreditation of testing laboratories or CLAs for FCC cybersecurity certification programs.[6]

At this time, recognition will be limited to U.S. domestic accreditation bodies only. The Bureau may request additional information, or showings, as needed, to expand recognition to international accreditation bodies at a later date. [7]

How to File for Recognition. Accreditation Bodies may file a request for recognition at any time. Letters requesting recognition and supporting materials are to be filed electronically in **PS Docket No. 24-714** using the Internet by accessing the Commission's Electronic Comment Filing System (ECFS): https://www.fcc.gov/ecfs with a courtesy copy sent to FCC staff as a .pdf file via email to CyberTrustMark@fcc.gov.

Further Information. For further information regarding this proceeding, please contact Drew Morin, Deputy Division Chief, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau by email to Drew.Morin@fcc.gov or Tara B. Shostek, Attorney Advisor, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau at Tara.Shostek@fcc.gov.

Action by the Chief, Public Safety and Homeland Security Bureau.

-FCC-

[3] 47 CFR § 8.218(b)(2); ISO/IEC 17025:2017(E), *General requirements for the competence of testing and calibration laboratories*, Third Edition, November 2017; IBR approved for §§ 8.217; 8.220. Demonstrated experience may also include, but is not limited to, the availability of trained personnel/assessors and necessary equipment to perform the accreditation.

[4] *See* 47 CFR § 8.219(b) ("In the United States, the Commission, in accordance with its procedures, allows qualified accrediting bodies to accredit CLAs based on ISO/IEC 17065 and other qualification criteria ISO/IEC 17065:2012, *Conformity Assessment – Requirements for Bodies Certifying Products, Processes and Services*, First Edition, 2012-09-15, IBR approved for § 8.220.) Demonstrated experience may also include, but is not limited to, the availability of trained personnel/assessors and necessary equipment to perform the accreditation.

[5] 47 CFR § 8.218(b)(3). To comply with this requirement, accrediting bodies may detail technical experience with IoT security features addressing the elements of the NIST Core Baseline, including asset identification, product configuration, data protection, interface access control, software updates, cybersecurity state awareness. documentation, information and query reception, information dissemination, and product education and awareness.

[6] 47 CFR § 8.218(b)(4). In this regard, requesting accrediting bodies must commit to implementing additional and/or changed assessment requirements as the Commission's certification program develops over time.

[7] *See generally* 47 CFR § 8.218(b); *IoT Labeling Order* at 25, para. 45 & n.178.