



PUBLIC NOTICE

**Federal Communications Commission
45 L St., N.E.
Washington, D.C. 20554**

News Media Information 202-418-0500
Internet: <https://www.fcc.gov>

**DA 26-75
January 26, 2026**

**PUBLIC SAFETY AND HOMELAND SECURITY BUREAU ANNOUNCES
20-BUSINESS DAY FILING WINDOW FOR CYBERSECURITY LABEL ADMINISTRATOR
APPLICATIONS UNDER THE U.S. CYBER TRUST MARK PROGRAM AND REITERATES
PROGRAM OBLIGATIONS**

PS Docket No. 23-239

By this Notice, the Federal Communications Commission's (FCC or Commission) Public Safety and Homeland Security Bureau (Bureau) announces a 20-business day filing window for applications from entities seeking to be recognized as a Cybersecurity Label Administrator (CLA). **This filing window will open on January 27, 2026, and close February 24, 2026.¹**

In March 2024, the Commission established a framework for a voluntary cybersecurity labeling program for consumer wireless Internet of Things (IoT) products (U.S. Cyber Trust Mark Program), which includes third party administrators to support the program.² In September 2024, the Bureau opened an initial filing window on delegated authority from the Commission for applications from entities seeking authority to be recognized as a CLA and as Lead Administrator.³ Thus far, the Bureau conditionally approved 11 CLAs, and approved UL LLC (UL Solutions) as Lead Administrator.⁴ UL Solutions withdrew as Lead Administrator effective December 19, 2025.⁵ The Bureau opened a 15-

¹ While the Bureau does not routinely grant extensions of time, applicants requiring additional time may, in accordance with Section 1.46 of the Commission's rules, request an extension of time for up to 10 additional calendar days to complete their applications. 47 CFR § 1.46.

² *Cybersecurity Labeling for Internet of Things*, PS Docket No. 23-239, Report and Order and Further Notice of Proposed Rulemaking, 39 FCC Rcd 2497, 2522, para. 48 (2024) (*IoT Labeling Order*).

³ See *Public Safety and Homeland Security Bureau Announces 15-Day Filing Window for Cybersecurity Labeling Administrator and Lead Administrator Applications Under the Cybersecurity Labeling for Internet of Things Program*, PS Docket No. 23-239, Public Notice, DA 24-900 (Sept. 10, 2024) (*Initial Filing Window Public Notice*); *IoT Labeling Order*, 39 FCC Rcd at 2532, para. 64. CLA responsibilities are outlined in the *IoT Labeling Order*. 39 FCC Rcd at 2523-25, paras. 52-53; 47 CFR § 8.220.

⁴ *Public Safety and Homeland Security Bureau Announces Conditionally Approved Cybersecurity Label Administrators for the Internet of Things Cybersecurity Labeling Program*, PS Docket No. 23-239, Public Notice, DA 24-1241 (Dec. 11, 2024); *Public Safety and Homeland Security Bureau Selects UL LLC to Serve as Lead Administrator of the Internet of Things Cybersecurity Labeling Program*, PS Docket No. 23-239, Public Notice, DA 24-1214 (Dec. 4, 2024).

⁵ Letter from Chanté Maurio, VP and GM, Identity Management and Security, UL Solutions, to Zenji Nakazawa, Chief, Public Safety and Homeland Security Bureau, FCC, PS Docket No. 23-239 (filed Dec. 19, 2025). We note that one CLA has also withdrawn, effective August 15, 2025. Letter from Umair Javed, Senior Vice President and General Counsel and Thomas K. Sawanobori, Senior Vice President and Chief Technology Officer, CTIA Certification LLC to Marlene H. Dortch, Secretary, FCC, PS Docket No. 23-239 (filed Aug. 15, 2025).

business day application filing window for entities seeking designation as the Lead Administrator on January 7, which will close on January 28, 2026.⁶

The Bureau is now opening a new filing window for applications for CLA.⁷ The Bureau outlined the format of CLA applications, and the process for Bureau selection of these administrators, among other issues, in its September 2024 *Initial Filing Window Public Notice*.⁸ The Bureau also provided guidance for who may apply and the relevant application procedures.⁹ Applicants for CLA are advised to follow the same instructions, including the general filing instructions, provided in the *Initial Filing Window Public Notice*, as well as the additional guidance on confidential filing requirements published in October 2024.¹⁰ We reiterate that conditionally approved CLAs are obligated to maintain their commitments made under their applications, including, demonstrations and certifications provided with respect to national security, obtaining accreditation pursuant to all of the requirements associated with ISO/IEC 17065 with the forthcoming FCC program scope, and implementing and updating cybersecurity risk management plans.¹¹

After the application filing window closes on February 24, 2026, the Bureau will review administrators' applications for compliance with each criteria set forth in the *IoT Labeling Order* and to best ensure the success of the program.¹² Conditional approval of CLA applications will not allow CLAs to certify products to use the FCC IoT Label before obtaining accreditation to the Commission's scope, and before complying with any additional criteria the Bureau may adopt, as necessary, to efficiently select entities seeking to be recognized as a CLA.¹³ **The Bureau's selection of CLA(s) will be announced by public notice.**

People with Disabilities

To request materials in accessible formats for people with disabilities (Braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at 202-418-0530 (voice).

Additional Information

For further information regarding this proceeding, please contact Drew Morin, Deputy Division Chief, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security

⁶ *Public Safety and Homeland Security Bureau Announces 15-Business Day Filing Window for Lead Administrator Applications Under the U.S. Cyber Trust Mark Program*, PS Docket No. 23-239, Public Notice, DA 26-18 (Jan. 6, 2026).

⁷ The *IoT Labeling Order* delegated authority to the Bureau to open additional application filing windows, as necessary, for entities seeking authority to be recognized by the Bureau as a CLA. *IoT Labeling Order*, 39 FCC Rcd at 2523, 2532, paras. 51, 64.

⁸ *Initial Filing Window Public Notice* at 2-15, paras. 3-32 (setting forth the format, filing fees, and selection process for CLA and Lead Administrator applications, as well as Lead Administrator cost-sharing among the CLAs, guardrails for Lead Administrator neutrality, and confidentiality and security requirements).

⁹ *Initial Filing Window Public Notice* at 15-21, paras. 33-41.

¹⁰ *Initial Filing Window Public Notice* at 24, Appx A; *Public Safety and Homeland Security Bureau Provides Additional Guidance on Confidential Filing Requirements for Cybersecurity Label Administrator and Lead Administrator Applications Under the Cybersecurity Labeling for Internet of Things Program*, PS Docket No. 23-239, Public Notice, DA 24-1037 (Oct. 3, 2024).

¹¹ *Initial Filing Window Public Notice* at 14-19, paras. 30, 33-35, 37.

¹² The Bureau may request clarifying information from applicants in its review, as needed.

¹³ *Initial Filing Window Public Notice* at 8, para. 15; 47 CFR § 8.220; *IoT Labeling Order* at 2532, para. 64.

Bureau or Tara B. Shostek, Attorney Advisor, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau at CyberTrustMark@fcc.gov.

Privacy Act Statement

Authority. The FCC is authorized to collect the information pursuant to the authority contained in sections 1, 2, 4(i), 4(n), 302, 303(r), 312, 333, and 503, of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 152, 154(i), 154(n), 302a, 303(r), 312, 333, 503; the IoT Cybersecurity Improvement Act of 2020, 15 U.S.C. § 278g-3a to § 278g-3e.

Purpose. The information collected in this Application includes contact and certification information from entities voluntarily applying to serve as CLA in this FCC program. The information is used to communicate with such entities and enforce their compliance with statements made in their applications.

Routine Uses. While CLA applications will be presumed confidential, in addition to those disclosures generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act of 1974, as amended, the FCC may disclose contact and certification information collected from applicants as is determined to be relevant and necessary, outside the FCC as a routine use pursuant to 5 U.S.C. § 552a(b)(3), including: to authorized third parties to administer, support, participate in, or receive information related to FCC programs and activities; to other Federal agencies in order to administer, support, participate in, or receive information related to FCC programs and activities; and to non-federal personnel, including contractors, who have been engaged to assist the FCC in the performance of a contract service, grant, cooperative agreement, or other activity related to this system of records and who need to have access to the records in order to perform their activity.

A full, detailed list of the routine uses is published in the system of records notice associated with this collection, FCC-2, Business Contacts and Certifications, which is available at <https://www.fcc.gov/sites/default/files/sor-fcc-2.pdf>.

Disclosure. This information collection is voluntary. The Public Safety and Homeland Security Bureau's Public Notice provides entities the opportunity to apply to be designated a CLA.