(c) The term ''provider'' shall denote any provider of voicemail or interactive menu service.

[83 FR 44842, Sept. 4, 2018]

§ 7.16 Informal or formal complaints.

Any person may file either a formal or informal complaint against a manufacturer or provider alleging violations of section 255 or this part subject to the enforcement requirements set forth in §§ 14.30 through 14.38 of this chapter.

[83 FR 44842, Sept. 4, 2018]

Part 8—SAFEGUARDING AND SECURING THE INTERNET

Subpart A—Protections for Internet Openness

Subpart B—Cybersecurity Labeling Program for IoT Products

AUTHORITY: 47 U.S.C. 151, 152, 153, 154, 163, 201, 202, 206, 207, 208, 209, 216, 217, 257, 301, 302a, 303, 304, 307, 309, 312, 316, 332, 403, 501, 503, 522, 1302, 1753.

SOURCE: 76 FR 59232, Sept. 23, 2011, unless otherwise noted.

Subpart A—Protections for Internet Openness

§ 8.1 Definitions.

(a) [Reserved]

(b) *Broadband Internet access service.* A mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all internet endpoints, including any capabilities that are incidental to and enable the operation of the communications service, but excluding dial-up internet access service. This term also encompasses any service that the Commission finds to be providing a functional equivalent of the service described in the previous sentence or that is used to evade the protections set forth in this part.

(c) *Edge provider.* Any individual or entity that provides any content, application, or service over the internet, and any individual or entity that provides a device used for accessing any content, application, or service over the internet.

(d) *End user.* Any individual or entity that uses a broadband internet access service.

(e) *Reasonable network management.* A network management practice is a practice that has a primarily technical network management justification, but does not include other business practices. A network management practice is reasonable if it is primarily used for and tailored to achieving a legitimate network management purpose, taking into account the particular network architecture and technology of the broadband internet access service.

[89 FR 45554, May 22, 2024. Redesignated at 89 FR 61272, July 30, 2024]

§ 8.2 Transparency.

(a) Any person providing broadband internet access service shall publicly disclose accurate information regarding the network management practices, performance characteristics, and commercial terms of its broadband

internet access services sufficient to enable consumers to make informed choices regarding the purchase and use of such services and entrepreneurs and other small businesses to develop, market, and maintain internet offerings. Such disclosure shall be made via a publicly available, easily accessible website or through transmittal to the Commission.

(1) Any person providing broadband internet access service shall create and display an accurate broadband consumer label for each stand-alone broadband internet access service it currently offers for purchase. The label must be prominently displayed, publicly available, and easily accessible to consumers, including consumers with disabilities, at the point of sale with the content and in the format prescribed by the Commission in ''[Fixed or Mobile] Broadband Consumer Disclosure,'' in figure 1 to this paragraph (a)(1).

FIGURE 1 TO PARAGRAPH (A)(1)—[FIXED OR MOBILE] BROADBAND CONSUMER DISCLOSURE LABEL

Broadband Facts

Provider Name

Service Plan Name and/or Speed Tier

Fixed or Mobile Broadband Consumer Disclosure

Monthly Price [$]

This Monthly Price [is/is not] an introductory rate. [if introductory rate is applicable, identify length of introductory period and the rate that will apply after introductory period concludes]

This Monthly Price [does not] require[s] a [x year/x month] contract. [only required if applicable; if so, provide link to terms of contract]

Additional Charges & Terms

Provider Monthly Fees
[Itemize each fee or enter "None."] **[$]**

One-time Fees at the Time of Purchase
[Itemize each fee or enter "None."] **[$]**

Early Termination Fee **[$]**

Government Taxes **[Varies by Location/Taxes Included]**

Discounts & Bundles

Click Here for available billing discounts and pricing options for broadband service bundled with other services like video, phone, and wireless service, and use of your own equipment like modems and routers. [Any links to such discounts and pricing options on the provider's website must be provided in this section.]

Affordable Connectivity Program (ACP)

The ACP is a government program to help lower the monthly cost of internet service. To learn more about the ACP, including to find out whether you qualify, visit GetInternet.gov.

Participates in the ACP **[Yes/No]**

Speeds Provided with Plan

Typical Download Speed **[] Mbps**
Typical Upload Speed **[] Mbps**
Typical Latency **[] ms**

Data Included with Monthly Price **[] GB**
Charges for Additional Data Usage **[$/GB]**

Network Management **Read our Policy**
Privacy **Read our Policy**

Customer Support

Contact Us: example.com/support / (555) 555-5555

Learn more about the terms used on this label by visiting the Federal Communications Commission's Consumer Resource Center.

fcc.gov/consumer

[Unique Plan Identifier Ex. F0005937974123ABC456EMC789]

(2) Broadband internet access service providers shall display the label required under paragraph (a)(1) of this section at each point of sale. *Point of sale* is defined to mean a provider's website and any alternate sales channels through which the provider's broadband internet access service is sold, including a provider-owned retail location, third-party retail location, and over the phone. For labels displayed on provider websites, the label must be displayed in close proximity to the associated advertised service plan. *Point of sale* also means the time a consumer begins investigating and comparing broadband service offerings available to them at their location. For alternate sales channels, providers must document each instance when it directs a consumer to a label and retain such documentation for two years. This requirement will be deemed satisfied if, instead, the provider: establishes the business practices and processes it will follow in distributing the label through alternative sales channels; retains training materials and related business practice documentation for two years; and provides such information to the Commission upon request, within thirty days. *Point of sale* for purposes of the E-Rate and Rural Health Care programs is defined as the time a service provider submits its bid to a program participant. Providers participating in the E-Rate and Rural Health Care programs must provide their labels to program participants when they submit their bids to participants. Broadband internet access service providers that offer online account portals to their customers shall also make each customer's label easily accessible to the customer in such portals.

(3) The content of the label required under paragraph (a)(1) of this section must be displayed on the broadband internet access service provider's website in a machine-readable format. Broadband internet access service providers must provide the information in any label separately in a spreadsheet file format on their websites via a dedicated uniform resource locator (URL) that contains all of their labels. Providers must publicize the URL with the label data in the transparency disclosures required under this paragraph (a).

(4) The label required under paragraph (a)(1) of this section must be provided in English and in any other languages in which the broadband internet access service provider markets its services in the United States.

(5) Broadband internet access service providers shall maintain an archive of all labels required under paragraph (a)(1) of this section for a period of no less than two years from the time the service plan reflected in the label is no longer available for purchase by a new subscriber and the provider has removed the label from its website or alternate sales channels. Providers must provide any archived label to the Commission, upon request, within thirty days. Providers must provide an archived label, upon request and within thirty days, to an existing customer whose service plan is associated with the particular label. A provider is not required to display a label once the associated service plan is no longer offered to new subscribers.

(6) Broadband consumer label requirements and the transparency rule in paragraph (a) of this section are subject to enforcement using the same processes and procedures. The label required under paragraph (a)(1) of this section is not a safe harbor from the transparency rule or any other requirements established by the Commission.

(7) Compliance with paragraphs (a)(1), (2), and (4) through (6) of this section for providers with 100,000 or fewer subscriber lines is required as of October 10, 2024, and for all other providers is required as of April 10, 2024, except that compliance with the requirement in paragraph (a)(2) of this section to make labels accessible in online account portals will not be required for all providers until October 10, 2024. Compliance with paragraph (a)(3) of this section is required for all providers as of October 10, 2024.

(b) Broadband internet access service is a mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all internet endpoints, including any capabilities that are incidental to and enable the

operation of the communications service, but excluding dial-up internet access service. This term also encompasses any service that the Commission finds to be providing a functional equivalent of the service described in the previous sentence or that is used to evade the protections set forth in this part. For purposes of paragraphs (a)(1) through (6) of this section, ''mass-market'' services exclude service offerings customized for the customer through individually negotiated agreements even when the services are supported by federal universal service support.

[83 FR 7922, Feb. 22, 2018, as amended at 87 FR 76978, Dec. 16, 2022; 88 FR 52043, Aug. 7, 2023; 88 FR 63859, Sept. 18, 2023; 88 FR 73535, Oct. 26, 2023. Redesignated and amended at 89 FR 45554, May 22, 2024. Redesignated at 89 FR 61272, July 30, 2024]

EFFECTIVE DATE NOTE: At 89 FR 45554, May 22, 2024, § 8.2 was amended by revising the introductory text of paragraph (a); removing paragraph (a)(7); and revising paragraph (b). These actions were delayed indefinitely. For the convenience of the user, the added and revised text is set forth as follows:

§ 8.2 Transparency.

(a) A person engaged in the provision of broadband internet access service shall publicly disclose accurate information regarding the network management practices, performance, and commercial terms of its broadband internet access services sufficient for consumers to make informed choices regarding use of such services and for content, application, service, and device providers to develop, market, and maintain internet offerings. Disclosures made under this paragraph (a) must be displayed on the broadband internet access service provider's website in a machine-readable format.

* * * * *

(b) Compliance with paragraphs (a)(1), (2), and (4) through (6) of this section for providers with 100,000 or fewer subscriber lines is required as of October 10, 2024, and for all other providers is required as of April 10, 2024, except that compliance with the requirement in paragraph (a)(2) of this section to make labels accessible in online account portals will not be required for all providers until October 10, 2024. Compliance with paragraph (a)(3) of this section is required for all providers as of October 10, 2024.

* * * * *

§ 8.3 Conduct-based rules.

(a) *No blocking.* A person engaged in the provision of broadband internet access service, insofar as such person is so engaged, shall not block lawful content, applications, services, or non-harmful devices, subject to reasonable network management.

(b) *No throttling.* A person engaged in the provision of broadband internet access service, insofar as such person is so engaged, shall not impair or degrade lawful internet traffic on the basis of internet content, application, or service, or use of a non-harmful device, subject to reasonable network management.

(c) *No paid prioritization.* (1) A person engaged in the provision of broadband internet access service, insofar as such person is so engaged, shall not engage in paid prioritization. ''Paid prioritization'' refers to the management of a broadband provider's network to directly or indirectly favor some traffic over other traffic, including through use of techniques such as traffic shaping, prioritization, resource reservation, or other forms of preferential traffic management, either:

(i) In exchange for consideration (monetary or otherwise) from a third party; or

(ii) To benefit an affiliated entity.

(2) The Commission may waive the ban on paid prioritization only if the petitioner demonstrates that the practice would provide some significant public interest benefit and would not harm the open nature of the internet.

(d) *No unreasonable interference or unreasonable disadvantage standard for internet conduct.* (1) Any person engaged in the provision of broadband internet access service, insofar as such person is so engaged, shall not unreasonably interfere with or unreasonably disadvantage:

(i) End users' ability to select, access, and use broadband internet access service or the lawful internet content, applications, services, or devices of their choice; or

(ii) Edge providers' ability to make lawful content, applications, services, or devices available to end users.

(2) Reasonable network management shall not be considered a violation of this paragraph (d).

(e) *Effect on other obligations or authorizations.* Nothing in this part supersedes any obligation or authorization a provider of broadband internet access service may have to address the needs of emergency communications or law enforcement, public safety, or national security authorities, consistent with or as permitted by applicable law, or limits the provider's ability to do so. Nothing in this part prohibits reasonable efforts by a provider of broadband internet access service to address copyright infringement or other unlawful activity.

[89 FR 45554, May 22, 2024. Redesignated at 89 FR 61272, July 30, 2024]

§ 8.6 Advisory opinions.

(a) *Procedures.* (1) Any entity that is subject to the Commission's open internet rules in this part may request an advisory opinion from the Enforcement Bureau regarding the permissibility of its proposed policies and practices relating to broadband internet access service. Requests for advisory opinions may be filed via the Commission's website or with the Office of the Secretary and must be copied to the Chief of the Enforcement Bureau and the Chief of the Investigations and Hearings Division of the Enforcement Bureau.

(2) The Enforcement Bureau may, in its discretion, determine whether to issue an advisory opinion in response to a particular request or group of requests and will inform each requesting entity, in writing, whether the Bureau plans to issue an advisory opinion regarding the matter in question.

(3) Requests for advisory opinions must relate to a proposed policy or practice that the requesting party intends to pursue. The Enforcement Bureau will not respond to requests for opinions that relate to ongoing or prior conduct, and the Bureau may initiate an enforcement investigation to determine whether such conduct violates the open internet rules in this part. Additionally, the Bureau will not respond to requests if the same or substantially the same conduct is the subject of a current Government investigation or proceeding, including any ongoing litigation or open rulemaking at the Commission.

(4) Requests for advisory opinions must be accompanied by all material information sufficient for Enforcement Bureau staff to make a determination on the policy or practice for which review is requested. Requesters must certify that factual representations made to the Bureau are truthful and accurate, and that they have not intentionally omitted any information from the request. A request for an advisory opinion that is submitted by a business entity or an organization must be executed by an individual who is authorized to act on behalf of that entity or organization.

(5) Enforcement Bureau staff will have discretion to ask parties requesting advisory opinions, as well as other parties that may have information relevant to the request or that may be impacted by the proposed conduct, for additional information that the staff deems necessary to respond to the request. Such additional information, if furnished orally or during an in-person conference with Bureau staff, shall be promptly confirmed in writing. Parties are not obligated to respond to staff inquiries related to advisory opinions. If a requesting party fails to respond to a staff inquiry, then the Bureau may dismiss that party's request for an advisory opinion. If a party voluntarily responds to a staff inquiry for additional information, then it must do so by a deadline to be specified by Bureau staff. Advisory opinions will expressly state that they rely on the representations made by the requesting party, and that they are premised on the specific facts and representations in the request and any supplemental submissions.

(b) *Response.* After review of a request submitted under this section, the Enforcement Bureau will:

(1) Issue an advisory opinion that will state the Bureau's present enforcement intention with respect to whether or not the proposed policy or practice detailed in the request complies with the Commission's open internet rules in this part;

(2) Issue a written statement declining to respond to the request; or

(3) Take such other position or action as it considers appropriate. An advisory opinion states only the enforcement intention of the Enforcement Bureau as of the date of the opinion, and it is not binding on any party. Advisory opinions will be issued without prejudice to the Enforcement Bureau or the Commission to reconsider the questions involved, or to rescind or revoke the opinion. Advisory opinions will not be subject to appeal or further review.

(c) *Enforcement effect.* The Enforcement Bureau will have discretion to indicate the Bureau's lack of enforcement intent in an advisory opinion based on the facts, representations, and warranties made by the requesting party. The requesting party may rely on the opinion only to the extent that the request fully and accurately contains all the material facts and representations necessary to issuance of the opinion and the situation conforms to the situation described in the request for opinion. The Bureau will not bring an enforcement action against a requesting party with respect to any action taken in good faith reliance upon an advisory opinion if all of the relevant facts were fully, completely, and accurately presented to the Bureau, and where such action was promptly discontinued upon notification of rescission or revocation of the Commission's or Bureau's approval.

(d) *Public disclosure.* The Enforcement Bureau will make advisory opinions available to the public on the Commission's website. The Bureau will also publish the initial request for guidance and any associated materials. Parties soliciting advisory opinions may request confidential treatment of information submitted in connection with a request for an advisory opinion pursuant to § 0.459 of this chapter.

(e) *Withdrawal of request.* Any requesting party may withdraw a request for review at any time prior to receipt of notice that the Enforcement Bureau intends to issue an adverse opinion, or the issuance of an opinion. The Enforcement Bureau remains free, however, to submit comments to such requesting party as it deems appropriate. Failure to take action after receipt of documents or information, whether submitted pursuant to this procedure or otherwise, does not in any way limit or stop the Bureau from taking such action at such time thereafter as it deems appropriate. The Bureau reserves the right to retain documents submitted to it under this procedure or otherwise and to use them for all governmental purposes.

[89 FR 45554, May 22, 2024. Redesignated at 89 FR 61272, July 30, 2024]

Subpart B—Cybersecurity Labeling Program for IoT Products

SOURCE: 89 FR 61272, July 30, 2024, unless otherwise noted.

§ 8.201 Incorporation by reference.

Certain material is incorporated by reference into this subpart with the approval of the Director of the Federal Register in accordance with 5 U.S.C. 552(a) and 1 CFR part 51. All approved incorporation by reference (IBR) material is available for inspection at the Federal Communications Commission (FCC or Commission) and at the National Archives and Records Administration (NARA). Contact the FCC at the address indicated in 47 CFR 0.401(a), phone: (202) 418–0270. For information on the availability of this material at NARA, visit *www.archives.gov/federal-register/cfr/ibr-locations* or email *fr.inspection@nara.gov*. The material may be obtained from the International Electrotechnical Commission (IEC), IEC Central Office, 3, rue de Varembe, CH–1211 Geneva 20, Switzerland, Email: *inmail@iec.ch*, *www.iec.ch*.

(a) ISO/IEC 17011:2017(E), *Conformity assessment—Requirements for accreditation bodies accrediting conformity assessment bodies*, Second Edition, November 2017; IBR approved for § 8.217.

(b) 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.

(c) ISO/IEC 17065:2012(E), *Conformity assessment—Requirements for bodies certifying products, processes and services*, First Edition, 2012–09–15; IBR approved for § 8.220.

NOTE 1 TO § 8.201: The standards listed in this section are co-published with the International Organization for Standardization

(ISO), 1, ch. De la Voie-Creuse, CP 56, CH–1211, Geneva 20, Switzerland; *www.iso.org;* Tel.: + 41 22 749 01 11; Fax: + 41 22 733 34 30; email: *central@iso.org*.

NOTE 2 TO § 8.201: ISO publications can also be purchased from the American National Standards Institute (ANSI) through its NSSN operation (*www.nssn.org*), at Customer Service, American National Standards Institute, 25 West 43rd Street, New York, NY 10036, telephone (212) 642–4900.

§ 8.202 Basis and purpose.

In order to elevate the Nation's cybersecurity posture and provide consumers with assurances regarding their baseline cybersecurity, thereby addressing risks of harmful radiofrequency interference to and from consumer internet-connected (Internet of Things or IoT) products the Federal Communications Commission establishes a labeling program for consumer IoT products.

§ 8.203 Definitions.

(a) *Affiliate*. For purposes of this subpart and the IoT labeling program, an *affiliate* is defined as a person that (directly or indirectly) owns or controls, is owned or controlled by, or is under common ownership or control with, another person. For purposes of this subpart, the term *own* means to own an equity interest (or the equivalent thereof) of more than 10 percent.

(b) *Consumer IoT products*. IoT products intended primarily for consumer use, rather than enterprise or industrial use. *Consumer IoT products* exclude medical devices regulated by the U.S. Food and Drug Administration (FDA) and excludes motor vehicles and motor vehicle equipment regulated by the National Highway Traffic Safety Administration (NHTSA).

(c) *Cybersecurity Label Administrator (CLA)*. An accredited third-party entity that is recognized and authorized by the Commission to manage and administer the labeling program in accordance with the Commission's rules in this subpart.

(d) *Cybersecurity Testing Laboratory (CyberLAB)*. Accredited third-party entities recognized and authorized by a CLA to assess consumer IoT products for compliance with requirements of the labeling program.

(e) *Cyber Trust Mark*. A visual indicator indicating a consumer IoT product complies with program requirements of the labeling program and the Commission's minimum cybersecurity requirements in this subpart.

(f) *FCC IoT Label*. A binary label displayable with a consumer IoT product complying with program requirements of the labeling program, the binary label bearing the Cyber Trust Mark, and a scannable QR code that directs consumers to a registry containing further information on the complying consumer IoT product.

(g) *Intentional radiator*. A device that intentionally generates and emits radiofrequency energy by radiation or induction.

(h) *Internet-connected device*. A device capable of connecting to the internet and exchanging data with other devices or centralized systems over the internet.

(i) *IoT device*. (1) An internet-connected device capable of intentionally emitting radiofrequency energy that has at least one transducer (sensor or actuator) for interacting directly with the physical world; coupled with

(2) At least one network interface (*e.g.*, Wi-Fi, Bluetooth) for interfacing with the digital world.

(j) *IoT product*. An IoT device and any additional product components (*e.g.*, backend, gateway, mobile app) that are necessary to use the IoT device beyond basic operational features, including data communications links to components outside this scope but excluding those external components and any external third-party components that are outside the manufacturer's control.

(k) *Labeling program*. A voluntary program for consumer IoT products that allows a complying consumer IoT product to display an FCC IoT Label.

(l) *Lead Administrator*. A CLA selected from among Cybersecurity Label Administrators (CLAs) to be responsible for carrying out additional administrative responsibilities of the labeling program.

(m) *Product components*. Hardware devices, plus supporting components that generally fall into three main types per NISTIR 8425: specialty networking/gateway hardware (*e.g.*, a hub within the system where the IoT device is

used); companion application software (*e.g.*, a mobile app for communicating with the IoT device); and backends (*e.g.*, a cloud service, or multiple services, that may store and/or process data from the IoT device). Should a product component also support other IoT products through alternative features and interfaces, these alternative features and interfaces may, through risk-assessment, be considered as separate from and not part of the IoT product for purposes of authorization.

(n) *Registry*. Information presented to consumers about consumer IoT products that comply with the program requirements of the labeling program, the registry is publicly accessible through a link from the QR Code of the FCC IoT Label displayed with the complying consumer IoT product, and containing information about the complying consumer IoT product, manufacturer of the complying consumer IoT product, and other information as required by the labeling program.

§ 8.204 Prohibition on use of the FCC IoT Label on products produced by listed sources.

All consumer IoT products produced by sources listed in this subpart are prohibited from obtaining use of the FCC IoT Label under this subpart. This includes:

(a) All communications equipment on the Covered List, as established pursuant to 47 CFR 1.50002;

(b) All IoT products containing IoT devices or product components produced by entities listed in paragraph (c) or (d) of this section;

(c) IoT devices or IoT products produced by any entity, its affiliates, or subsidiaries identified on the Covered List as producing covered equipment, as established pursuant to 47 CFR 1.50002;

(d) IoT devices or IoT products produced by any entity, its affiliates, or subsidiaries identified on the Department of Commerce's Entity List, 15 CFR part 744, supplement no. 4, and/or the Department of Defense's List of Chinese Military Companies, U.S. Department of Defense, Entities Identified as Chinese Military Companies Operating in the United States in Accordance with Section 1260H of the William M. (''Mac'') Thornberry National Defense Authorization Act for Fiscal Year 2021 (Pub. L. 116–283), Tranche 2 (2022), *https://media.defense.gov/2022/Oct/05/2003091659/-1/-1/0/1260H%20COMPANIES.PDF*. and

(e) Products produced by any entity owned or controlled by or affiliated with any person or entity that has been suspended or debarred from receiving Federal procurements or financial awards, to include all entities and individuals published as ineligible for award on the General Service Administration's System for Award Management.

§ 8.205 Cybersecurity labeling authorization.

(a) Cybersecurity labeling authorization is an authorization issued by a Cybersecurity Label Administrator (CLA) and authorized under the authority of the Commission, which grants an applicant of a complying consumer IoT product to display the FCC IoT Label on the relevant packaging for the complying consumer product, based on compliance with the program requirements as determined by the CLA.

(b) Cybersecurity labeling authorization attaches to all units of the complying consumer IoT product subsequently marketed by the grantee that are identical (see § 8.206) to the sample determined to comply with the program requirements except for permissive changes or other variations authorized by the Commission.

§ 8.206 Identical defined.

As used in this subpart, the term *identical* means identical within the variation that can be expected to arise as a result of quantity production techniques.

§ 8.207 Responsible party.

In the case of a complying consumer IoT product that has been granted authorization to use the FCC IoT Label, the applicant to whom that grant of cybersecurity labeling authorization is issued is responsible for continued compliance with the program requirements for continued use of the FCC IoT Label.

§ 8.208 Application requirements.

(a) An application to certify the consumer IoT product as being compliant with the labeling program shall be submitted in writing to a Cybersecurity Labeling Administrator (CLA) in the form and format prescribed by the Commission. Each application shall be accompanied by all information required by this subpart.

(b) The applicant shall provide to the CLA in the application all information that the CLA requires to determine compliance with the program requirements of the labeling program.

(c) The applicant will provide a declaration under penalty of perjury that all of the following are true and correct:

(1) The product for which the applicant seeks to use the FCC IoT Label through cybersecurity certification meets all the requirements of the IoT labeling program.

(2) The applicant is not identified as an entity producing covered communications equipment on the Covered List, established pursuant to 47 CFR 1.50002.

(3) The product is not comprised of ''covered'' equipment on the Covered List.

(4) The product is not produced by any entity, its affiliates, or subsidiaries identified on the Department of Commerce's Entity List, 15 CFR part 744, supplement no. 4, and/or the Department of Defense's List of Chinese Military Companies, U.S. Department of Defense, Entities Identified as Chinese Military Companies Operating in the United States in Accordance with Section 1260H of the William M. (''Mac'') Thornberry National Defense Authorization Act for Fiscal Year 2021 (Pub. L. 116–283), Tranche 2 (2022), *https://media.defense.gov/2022/Oct/05/2003091659/-1/-1/0/1260H%20COMPANIES.PDF;* and

(5) The product is not owned or controlled by or affiliated with any person or entity that has been suspended or debarred from receiving Federal procurements or financial awards, to include all entities and individuals published as ineligible for award on the General Service Administration's System for Award Management as described in § 8.204.

(6) The applicant has taken every reasonable measure to create a securable product.

(7) The applicant will, until the support period end date disclosed in the registry, diligently identify critical vulnerabilities in our products and promptly issue software updates correcting them, unless such updates are not reasonably needed to protect against security failures.

(8) The applicant will not elsewhere disclaim or otherwise attempt to limit the substantive or procedural enforceability of this declaration or of any other representations and commitments made on the FCC IoT Label or made for purposes of acquiring or maintaining authorization to use it.

(d) The applicant shall provide a written and signed declaration to the CLA that all statements it makes in the application are true and correct to the best of its knowledge and belief.

(e) Each application, including amendments thereto, and related statements of fact and authorizations required by the Commission, shall be signed by the applicant or their authorized agent.

(f) The applicant declares the product is reasonably secure and will be updated through minimum support period for the product and the end date of the support period must be disclosed.

(g) The applicant shall declare under penalty of perjury that the consumer IoT product for which the applicant is applying for participation in the labeling program is not prohibited pursuant to § 8.204.

(h) If the identified listed sources under § 8.204 are modified after the date of the declaration required by paragraph (c) of this section but prior to grant of authorization to use the FCC IoT Label, then the applicant shall provide a new declaration as required by paragraph (c).

(i) The applicant shall designate an agent located in the United States for the purpose of accepting service of process on behalf of the applicant.

(1) The applicant shall provide a written attestation:

(i) Signed by both the applicant and its designated agent for service of process, if different from the applicant;

(ii) Acknowledging the applicant's consent and the designated agent's obligation to accept service of process in the United States for matters related to the applicable product, and at the physical U.S. address and email address of its designated agent; and

(iii) Acknowledging the applicant's acceptance of its obligation to maintain an agent for service of process in the United States for no less than one year after either the grantee has permanently terminated all marketing and importation of the applicable equipment within the U.S., or the conclusion of any Commission-related administrative or judicial proceeding involving the product, whichever is later.

(2) An applicant located in the United States may designate itself as the agent for service of process.

(j) Technical test data submitted to the CLA shall be signed by the person who performed or supervised the tests. The person signing the test data shall attest to the accuracy of such data. The CLA may require the person signing the test data to submit a statement showing that they are qualified to make or supervise the required measurements.

(k) *Signed*, as used in this section, means an original handwritten signature or any symbol executed or adopted by the applicant or CLA with the intent that such symbol be a signature, including symbols formed by computer-generated electronic impulses.

§ 8.209 Grant of authorization to use FCC IoT Label.

(a) A CLA will grant cybersecurity labeling authorization if it finds from an examination of the application and supporting data, or other matter which it may officially notice, that the consumer IoT product complies with the program requirements.

(b) Grants will be made in writing showing the effective date of the grant.

(c) Cybersecurity certification shall not attach to any product, nor shall any use of the Cyber Trust Mark be deemed effective, until the application has been granted.

(d) Grants will be effective from the date of authorization.

(e) The grant shall identify the CLA granting the authorization and the Commission as the issuing authority.

(f) In cases of a dispute, the Commission will be the final arbiter.

§ 8.210 Dismissal of application.

(a) An application that is not in accordance with the provisions of this subpart may be dismissed.

(b) Any application, upon written request signed by the applicant or their agent, may be dismissed prior to a determination granting or denying the authorization requested.

(c) If an applicant is requested to submit additional documents or information and fails to submit the requested material within the specified time period, the application may be dismissed.

§ 8.211 Denial of application.

If the CLA is unable to make the findings specified in § 8.209(a), it will deny the application. Notification of the denial to the applicant will include a statement of the reasons for the denial.

§ 8.212 Review of CLA decisions.

(a) *Seeking review from a CLA.* Any party aggrieved by an action taken by a CLA must first seek review from the CLA. The CLA should respond to appeals of their decisions in a timely manner and within 10 business days of receipt of a request for review.

(b) *Seeking review from the Commission.* A party aggrieved by an action taken by a CLA may, after seeking review by the CLA, seek review from the Commission.

(c) *Filing deadlines.* (1) An aggrieved party seeking review of a CLA decision by the CLA shall submit such a request within sixty (60) days from the date the CLA issues a decision. Such request shall be deemed submitted when received by the CLA.

(2) An aggrieved party seeking review of a CLA decision by the Commission shall file such a request within sixty (60) days from the date the CLA issues a decision on the party's request for review. Parties must adhere to the time periods for filing oppositions and replies set forth in 47 CFR 1.45.

(d) *Review by the Public Safety and Homeland Security Bureau or the Commission.* (1) Requests for review of CLA decisions that are submitted to the Federal Communications Commission shall be considered and acted upon by the Public Safety and Homeland Security Bureau; provided, however, that requests for review that raise novel questions of fact, law or policy shall be considered by the full Commission.

(2) An aggrieved party may seek review of a decision issued under delegated authority by the Public Safety and Homeland Security Bureau pursuant to the rules set forth in 47 CFR part 1.

(e) *Standard of review.* (1) The Public Safety and Homeland Security Bureau shall conduct de novo review of request for review of decisions issued by the CLA.

(2) The Federal Communications Commission shall conduct de novo review of requests for review of decisions by the CLA that involve novel questions of fact, law, or policy; provided, however, that the Commission shall not conduct de novo review of decisions issued by the Public Safety and Homeland Security Bureau under delegated authority.

(f) *Time periods for Commission review of CLA decisions.* (1) The Public Safety and Homeland Security Bureau shall, within forty-five (45) days, take action in response to a request for review of a CLA decision that is properly before it. The Public Safety and Homeland Security Bureau may extend the time period for taking action on a request for review of a CLA decision for a period of up to ninety days. The Commission may also at any time, extend the time period for taking action of a request for review of a CLA decision pending before the Public Safety and Homeland Security Bureau.

(2) The Commission shall issue a written decision in response to a request for review of a CLA decision that involves novel questions of fact, law, or policy within forty-five (45) days. The Commission may extend the time period for taking action on the request for review of a CLA decision. The Public Safety and Homeland Security Bureau also may extend action on a request for review of a CLA decision for a period of up to ninety days.

(g) *No authorization pending CLA review.* While a party seeks review of a CLA decision, they are not authorized to use the FCC IoT Label until the Commission issues a final decision authorizing their use of the FCC IoT Label.

§ 8.213 Limitations on grants to use the FCC IoT Label.

(a) A grant of authorization to use the FCC IoT Label remains effective until set aside, revoked or withdrawn, rescinded, surrendered, or a termination date is otherwise established by the Commission.

(b) No person shall, in any advertising matter, brochure, etc., use or make reference to the FCC IoT Label or the Cyber Trust Mark in a deceptive or misleading manner.

§ 8.214 IoT product defect and/or design change.

When a complaint is filed directly with the Commission or submitted to the Commission by the Lead Administrator or other party concerning a consumer IoT product being non-compliant with the labeling program, and the Commission determines that the complaint is justified, the Commission may require the grantee to investigate such complaint and report the results of such investigation to the Commission within 20 days. The report shall also indicate what action if any has been taken or is proposed to be taken by the grantee to correct the defect, both in terms of future production and with reference to articles in the possession of users, sellers, and distributors.

§ 8.215 Retention of records.

(a) For complying consumer IoT products granted authorization to use the FCC IoT Label, the grantee shall maintain the records listed as follows:

(1) A record of the original design and specifications and all changes that have been made to the complying consumer IoT product that may affect compliance with the standards and testing procedures of this subpart.

(2) A record of the procedures used for production inspection and testing

to ensure conformance with the standards and testing procedures of this subpart.

(3) A record of the test results that demonstrate compliance with the appropriate regulations in this chapter.

(b) Records shall be retained for a two-year period after the marketing of the associated product has been permanently discontinued, or until the conclusion of an investigation or a proceeding if the grantee is officially notified that an investigation or any other administrative proceeding involving its product has been instituted.

§ 8.216 Termination of authorization to use the FCC IoT Label.

(a) Grant of authorization to use the FCC IoT Label is automatically terminated by notice of the Bureau following submission of a report as specified in § 8.214 has not been adequately corrected:

(1) For false statements or representations made either in the application or in materials or response submitted in connection therewith or in records required to be kept by § 8.215.

(2) If upon subsequent inspection or operation it is determined that the consumer IoT product does not conform to the pertinent technical requirements in this subpart or to the representations made in the original application.

(3) Because of conditions coming to the attention of the Commission which would warrant it in refusing to grant authorization to use the FCC IoT Label.

(4) Because the grantee or affiliate has been listed as described in § 8.204.

(b) [Reserved]

§ 8.217 CyberLABs.

(a) A CyberLAB providing testing of products seeking a grant of authorization to use the FCC IoT Label shall be accredited by a recognized accreditation body, which must attest that the CyberLAB has demonstrated:

(1) Technical expertise in cybersecurity testing and conformity assessment of IoT devices and products.

(2) Compliance with accreditation requirements based on ISO/IEC 17025 (incorporated by reference, see § 8.201).

(3) Knowledge of FCC rules and procedures associated with products compliance testing and cybersecurity certification.

(4) Necessary equipment, facilities, and personnel to conduct cybersecurity testing and conformity assessment of IoT devices and products.

(5) Documented procedures for conformity assessment.

(6) Implementation of controls to eliminate potential conflicts of interests, particularly with regard to commercially sensitive information.

(7) That the CyberLAB is not an organization, its affiliates, or subsidiaries identified by the listed sources of prohibition under § 8.204.

(8) That it has certified the truth and accuracy of all information it has submitted to support its accreditation.

(b) Once accredited or recognized the CyberLAB will be periodically audited and reviewed to ensure they continue to comply with the requirements of the ISO/IEC 17025 standard.

(c) The Lead Administrator will verify that the CyberLAB is not listed in any of the lists in § 8.204.

(d) The Lead Administrator will maintain a list of accredited CyberLABs that it has recognized, and make publicly available the list of accredited CyberLAB. Inclusion of a CyberLAB on the accredited list does not constitute Commission endorsement of that facility. Recognition afforded to a CyberLAB under the labeling program will be automatically terminated for entities that are subsequently placed on the Covered List, listed sources of prohibition under § 8.204, or of it, its affiliate, or subsidiary is owned or controlled by a foreign adversary country defined by the Department of Commerce in 15 CFR 7.4.

(e) In order to be recognized and included on the list in paragraph (d) of this section, the accrediting organization must submit the information in paragraphs (e)(1) through (9) of this section to the Lead Administrator:

(1) Laboratory name, location of test site(s), mailing address and contact information;

(2) Name of accrediting organization;

(3) Scope of laboratory accreditation;

(4) Date of expiration of accreditation;

(5) Designation number;
(6) FCC Registration Number (FRN);
(7) A statement as to whether or not the laboratory performs testing on a contract basis;
(8) For laboratories outside the United States, details of the arrangement under which the accreditation of the laboratory is recognized; and
(9) Other information as requested by the Commission.

(f) A laboratory that has been accredited with a scope covering the measurements required for the types of IoT products that it will test shall be deemed competent to test and submit test data for IoT products subject to cybersecurity certification. Such a laboratory shall be accredited by a Public Safety and Homeland Security Bureau-recognized accreditation organization based on ISO/IEC 17025. The organization accrediting the laboratory must be recognized by the Public Safety and Homeland Security Bureau to perform such accreditation based on ISO/IEC 17011 (incorporated by reference, see § 8.201). The frequency for reassessment of the test facility and the information that is required to be filed or retained by the testing party shall comply with the requirements established by the accrediting organization, but shall occur on an interval not to exceed two years.

§ 8.218 Recognition of CyberLAB accreditation bodies.

(a) A party wishing to become a laboratory accreditation body recognized by the Public Safety and Homeland Security Bureau (PSHSB or Bureau) must submit a written request to the Chief of PSHSB requesting such recognition. PSHSB will make a determination based on the information provided in support of the request for recognition.

(b) Applicants shall provide the information in paragraphs (b)(1) through (4) of this section as evidence of their credentials and qualifications to perform accreditation of laboratories that test equipment to Commission requirements, consistent with the requirements of § 8.217(e). PSHSB may request additional information, or showings, as needed, to determine the applicant's credentials and qualifications.

(1) 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) Experience with the accreditation of conformity assessment testing laboratories to ISO/IEC 17025.

(3) Accreditation personnel/assessors with specific technical experience on the Commission cybersecurity certification rules and requirements.

(4) Procedures and policies developed for the accreditation of testing laboratories for FCC cybersecurity certification programs.

§ 8.219 Approval/recognition of Cybersecurity Label Administrators.

(a) An accredited third-party entity wishing to become a Cybersecurity Label Administrator (CLA) must file a written application with the Commission. The Commission may approve the written application for the accredited third-party entity to be recognized and authorized by the Commission as a CLA to manage and administer the labeling program by meeting the requirements of paragraph (b) of this section. An accredited third-party entity is recognized and authorized by the Commission to manage and administer the labeling program in accordance with the Commission's rules in this subpart.

(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. CLAs shall comply with the requirements in § 8.220.

§ 8.220 Requirements for CLAs.

(a) *In general.* CLAs designated by the Commission, or designated by another authority recognized by the Commission, shall comply with the requirements of this section. Each entity seeking authority to act as a CLA must file an application with the Commission for consideration by PSHSB, which includes a description of its organization structure, an explanation of how it will avoid personal and organizational conflict when processing applications, a description of its processes for evaluating applications seeking authority to use the FCC IoT

Label, and a demonstration of expertise that will be necessary to effectively serve as a CLA including, but not limited to, the criteria in paragraph (c) of this section.

(b) *Methodology for reviewing applications.* (1) A CLA's methodology for reviewing applications shall be based on type testing as identified in ISO/IEC 17065 (incorporated by reference, see § 8.201).

(2) A CLA's grant of authorization to use the FCC IoT Label shall be based on the application with all the information specified in this part. The CLA shall review the application to determine compliance with the Commission's requirements in this subpart and shall issue a grant of product cybersecurity certification in accordance with § 8.208.

(c) *Criteria for designation.* (1) To be designated as a CLA under this section, an entity shall demonstrate cybersecurity expertise and capabilities in addition to industry knowledge of IoT and IoT labeling requirements.

(2) The entity shall demonstrate expert knowledge of National Institute of Standards and Technology's (NIST) cybersecurity guidance, including but not limited to NIST's recommended criteria and labeling program approaches for cybersecurity labeling of consumer IoT products.

(3) The entity shall demonstrate expert knowledge of FCC rules and procedures associated with product compliance testing and certification.

(4) The entity shall demonstrate knowledge of Federal law and guidance governing the security and privacy of agency information systems.

(5) The entity shall demonstrate an ability to securely handle large volumes of information and demonstrate internal security practices.

(6) To expedite initial deployment of the FCC labeling program, the Commission will accept and conditionally approve applications from entities seeking to be designated as a CLA provided they commit to obtain accreditation pursuant to all the requirements associated with ISO/IEC 17065 with the appropriate scope within six (6) months of the effective date by the adopted standards and testing procedures and otherwise meet the FCC's IoT Labeling Program requirements. The entity must also demonstrate implementation of controls to eliminate actual or potential conflicts of interests (including both personal and organizational), particularly with regard to commercially sensitive information. The Bureau will finalize the entity's application upon receipt and demonstration of ISO/IEC 17065 accreditation with the appropriate scope.

(7) The entity is not owned or controlled by or affiliated with any entity identified on the Commission's Covered List, listed sources of prohibition under § 8.204, or of it, its affiliate, or subsidiary is owned or controlled by a foreign adversary country defined by the Department of Commerce in 15 CFR 7.4.

(8) The entity must demonstrate it has implemented controls to eliminate actual or potential conflicts of interests (including both personal and organizational), particularly with regard to commercially sensitive information, to include but not limited to, remaining impartial and unbiased and prevent them from giving preferential treatment to certain applications (*e.g.*, application line jumping) and from implementing heightened scrutiny of applications from entities not members or otherwise aligned with the CLA.

(d) *External resources.* (1) In accordance with the provisions of ISO/IEC 17065 the evaluation of a product, or a portion thereof, may be performed by bodies that meet the applicable requirements of ISO/IEC 17025, in accordance with the applicable provisions of ISO/IEC 17065 for external resources (outsourcing). Evaluation is the selection of applicable requirements and the determination that those requirements are met. Evaluation may be performed using internal CLA resources or external (outsourced) resources.

(2) A CLA shall not outsource review or decision activities.

(3) When external resources are used to provide the evaluation function, including the testing of products subject to labeling, the CLA shall be responsible for the evaluation and shall maintain appropriate oversight of the external resources used to ensure reliability of the evaluation. Such oversight shall include periodic audits of products that

have been tested and other activities as required in ISO/IEC 17065 when a CLA uses external resources for evaluation.

(e) *Commission approves a CLA.* (1) The Commission will approve as a CLA:

(i) Any entity in the United States that meets the requirements of this section.

(ii) The Commission will not approve as a CLA any organization, its affiliates, or subsidiaries listed in the listed sources of prohibition under § 8.204.

(2) The Commission will withdraw its approval of a CLA if the CLA's designation or accreditation is withdrawn, if the Commission determines there is just cause for withdrawing the approval, or upon request of the CLA. The Commission will limit the scope of products that can be certified by a CLA if its accreditor limits the scope of its accreditation or if the Commission determines there is good cause to do so. The Commission will notify a CLA in writing of its intention to withdraw or limit the scope of the CLA's approval and provide at least 60 days for the CLA to respond.

(3) The Commission will notify a CLA in writing when it has concerns or evidence that the CLA is not carrying out its responsibilities under the labeling program in accordance with the Commission's rules in this subpart and policies and request that it explain and correct any apparent deficiencies.

(4) The Public Safety and Homeland Security Bureau shall provide notice to the CLA that the Bureau proposes to terminate the CLA's authority and provide the CLA a reasonable opportunity to respond (not more than 20 days) before reaching a decision on possible termination.

(5) If the Commission withdraws its recognition of a CLA, all grants issued by that CLA will remain valid unless specifically set aside or revoked by the Commission.

(6) A list of recognized CLAs will be published by the Commission.

(f) *Scope of responsibility.* (1) A CLA shall receive and evaluate applications and supporting data requesting authority to use the FCC IoT Label on the product subject to the application.

(2) A CLA shall grant authorization to use the FCC IoT Label with a complying consumer IoT product in accordance with the Commission's rules in this subpart and policies.

(3) A CLA shall accept test data from any Lead Administrator-recognized accredited CyberLAB, subject to the requirements in ISO/IEC 17065 and shall not unnecessarily repeat tests.

(4) A CLA may establish and assess fees for processing applications and other Commission-required tasks.

(5) A CLA may only act on applications that it has received or which it has issued a certification authorizing use of the FCC IoT Label.

(6) A CLA shall dismiss an application that is not in accordance with the provisions of this subpart or when the applicant requests dismissal, and may dismiss an application if the applicant does not submit additional information or test samples requested by the CLA.

(7) A CLA shall ensure that manufacturers make all required information accessible to the IoT registry.

(8) A CLA shall participate in a consumer education campaign in coordination with the Lead Administrator.

(9) A CLA shall receive complaints alleging a product bearing the FCC IoT Label does not support the cybersecurity criteria conveyed by the Cyber Trust Mark and refer these complaints to the Lead Administrator which will notify the Public Safety and Homeland Security Bureau.

(10) A CLA may not:

(i) Make policy, interpret unclear provisions of the statute or rules, or interpret the intent of Congress;

(ii) Grant a waiver of the rules in this subpart; or

(iii) Take enforcement actions.

(11) All CLA actions are subject to Commission review.

(g) *Post-market surveillance requirements.* (1) In accordance with ISO/IEC 17065, a CLA shall perform appropriate post-market surveillance activities. These activities shall be based on type testing a certain number of samples of the total number of product types for which the CLA has certified use of the Label.

(2) PSHSB may request that a grantee of authority to use the FCC IoT Label submit a product sample directly to the CLA that evaluated the grantee's application as part of the post

market surveillance. Any product samples requested by the Commission and tested by the CLA will be counted toward a minimum number of samples that the CLA must test to meet its post market surveillance requirements.

(3) A CLA may also request a grantee submit samples of products that the CLA has certified to use the FCC IoT Label directly to the CLA.

(4) If during post market surveillance of a complying consumer IoT product, a CLA determines that the product fails to comply with the technical regulations (or other FCC requirements) for that product, the CLA shall immediately notify the grantee and the Commission in writing of its findings. The grantee shall provide a report to the CLA describing the actions taken to correct the situation, as provided in § 8.216, and the CLA shall provide a report of these actions to the Commission within 30 days.

(5) CLAs shall submit periodic reports to the Commission of their post-market surveillance activities and findings in a format and by a date specified by the Commission.

§ 8.221 Requirements for the Lead Administrator.

(a) *Establishing a Lead Administrator*. If more than one qualified entity is selected by the Commission to be a CLA, the Commission will select a Lead Administrator. The Lead Administrator shall:

(1) Interface with the Commission on behalf of the CLAs, including but not limited to submitting to the Bureau all complaints alleging a product bearing the FCC IoT Label does not meet the requirements of the Commission's labeling program;

(2) Coordinate with CLAs and moderate stakeholder meetings;

(3) Accept, review, and approve or deny applications from labs seeking recognition as a lab authorized to perform the conformity testing necessary to support an application for authority to affix the FCC IoT Label, and maintain a publicly available list of Lead Administrator-recognized labs and a list of labs that have lost their recognition;

(4) Within 90 days of election as Lead Administrator, the Lead Administrator will, in collaboration with the CLAs and stakeholders (*e.g.*, cyber experts from industry, government, and academia):

(i) Submit to the Bureau recommendations identifying and/or developing the technical standards and testing procedures for the Commission to consider with regard to at least one class of IoT products eligible for the IoT labeling program. The Bureau will evaluate the recommendations, subject to any required public notice and comment, incorporate them by reference into the Commission's rules in this subpart;

(ii) Submit to the Bureau a recommendation on how often a given class of IoT products must renew their request for authority to bear the FCC IoT Label, which may be dependent on the type of product, and that such a recommendation be submitted in connection with the relevant standards recommendations for an IoT product or class of IoT products. The Bureau will evaluate the recommendations, and if the Bureau approves of the recommendations, subject to any required public notice and comment, incorporate them by reference into the Commission's rules in this subpart;

(iii) Submit to the Bureau a recommendation on procedures for post market surveillance by the CLAs. The Bureau will evaluate the recommendations, and if the Bureau approves of the recommendations, subject to any required public notice and comment, incorporate them by reference into the Commission's rules in this subpart;

(iv) Make recommendations to the Bureau with regard to updates to the registry including whether the registry should be in additional languages, and if so, to recommend specific languages for inclusion; and

(v) Submit to the Bureau recommendations on the design of the FCC IoT Label, including but not limited to labeling design and placement (*e.g.*, size and white spaces, product packaging) and whether to include the product support end date on labels for certain products or category of products. The Bureau will evaluate the recommendations, and if the Bureau approves of the recommendations, subject

to any required public notice and comment, incorporate them by reference into the Commission's rules in this subpart;

(5) Within 45 days of publication of updates or changes to NIST guidelines, or adoption by NIST of new guidelines, recommend in collaboration with CLAs and other stakeholders any appropriate modifications to the labeling program standards and testing procedures to stay aligned with the NIST guidelines;

(6) Submit to the Commission reports on CLAs' post-market surveillance activities and findings in the format and by the date specified by Public Safety and Homeland Security Bureau;

(7) Develop in collaboration with stakeholders a consumer education campaign, submit the plan to the Public Safety and Homeland Security Bureau, and participate in consumer education;

(8) Receive complaints about the labeling program, including but not limited to consumer complaints about the registry and coordinate with manufacturers to resolve any technical problems associated with consumers accessing the information in the registry;

(9) Facilitate coordination between CLAs; and

(10) Submit to the Commission any other reports upon request of the Commission or as required by Commission rules in this subpart.

(b) *Criteria for designation*. In addition to completing the CLA application information, entities seeking to be the Lead Administrator will submit a description of how they will execute the duties of the Lead Administrator, including:

(1) Their previous experience in IoT cybersecurity;

(2) What role, if any, they have played in IoT labeling;

(3) Their capacity to execute the Lead Administrator duties;

(4) How they would engage and collaborate with stakeholders to identify or develop the Bureau recommendations;

(5) A proposed consumer education campaign; and

(6) Additional information the applicant believes demonstrates why they should be the Lead Administrator.

§ 8.222 Establishment of an IoT Registry.

(a) A grantee of authority to use the FCC IoT Label shall provide information about the complying consumer IoT product to the public. Information supplied by grantees shall be made available in a dynamic, decentralized, publicly accessible registry through a common Application Programming Interface (API) that is secure by design.

(b) A grantee of authority to use the FCC IoT Label shall publish the following information through the common API in the Registry:

(1) Product Name;

(2) Manufacturer name;

(3) Date the product received authorization (*i.e.*, cybersecurity certification) to affix the label and current status of the authorization (if applicable);

(4) Name and contact information of the CLA that authorized use of the FCC IoT Label;

(5) Name of the lab that conducted the conformity testing;

(6) Instructions on how to change the default password (specifically state if the default password cannot be changed);

(7) Information (or link) for additional information on how to configure the device securely;

(8) Information as to whether software updates and patches are automatic and how to access security updates/patches if they are not automatic;

(9) The date until which the entity promises to diligently identify critical vulnerabilities in the product and promptly issue software updates correcting them, unless such an update is not reasonably needed to protect against cybersecurity failures (*i.e.*, the minimum support period); alternatively, a statement that the device is unsupported and that the purchaser should not rely on the manufacturer to release security updates;

(10) Disclosure of whether the manufacturer maintains a Hardware Bill of Materials (HBOM) and/or a Software Bill of Materials (SBOM); and

(11) Additional data elements that the Bureau deems necessary.

PART 9—911 REQUIREMENTS

Subpart A—Purpose and Definitions

Sec.
9.1 Purpose.
9.2 [Reserved]
9.3 Definitions.

Subpart B—Telecommunications Carriers

9.4 Obligation to transmit 911 calls.
9.5 Transition to 911 as the universal emergency telephone number.
9.6 Obligation for providing a permissive dialing period.
9.7 Obligation for providing an intercept message.
9.8 Obligation of fixed telephony providers to convey dispatchable location.

Subpart C—Commercial Mobile Radio Service

9.9 Definitions.
9.10 911 Service.

Subpart D—Interconnected Voice over Internet Protocol Services

9.11 E911 Service.
9.12 Access to 911 and E911 service capabilities.

Subpart E—Telecommunications Relay Services for Persons With Disabilities

9.13 Jurisdiction.
9.14 Emergency calling requirements.

Subpart F—Multi-Line Telephone Systems

9.15 Applicability.
9.16 General obligations—direct 911 dialing, notification, and dispatchable location.
9.17 Enforcement, compliance date, State law.

Subpart G—Mobile-Satellite Service

9.18 Emergency Call Center service.

Subpart H—Resiliency, Redundancy, and Reliability of 911 Communications

9.19 Reliability of covered 911 service providers.
9.20 Backup power obligations.

Subpart I—911 Fees

9.21 Applicability.
9.22 Definitions.
9.23 Designation of acceptable obligations or expenditures for purposes of the Consolidated Appropriations Act, 2021, Division FF, Title IX, section 902(c)(1)(C).
9.24 Petition regarding additional purposes and functions.
9.25 Participation in annual fee report data collection.
9.26 Advisory committee participation.

Subpart J—Next Generation 911

9.27 Applicability, scope, and purpose.
9.28 Definitions.
9.29 Next Generation 911 transition requirements.
9.30 Next Generation 911 implementation deadlines.
9.31 Valid requests for delivery of 911 traffic in Internet Protocol-based formats.
9.32 Designation of NG911 Delivery Points.
9.33 Cost responsibilities.
9.34 Modification of NG911 requirements by mutual agreement.

AUTHORITY: 47 U.S.C. 151–154, 152(a), 155(c), 157, 160, 201, 202, 208, 210, 214, 218, 219, 222, 225, 251(e), 255, 301, 302, 303, 307, 308, 309, 310, 316, 319, 332, 403, 405, 605, 610, 615, 615 note, 615a, 615b, 615c, 615a–1, 616, 620, 621, 623, 623 note, 721, and 1471, and Section 902 of Title IX, Division FF, Pub. L. 116–260, 134 Stat. 1182, unless otherwise noted.

SOURCE: 84 FR 66760, Dec. 5, 2019, unless otherwise noted.

Subpart A—Purpose and Definitions

§ 9.1 Purpose.

The purpose of this part is to set forth the 911 and E911 service requirements and conditions applicable to telecommunications carriers (subpart B); commercial mobile radio service (CMRS) providers (subpart C); interconnected Voice over Internet Protocol (VoIP) providers (subpart D); providers of telecommunications relay services (TRS) for persons with disabilities (subpart E); multi-line telephone systems (MLTS) (subpart F); and Mobile-Satellite Service (MSS) providers (subpart G). The rules in this part also include requirements to help ensure the resiliency, redundancy, and reliability of communications systems, particularly 911 and E911 networks and/or systems (subpart H).

EFFECTIVE DATE NOTE: At 89 FR 78128, Sept. 24, 2024, §9.1 was revised. This action was delayed indefinitely. For the convenience of the user, the added and revised text is set forth as follows: