# Cybersecurity Labeling Management Measures

# (Draft for Comment)

## Chapter I General Provisions

**Article 1** The Measures are formulated in accordance with the Cybersecurity Law of the People's Republic of China and other relevant laws and regulations to enhance the cybersecurity capabilities of products, strengthen the protection of consumers' rights and interests, and safeguard cybersecurity and public interests.

**Article 2** The term "cybersecurity label" as used in the Measures refers to an information label that reflects the level of a product's inherent cybersecurity capabilities.

Products with internet connectivity functions are subject to the Measures. Specific products shall be subject to catalogue-based management.

**Article 3** The administration of cybersecurity labels adheres to the principle of coordinating development and security. Product manufacturers participate on a voluntary basis.

Product manufacturers are encouraged to enhance their products' cybersecurity capabilities in accordance with the Measures and affix cybersecurity labels.

Consumers are encouraged to prioritize the selection of products bearing cybersecurity labels.

**Article 4** The Cyberspace Administration of China and the Ministry of Industry and Information Technology are responsible for the administration of cybersecurity labels. They shall formulate and publish in batches the *Catalogue of Products Subject to Cybersecurity Labeling*, specifying the detailed implementation rules and the national standards or technical documents applicable to each product category. The China Electronics Standardization Institute (hereinafter referred to as the "Filing Agency") is authorized to undertake the filing, information release, and handling of violations related to cybersecurity labels.

## Chapter II Label Implementation

**Article 5** The cybersecurity capabilities corresponding to the cybersecurity label are graded, in ascending order, as Basic, Enhanced, and Leading. The corresponding label grades are represented by one star, two stars, and three stars, respectively. The Basic grade requires products to meet the fundamental security requirements of relevant national standards, such as the absence of weak or common default passwords, the establishment of a vulnerability management mechanism with dynamic patching, and the maintenance of software updates. The Enhanced grade requires a product's cybersecurity capability to reach an advanced domestic level. The Leading grade requires a product's cybersecurity capability to reach an advanced international level and, in addition, requires the product to undergo penetration testing to verify its capability to resist high-level cyberattacks.

The specific security requirements for each label grade pertaining to a product category shall be defined in the implementation rules. These security requirements shall align with current national and international standards and shall fully reference and incorporate relevant experiences from other countries and regions that have implemented cybersecurity labeling systems.

**Article 6** The cybersecurity label (English name: China Cybersecurity Label) shall include the following basic information:

(1) Name of the product manufacturer;

(2) Product model/ specification;

(3) Cybersecurity capability grade;

(4) Validity period of the cybersecurity label;

(5) Name of the testing laboratory;

(6) Number(s) of the national standard(s) or technical document(s) used as the basis;

(7) A filing information code, which can be scanned to obtain information such as the test report, key indicators, and the product manufacturer's declaration of conformity.

The basic format of the cybersecurity label is as follows:


The specific format of the label for each product category shall be specified in the corresponding

implementation rules and may be appropriately adjusted based on the product's actual form, building upon the aforementioned basic format.

**Article 7** For products required to bear the cybersecurity label, the product manufacturer shall conduct cybersecurity capability testing in accordance with the relevant requirements of the implementation rules to determine the cybersecurity capability grade and obtain a test report.

(1) For products requiring a One-Star or Two-Star label, the product manufacturer may conduct the testing using its own in-house laboratory or by commissioning a qualified third-party testing agency duly accredited according to law.

(2) For products requiring a Three-Star label, in addition to fulfilling the relevant testing requirements, the product manufacturer shall also commission a qualified third-party testing agency to conduct penetration testing.

**Article 8** The Filing Agency shall establish a Cybersecurity Label Filing Management Platform. Product manufacturers shall file their cybersecurity labels through this platform via an online process.

The following materials shall be submitted electronically during filing:

(1) Cybersecurity Label Filing Form;

(2) Test report for the cybersecurity capability grade;

(3) Designed cybersecurity label format for the product, in accordance with the implementation rules;

(4) Product Manufacturer's Declaration of Conformity;

(5) Business license of the product manufacturer;

(6) Documentation proving the relevant testing capabilities of the manufacturer's own in-house laboratory, or the accreditation certificate of the commissioned third-party testing agency;

(7) If the filing materials are submitted by an agent, the letter of authorization and other relevant documents from the product manufacturer shall also be submitted.

The product manufacturer and its agent shall be responsible for the authenticity, accuracy, and completeness of the aforementioned materials.

**Article 9** The Filing Agency shall, within 10 working days from the date of receiving complete filing materials, conduct a formal review of the materials' authenticity, accuracy, and completeness, complete the filing process, and announce the relevant filing information of the product.

Upon completion of the filing, the product manufacturer may print, use, and display the cybersecurity label in accordance with the requirements of the implementation rules.

**Article 10** The validity period of the cybersecurity label shall be specified in the relevant product

implementation rules. For products that have completed filing, if changes occur to key technical parameters or other factors that may affect the product's cybersecurity capabilities, or if the label exceeds its validity period, re-filing shall be required.

**Article 11** No organization or individual may forge or fraudulently use cybersecurity labels, or engage in false advertising by means of cybersecurity labels.

**Article 12** The Filing Agency shall establish and improve standardized procedures for cybersecurity label filing and carry out related work in an objective and impartial manner.

The product manufacturer's own in-house laboratory or a third-party testing agency shall strictly conduct tests in accordance with relevant standards, ensuring that test results are objective, impartial, truthful, and accurate. They shall not falsify test results or issue false test reports.

The Filing Agency and testing agencies shall not disclose any state secrets or trade secrets obtained during the course of their work.

## Chapter III Supervision and Administration

**Article 13** The Cyberspace Administration of China and the Ministry of Industry and Information Technology are responsible for organizing the supervision and inspection of the filing and usage of cybersecurity labels. If activities violating the provisions of the Measures are discovered, they shall be handled promptly in accordance with relevant regulations.

Local cyberspace administrations and communications administrations are responsible for organizing the supervision and inspection of cybersecurity label usage within their respective jurisdictions. If activities violating the provisions of the Measures are discovered, they shall promptly notify the Filing Agency.

**Article 14** The Filing Agency shall revoke the filing and issue a timely public announcement upon discovering any of the following circumstances:

(1) The filing materials contain falsifications;

(2) The cybersecurity label does not correspond to the actual cybersecurity capability;

(3) The used cybersecurity label does not comply with relevant regulations regarding format, specifications, or other labeling requirements;

(4) The product manufacturer terminates technical support services for the filed product;

(5) Other violations that warrant the revocation of the label.

**Article 15** If a product manufacturer forges or fraudulently uses cybersecurity labels or engages in false advertising by means of cybersecurity labels, the Filing Agency shall revoke the cybersecurity label filing for the relevant products, publicly announce the manufacturer's violation, and shall not accept new product filings from that manufacturer for a period of one year from the date of the announcement.

**Article 16** If a product manufacturer's own in-house laboratory or a third-party testing agency falsifies test results or issues false test reports, the Filing Agency shall revoke the cybersecurity label filing for the relevant products, publicly announce the testing agency's violation, and shall not accept test results from that agency for a period of one year from the date of the announcement.

**Article 17** Any organization or individual discovering activities that violate the provisions of the Measures may report them to the local cyberspace administration or communications administration. The local cyberspace administration and communications administration shall promptly investigate and handle the report, maintain confidentiality for the informant, and the Filing Agency shall cooperate during the investigation process.

**Article 18** If a product security vulnerability is discovered or becomes known during the cybersecurity capability testing process, it shall be reported, patched, and disclosed in accordance with the relevant requirements of the *Regulations on the Management of Network Product Security Vulnerabilities*.

### Chapter IV Supplementary Provisions

**Article 19** The term “cybersecurity capability” as used in the Measures refers to the capability of a network product itself—achieved through the implementation of necessary technical and managerial measures by the product manufacturer—to protect against attacks, intrusions, interference, damage, and illegal use, and to ensure the stable and reliable operation of the product as well as the integrity, confidentiality, and availability of network data.

**Article 20** Critical network equipment and specialized cybersecurity products shall be subject to security management in accordance with the *Announcement on Matters Concerning Adjusting the Security Management of Specialized Cybersecurity Products (No. 1, 2023)* issued by the Cyberspace Administration of China, the Ministry of Industry and Information Technology, the Ministry of Public Security, the Ministry of Finance, and the National Certification and Accreditation Administration. Such products shall not be included in the *Catalogue of Products Subject to Cybersecurity Labeling*.

**Article 21** The Measures shall come into effect on MM DD, 2026.

## Catalogue of Products Subject to Cybersecurity Labeling (First Batch)

## (Draft for Comment)

| Serial No. | Product Name | Scope of Application |
|---|---|---|
| CSL 001-2025 | Consumer Internet-Connected Cameras | Applies to standalone cameras with internet connectivity functions that are purchased and used by consumers to provide audio-visual information collection and processing services for individuals and households.<br>Does not apply to cameras intended for public security purposes. |