SESEC VI Translation

Translation of Implementation Rules and Practice Guide for Consumer Connected Cameras under China Cybersecurity Labeling

June | 2026

Seconded European Standardization Expert in China

(SESEC)

INTRODUCTION:

On 15 June 2026, the Cyberspace Administration of China(CAC), together with the Ministry of Industry and Information Technology (MIIT) and the Ministry of Public Security (MPS), jointly issued the first product catalogue and the supporting implementation rules under the ***Measure for the Administration of the China Cybersecurity Labeling*** (hereinafter referred to the Measures). Released in April 2026, the Measure took effect on 1 July 2026. The first catalogue covers only one category which is consumer-grade internet-connected cameras, while cameras used in the public security domains are excluded.

The Measures target products with internet connectivity - a feature common to what the EU Cyber Resilience Acts calls "product with digital elements". Unlike CRA' s mandatory market-access regime, however, the Chinese scheme operates on the principle of voluntary participation. Products such as Wi-Fi router, servers, and Virtual Private Network (VPN) are not covered, as they are already regulated as **Key Network Equipment and Exclusive Cybersecurity Products** under a separate catalogue issued and maintained by CAC since 2017.

The Labeling scheme mainly seeks to raise public awareness of cybersecurity and to phase out products with inadequate or outdated security capabilities through market-driven choices rather than mandates.

Published along with the implementation rules is the TC260 practice guide, ***TC260-PG-20265A Cybersecurity Labeling: Security Requirements for Consumer Connected Cameras,*** which sets out product security requirements across 5 technical dimensions.

Although the labeling scheme will stay voluntary, it is premature to judge that it will not bring about influence to market access and product competitiveness, especially when cybersecurity issues are always a critical matter of national interests.

SESEC strongly recommends that affected stakeholders study the Practice Guide and the national standards it references, assess whether their products meet the security capability requirements, and prepare early to stay competitive in the Chinese market.

An unofficial translation of both Implementation Rules and Practice Guide has been prepared by SESEC for European stakeholder's references.

Original version from the Cyberspace Administration of China's website:

https://www.cac.gov.cn/2026-06/18/c_1783525604615337.htm

DISCLAIMER:

This English version is an unofficial translation of the original Chinese document, produced by SESEC for reference purposes only. In the event of any discrepancies between the English and Chinese versions, the Chinese version shall prevail. SESEC accepts no responsibility or liability for any errors, inaccuracies, or misunderstandings arising from this translation.

Index

CAC Implementation Rules for Consumer Connected Cameras under Cybersecurity Labeling

1 General Provisions

1.1 This document is formulated in accordance with the Measures for the Administration of Cybersecurity Labeling (hereinafter referred to as the "Measures").

1.2 This document applies to the filing and use of the Cybersecurity Label for consumer connected cameras. For the purposes of this document, a "consumer connected camera" means a standalone camera with internet connectivity that is purchased and used by individual consumers or organizations and that provides audio and video information collection and processing services for individuals or organizations.

This document does not apply to cameras used in the domain of public security.

1.3 Manufacturers of consumer connected camera products may obtain the Cybersecurity Label on a voluntary basis in accordance with this document.

1.4 The China Electronics Standardization Institute (hereinafter referred to as the "Filing Body") shall undertake the filing of the Cybersecurity Label, the publication of information, and related work.

2 Design and Specifications of the Cybersecurity Label

2.1 The Cybersecurity Label is a colored label on a blue background, with a length of 46.9 mm and a width of 50 mm. The label may be enlarged or reduced in proportion, provided that the graphics, text, and filing information code remain clear and legible.

2.2 The Cybersecurity Label for consumer connected cameras shall contain the following information:

(1) the name of the product manufacturer;

(2) the specifications and model of the product;

(3) the cybersecurity capability level;

(4) the validity period of the Cybersecurity Label;

(5) the name of the testing laboratory;

(6) the reference number of the national standard or technical document relied upon; and

(7) the filing information code, by scanning which the test report, key indicators, the product manufacturer's declaration of conformity, and other information may be accessed.

2.3 A sample illustration of the Cybersecurity Label is shown in Figure 1 and may be downloaded from the Cybersecurity Label Filing Management Platform (hereinafter referred to as the "Filing Management Platform").

Figure 1 Sample Illustration of the Cybersecurity Label

3 Testing of Cybersecurity Capabilities

3.1 The cybersecurity capabilities of consumer connected cameras corresponding to the Cybersecurity Label are classified, in ascending order, into three levels: Basic Level, Enhanced Level, and Leading Level, and the corresponding label grades are represented by one star, two stars, and three stars, respectively.

3.2 The cybersecurity capabilities of consumer connected cameras shall be tested in accordance with the Cybersecurity Standard Practice Guide — ***TC260-PG-20265A Cybersecurity Labeling: Security Requirements for Consumer Connected Cameras***, so as to determine the level of each individual cybersecurity capability item, namely physical and hardware security, system and software security, network and communication security, data security and personal information protection, and security assurance. A cybersecurity capability level may be granted only where all individual requirements at that level are satisfied.

3.3 Products for which the following elements are identical may be classified into the same testing unit:

(1) the manufacturer, brand, and generation number of the chip;

(2) the version of the firmware, which generally contains the operating system, functional software, third-party components, and the like;

(3) the type and version of the communication module;

(4) the device access management mode, e.g., management via a management webpage or management via an application; and

(5) configurations that affect the product's attack surface and cybersecurity capabilities, including physical interfaces, communication protocols, network ports, application interfaces, the methods and strength of identity authentication, access control methods, encryption schemes, and the like.

3.4 Where products are tested on a testing-unit basis, the product manufacturer shall issue a statement on the classification of testing units, declaring that the elements used to classify the testing unit are identical across the different models within the same testing unit.

The testing institution shall select one product within the same testing unit for testing, randomly select a

certain number of models for product consistency testing and differential verification, and issue a test report. The number of product models randomly selected by the testing institution shall be 10% of the total number of models in the testing unit, rounded up.

The classification of the testing unit and the test results shall be valid only where the products pass the consistency testing and differential verification; where the products fail, the classification of testing units and the product testing shall be carried out anew.

3.5 The product manufacturer shall test its products, determine the cybersecurity capability level, and obtain a test report in the following manner:

(1) for consumer connected camera products to be labeled with the one-star or two-star grade, the product manufacturer may conduct the testing using its own testing laboratory or entrust a third-party testing institution that has obtained qualification accreditation in accordance with the law;

(2) for products to be labeled with the three-star grade, the product manufacturer shall, on the basis of satisfying the relevant testing requirements, additionally entrust a qualified third-party testing institution to conduct penetration testing; and

(3) for products to be labeled with the two-star grade, the manufacturer's own testing laboratory used for product testing shall hold CNAS accreditation, with an accredited scope covering cybersecurity testing.

4 Determination of the Information on the Cybersecurity Label

4.1 The name of the product manufacturer refers to the name of the owner or user of the product brand that bears legal liability for product quality.

4.2 The specifications and model of the product shall be consistent with those shown on the product nameplate.

4.3 The cybersecurity capability level of the product shall be consistent with the cybersecurity capability level shown in the test report.

4.4 The validity period of the Cybersecurity Label for consumer connected cameras is three years, commencing from the date on which the product filing information is announced.

4.5 The name of the testing laboratory refers to the name of the manufacturer's own testing laboratory or of the third-party testing institution that tested the product's cybersecurity capabilities, and shall be consistent with the testing institution shown in the test report.

4.6 The testing basis shall be the currently valid version of the ***Cybersecurity Standard Practice Guide — Cybersecurity Labeling: Security Requirements for Consumer Connected Cameras***.

4.7 The product filing information code shall be generated by the Filing Management Platform upon completion of the filing.

5 Filing of the Cybersecurity Label

5.1 The product manufacturer shall apply for filing with the Filing Body, complete the filing information on the Filing Management Platform, and submit the relevant filing materials prescribed by the Measures; templates of the materials may be downloaded from the Filing Management Platform. The product manufacturer and its agent shall be responsible for the authenticity, accuracy, and completeness of the aforesaid materials.

The filing materials are as follows:

(1) the Cybersecurity Label filing form;

(2) the test report;

(3) the designed artwork of the product's Cybersecurity Label;

(4) the product manufacturer's declaration of conformity;

(5) the product manufacturer's business license;

(6) where testing is conducted by the manufacturer's own testing laboratory, supporting materials evidencing the laboratory's testing capability (including laboratory qualifications, personnel competence, social insurance certificates of the personnel, equipment capability, and quality system documents); where the laboratory has obtained relevant national accreditation, copies of the corresponding accreditation certificates shall also be provided; where a third-party testing institution is entrusted to conduct the testing, supporting materials evidencing the capability of the third-party testing institution as referred to in the ***Cybersecurity Standard Practice Guide — Cybersecurity Labeling: Security Requirements for Consumer Connected Cameras*** shall also be provided;

(7) for consumer connected cameras that support access to telecommunications networks, information on the network access license for telecommunications equipment shall be provided; and

(8) where the filing materials are submitted by an agent, the product manufacturer's power of attorney and other relevant documents shall be submitted.

5.2 The Filing Body shall, within ten working days from the date of receipt of the complete filing materials, conduct a formal examination of the authenticity, accuracy, and completeness of the materials; where the materials fail the formal examination, the Filing Body shall notify the product manufacturer to supplement and correct the relevant materials in a timely manner. Upon passing the examination, the Filing Body shall complete the filing and announce the relevant filing information of the product together with the specimen of the Cybersecurity Label.

5.3 Where, for a product for which filing has been completed, any key technical parameter changes in a manner that may affect the product's cybersecurity capabilities, or where the validity period of the label has expired, the product shall be re-tested and re-filed in accordance with the currently valid version of the ***Cybersecurity Standard Practice Guide — Cybersecurity Labeling: Security Requirements for Consumer Connected Cameras***.

The key technical parameters include:

(1) the manufacturer, brand, and generation number of the chip;

(2) the types of the operating system and of the third-party components in the firmware;

(3) the type of the communication module;

(4) the device access management mode, e.g., management via a management webpage or management via an application; and

(5) configurations that affect the product's attack surface and cybersecurity capabilities, including physical interfaces, communication protocols, network ports, application interfaces, the methods and strength of identity authentication, access control methods, encryption schemes, and the like.

5.4 The Filing Body and testing institutions shall not disclose any state secrets or trade secrets obtained in the course of their work.

6 Announcement of the Cybersecurity Label

6.1 The Filing Body shall provide the general public with services for querying product Cybersecurity Label information, and shall promptly announce any violations by product manufacturers and testing institutions.

6.2 In any of the following circumstances, the Filing Body shall revoke the relevant filing information of the product and promptly make an announcement:

(1) the filing materials are falsified;

(2) the Cybersecurity Label is inconsistent with the product's actual cybersecurity capabilities;

(3) the Cybersecurity Label used does not conform to the labeling requirements concerning its design, specifications, and the like;

(4) the product manufacturer has terminated technical support services for the filed product; or

(5) other violations for which the filing shall be revoked.

6.3 Where a product manufacturer forges or fraudulently uses the Cybersecurity Label, or uses the Cybersecurity Label for false promotion, the Filing Body shall, in addition to revoking the filing of the Cybersecurity Label for the relevant products and announcing the manufacturer's violation, cease to accept filings of its products for one year from the date of the announcement.

6.4 Where a product manufacturer's own testing laboratory or a third-party testing institution forges test results or issues a false test report, the Filing Body shall revoke the filing of the Cybersecurity Label for the relevant products, announce the testing institution's violation, and cease to accept its test results for one year from the date of the announcement.

6.5 Where a product manufacturer, a third-party testing institution, or any other party engages in conduct such as fraud in cybersecurity capability testing or forgery or fraudulent use of the Cybersecurity Label, the competent authorities shall impose penalties in accordance with laws and regulations such as the Cybersecurity Law of the People's Republic of China and the Measures for the Supervision and Administration of Inspection and Testing Institutions.

6.6 Any organization or individual may lodge a complaint or report a violation concerning the Cybersecurity Label through the following channels:

Chinese Telephone/Fax: +86 (010) 64102777(Note: country code + area code + landline number)

Website: the Filing Management Platform (www.cncsl.cn).

7 Printing, Use, and Display of the Cybersecurity Label

7.1 Upon completion of the filing, the product manufacturer may print, use, and display the Cybersecurity Label on its own, and shall be responsible for the quality of the printing.

7.2 The Cybersecurity Label may be affixed to or hung on a conspicuous part of the consumer connected camera product, or displayed on the product packaging, in the user manual, on the device's start-up screen, in the application management interface, or the like. For products traded online, the corresponding Cybersecurity Label may be displayed in a prominent position on the main page on which the product information is displayed.

7.3 The Cybersecurity Label shall comply with the provisions of Section 2 of this document, and its graphics, text, and colors shall not be altered. Where actually required, the paper version of the label may be printed in monochrome.

TC260 Practie Guide — Security Requirements for Consumer Connected Cameras under Cybersecurity Labeling

1 Scope

This document specifies the technical cybersecurity requirements and security assurance requirements for consumer connected cameras, and sets out three tiers of security capability requirements: Basic Tier, Enhanced Tier and Leading Tier.

2 Normative References

The following referenced documents constitute the indispensable provisions of this document through normative citation herein. For dated references, only the version cited applies. For undated references, the latest edition (including all amendment slips) of the referenced document shall apply.

- ***GB 46864-2025*** Information Security Technology — Electronic Product Information Erasure Technical Requirements
- ***GB/T 25069-2022*** Information Security Technology — Terminology
- GB/T 35273-2020 Information Security Technology — Personal Information Security Specification
- ***GB/T 38674-2020*** Information Security Technology — Secure Programming Guide for Application Software
- ***GB/T 39276-2020*** Information Security Technology — General Security Requirements for Network Products and Services
- ***GB/T 45574-2025*** Data Security Technology — Security Requirements for Processing Sensitive Personal Information

3 Terms and Definitions

3.1 Consumer Connected Camera

An independent camera purchased and used by natural persons or organizations to provide audio and video information collection and processing services, with internet connectivity functions.
Note: This definition excludes cameras deployed for public security scenarios.

3.2 Critical Security Parameter (CSP)

Security-related information whose disclosure or tampering would compromise the security of a cryptographic module.
Examples: Secret and private cryptographic keys, authentication data such as passphrases, personal identification numbers (PINs), certificates or other trust anchors.
Note: Key critical security parameters requiring prioritized protection in consumer connected cameras include device root keys, user identity authentication information, device authentication information, keys ensuring authenticity and integrity of security updates, and keys ensuring confidentiality and integrity of network communications.
[Source: ***GB/T 25069-2022***, with modifications]

3.3 Firmware

An ordered set of instructions and associated data functionally independent of main memory, typically stored in read-only memory (ROM).
[Source: ***GB/T 25069-2022***]

3.4 Device Binding

The process of establishing an exclusive ownership relationship between a user account and a consumer connected camera device.

3.5 Hardcode

The practice of substituting a fixed constant value for a variable during coding.
[Source: ***GB/T 38674-2020***]

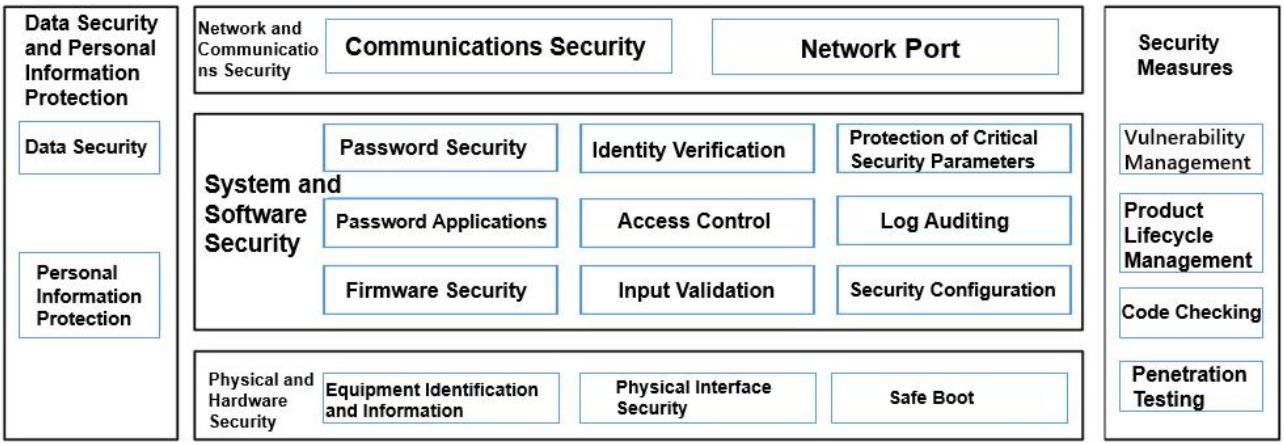
4 Overview

This document establishes a security framework for consumer connected cameras covering five dimensions: Physical & Hardware Security, System & Software Security, Network & Communication Security, Data Security & Personal Information Protection, and Security Assurance (see Figure 1).
The cybersecurity capabilities of consumer connected cameras are classified into three tiers with progressively higher security levels: Basic Tier, Enhanced Tier and Leading Tier.

- Basic Tier: The product meets fundamental baseline cybersecurity standards.
- Enhanced Tier: The product reaches advanced cybersecurity levels among similar products.
- Leading Tier: The product achieves industry-leading cybersecurity performance among similar products.

A product may obtain a corresponding cybersecurity capability tier only if it complies with all individual requirements of that tier. The mandatory security requirements applicable to products of each tier are specified in Annex A, and test evaluation methodologies are provided in Annex B.
Third-party testing institutions conducting testing for Basic Tier and Enhanced Tier products shall satisfy the requirements specified in Clause C.1 of Annex C. Institutions undertaking testing for Leading Tier products shall comply with both Clause C.1 and C.2 of Annex C.

Figure 1 Security Framework for Consumer Connected Cameras



5 Basic Tier Requirements

5.1 Physical & Hardware Security

5.1.1 Device Identification & Information

Consumer connected cameras shall satisfy the following requirements:
a) Be assigned a unique device identifier;
Note: A device identifier refers to a unique symbolic identifier used to identify or verify the legitimate identity of a device.
b) Clearly mark the device model, product name and other information on the exterior of the device.

5.2 System & Software Security

5.2.1 Passphrase Security

Consumer connected cameras shall satisfy the following requirements:
a) Where passphrases are adopted for identity authentication, weak passphrases are prohibited. Passphrases shall be no less than 8 characters long and contain at least two categories selected from numerals, lowercase letters, uppercase letters and special characters.
Note: This clause covers, without limitation, randomly generated initial passphrases, passphrases initially

set by users, passphrases configured during device activation, and passphrases set or modified during device use.
b) For devices adopting factory preset passphrase login, each individual device shall be provisioned with a unique randomly generated initial passphrase. Fixed or universal default passphrases are forbidden, and passphrase complexity shall comply with Clause 5.2.1 a).
c) For devices adopting an activation mechanism at factory delivery, all operations other than activation shall be blocked before the completion of device activation. Where activation requires users to set a passphrase, the passphrase shall satisfy the complexity requirements of Clause 5.2.1 a).
Note: Activation refers to a mechanism requiring users to perform relevant operations upon first use to enable device functions, including passphrase setup, QR code scanning and other means.
d) Implement anti-brute-force protection for passphrases; protective measures shall be triggered after exceeding a specified number of consecutive failed login attempts.
Note: Protective measures include account locking, IP locking, login delay, verification code login and the like; the threshold for failed login attempts shall preferably be less than 10 times.
e) Provide a physical button or other secure means to restore the device to factory default settings when users forget their account credentials or passphrases.

5.2.2 Identity Authentication

Consumer connected cameras shall satisfy the following requirements:
a) Assign a unique identifier to each user identity, and deploy protective measures to prevent tampering of such identifiers.
b) No undisclosed accounts or login mechanisms shall exist.
Note: Undisclosed accounts include test accounts, operation & maintenance accounts, unused third-party software accounts and the like; undisclosed login methods include special key combinations and others.
c) Authenticate all accessing subjects for all network-based device login channels.
Note: Login channels include network ports, WEB management interfaces, management applications and so forth.
d) Where digital certificates are used for identity authentication, the device digital certificate shall be bound to the device identifier.

5.2.3 Critical Security Parameter Protection

Consumer connected cameras shall satisfy the following requirements:
a) Adopt cryptographic technologies to protect the confidentiality of identity authentication information.
b) No critical security parameters shall be hardcoded within the device software code.

5.2.4 Cryptography Application

Cryptographic technologies deployed in consumer connected cameras for identity authentication, security updates, network communications, data storage, secure boot and other scenarios shall comply with national cryptography administration regulations.

5.3 Data Security & Personal Information Protection

5.3.1 Data Security

Products shall provide users with an information erasure function complying with GB 46864-2025.
Note: The function shall be provided by the product or its management terminal for independent user operation.

5.3.2 Personal Information Protection

Consumer connected cameras shall satisfy the following requirements:
a) Where personal information is processed, publicly display personal information processing rules on product management interfaces, user manuals or linked pages for users to review, copy or download for offline review. The rules shall cover, without limitation:

1. Name and contact information of the personal information processor;
2. Categories of processed personal information, together with corresponding processing purposes and methods;
3. Clear indication of whether personal information is stored within mainland China, storage duration,

and disposal procedures upon expiry of the storage period;
4. Explanation of processing necessity, impacts on users' personal rights and interests, and adopted security safeguards;
5. Methods and channels for users to access, copy, transfer, correct, supplement and delete personal information, cancel accounts, and withdraw consent.

b) Collection of personal information shall comply with Clauses 5.2 and 5.4 of GB/T 35273-2020.
c) Storage of personal information shall comply with Clauses 6.1 and 6.3 of GB/T 35273-2020.
d) No associative analysis of individual identities captured in images or videos shall be performed without user consent, except for statutory obligations or other provisions stipulated by laws and regulations.
e) Processing of sensitive personal information shall comply with Chapter 5 and Clause 6.1 of ***GB/T 45574-2025***.

5.4 Security Assurance

5.4.1 Vulnerability Management

Manufacturers of consumer connected cameras shall satisfy the following requirements:
a) Ensure devices contain no known high-risk or higher-severity vulnerabilities.
Note: Known high-risk vulnerabilities refer to vulnerabilities recorded in national vulnerability databases including CNVD, CNNVD, NVDB and others.
b) Explicitly disclose and publicize device model information, and continuously provide security updates within timeframes specified by regulations or agreed by parties.
c) Establish and implement tracking and emergency response mechanisms for security defects and vulnerabilities of product hardware, software and associated components to address defects and vulnerabilities identified during operation and maintenance.
d) Upon discovery of device security defects or vulnerabilities, submit relevant vulnerability information in accordance with the *Regulations on Administration of Cybersecurity Vulnerabilities of Network Products*, and promptly notify users of relevant security risks.

6 Enhanced Tier Requirements

6.1 Physical & Hardware Security

6.1.1 Device Identification & Information

In addition to complying with Clause 5.1.1, the following requirements shall also be met:
Deploy protective measures to prevent tampering of the unique device identifier.

6.1.2 Physical Interface Security

Consumer connected cameras shall satisfy the following requirements:
a) Disable all non-essential physical interfaces and debugging interfaces at factory delivery.
b) Provide users with a function to disable debugging interfaces, together with documentation explaining all physical interfaces.

6.1.3 Secure Boot

Consumer connected cameras shall implement a secure boot mechanism that verifies the authenticity and integrity of device firmware and boot components before normal startup is permitted.

6.2 System & Software Security

6.2.1 Passphrase Security

Shall comply with Clause 5.2.1.

6.2.2 Identity Authentication

In addition to complying with Clause 5.2.2, the following requirements shall also be met:
a) Authenticate all accessing subjects for login via physical device interfaces.
b) Critical operations such as modifying cybersecurity configurations and accessing sensitive personal information shall preferably require an authentication factor separate from device login credentials, or

security validation of the operating environment.
Note: Security validation methods include device login verification, network environment validation, operation behavior validation and the like.

6.2.3 Critical Security Parameter Protection

In addition to complying with Clause 5.2.3, the following requirements shall also be met:
a) Adopt cryptographic technologies to protect both the confidentiality and integrity of critical security parameters.
b) Establish standardized management workflows for critical security parameters.
Note 1: Managed objects include root keys, as well as critical security parameters for communication security protection, security update protection and sensitive personal information protection.
Note 2: Management workflows cover key generation, key configuration, key usage, key storage, key revocation and key destruction.
c) Ensure that core critical security parameters are unique for each individual device.
Note: Core critical security parameters include device root keys, keys ensuring authenticity and integrity of security updates, and keys ensuring confidentiality and integrity of network communications.

6.2.4 Cryptography Application

Shall comply with Clause 5.2.4.

6.2.5 Access Control

Consumer connected cameras shall satisfy the following requirements:
a) For devices supporting device binding functions:

1. Require interactive confirmation between the user and the device during binding.

Note: Interaction methods include physical button confirmation, Bluetooth/Wi-Fi pairing, acoustic signal authentication, QR code verification and others, to prevent unauthorized third-party binding.

2. After successful device binding, only accept control instructions originating from the bound account or its authorized sub-accounts.
3. After successful device binding, reject binding requests from other accounts unless the original bound user actively performs unbinding operations.

b) For devices supporting authorization functions:

4. Access control policies shall adhere to the principle of least privilege; by default, users other than device administrators shall be denied access to controlled resources and core functions.

Note: Only device administrators are authorized to modify access control policies.

5. The permission sharing function shall be exclusively available to device administrators; ordinary users shall not possess access to this function.
6. Deploy protective measures to ensure secure permission sharing.

Note: Security protection measures for sharing include instant revocation of shared permissions, granular viewing rights for grantees, and preferably configurable sharing validity periods, watermarking for shared video streams and other measures.

6.2.6 Log Audit

Consumer connected cameras shall satisfy the following requirements:
a) Record audit logs for events including power on/off, user creation, configuration modification, software upgrades, passphrase changes, failed login attempts, privileged user logins and other events. Audit records shall include event type, event timestamp, triggering subject, and event processing result.
b) Implement access control and protective mechanisms for audit logs to prevent unauthorized access, tampering and destruction of logs.

c) Deploy log storage overflow protection mechanisms to ensure continuous recording of the latest events after log storage capacity thresholds are reached.
d) Store audit logs on non-volatile storage media.

6.2.7 Firmware Security

Consumer connected cameras shall satisfy the following requirements:

a) Firmware upgrades shall implement security validation mechanisms to verify the authenticity and integrity of updated firmware packages.
b) Prompt users to perform automatic or manual security updates when new firmware versions are released; support resumption of interrupted updates.
c) Implement anti-rollback validation mechanisms to block unauthorized downgrade of firmware versions.
d) Prompt users to check and apply security updates upon initial device use or factory reset.

6.2.8 Input Validation

Consumer connected cameras shall perform security validation on all data inputs submitted via user interfaces and Application Programming Interfaces (APIs) to avoid abnormal behaviors during data processing.
Note: Abnormal data processing behaviors include SQL injection, operating system command injection, path traversal and other vulnerabilities.

6.2.9 Secure Configuration

Devices shall ship with secure default configurations, and provide users with guidance on secure setting configuration.

6.3 Network & Communication Security

6.3.1 Network Ports

Consumer connected cameras shall satisfy the following requirements:
a) Network services and port exposure shall follow the minimization principle; disable all non-mandatory network services and ports by default.
b) Minimize exposed port information when the device is in an unauthenticated state.
c) Allow users to manually disable non-essential network services.
d) Provide documentation detailing all network ports and corresponding services.

6.3.2 Communication Security

Consumer connected cameras shall satisfy the following requirements:
a) Adopt encryption technologies to protect the authenticity, confidentiality and integrity of transmitted critical security parameters and sensitive personal information.
b) Implement countermeasures against replay attacks.

6.4 Data Security & Personal Information Protection

6.4.1 Data Security

In addition to complying with Clause 5.3.1, the following requirements shall also be met:
a) Where device logs are uploaded for fault diagnosis, explicitly inform users of data collection methods, scope and purposes, and initiate uploads only after obtaining user consent.
b) Provide users with a switch to disable user data upload functions.
c) Adopt encryption and other security measures to protect the confidentiality and integrity of user data.

6.4.2 Personal Information Protection

In addition to complying with Clause 5.3.2, the following requirements shall also be met:
a) List all purposes, methods, categories of personal information provided to third processors and recipient entities in a clear inventory within personal information processing rules.
b) Provide convenient interactive channels via management terminals for users to exercise personal information rights, without imposing unreasonable restrictions on legitimate user requests.

6.5 Security Assurance

6.5.1 Vulnerability Management

Shall comply with Clause 5.4.1.

7 Leading Tier Requirements

7.1 Physical & Hardware Security

7.1.1 Device Identification & Information

Shall comply with Clause 6.1.1.

7.1.2 Physical Interface Security

Shall comply with Clause 6.1.2.

7.1.3 Secure Boot

Shall comply with Clause 6.1.3.

7.2 System & Software Security

7.2.1 Passphrase Security

Shall comply with Clause 6.2.1.

7.2.2 Identity Authentication

In addition to complying with Clause 6.2.2, the following requirement shall also be met:
Critical operations such as modifying cybersecurity configurations and accessing sensitive personal information shall require an authentication factor separate from device login credentials, or security validation of the operating environment.
Note: Security validation methods include device login verification, network environment validation, operation behavior validation and the like.

7.2.3 Critical Security Parameter Protection

In addition to complying with Clause 6.2.3, the following requirement shall also be met:
Protect device root keys via hardware-based protection mechanisms.
Note: Hardware protection methods include secure chips, dedicated secure storage partitions on system chips and other hardware security modules.

7.2.4 Cryptography Application

Shall comply with Clause 6.2.4.

7.2.5 Access Control

Shall comply with Clause 6.2.5.

7.2.6 Log Audit

In addition to complying with Clause 6.2.6, the following requirement shall also be met:
For devices deployed via cloud network platforms, audit logs shall be retained for a minimum period of 180 consecutive days.

7.2.7 Firmware Security

Shall comply with Clause 6.2.7.

7.2.8 Input Validation

Shall comply with Clause 6.2.8.

7.2.9 Secure Configuration

Shall comply with Clause 6.2.9.

7.3 Network & Communication Security

7.3.1 Network Ports

Shall comply with Clause 6.3.1.

7.3.2 Communication Security

Shall comply with Clause 6.3.2.

7.4 Data Security & Personal Information Protection

7.4.1 Data Security

Shall comply with Clause 6.4.1.

7.4.2 Personal Information Protection

In addition to complying with Clause 6.4.2, the following requirement is recommended:
Implement desensitization processing for sensitive personal information.
Note: Desensitization methods include blurring sensitive regions of images/videos, secure video encoding and other techniques.

7.5 Security Assurance

7.5.1 Vulnerability Management

Shall comply with Clause 6.5.1.

7.5.2 Product Lifecycle Management

Manufacturers of consumer connected cameras shall satisfy the following requirements:
a) Establish a full-lifecycle cybersecurity management mechanism covering design, development, testing, delivery, operation and maintenance phases.
b) Establish product security design workflows, conduct threat modeling in accordance with Clause 5.1.2.1 of ***GB/T 39276-2020*** to identify, analyze and mitigate device security threats.
c) Compile secure development documentation describing mechanisms and workflows ensuring confidentiality and integrity of data storage and transmission throughout device design and development.
d) Establish secure product development workflows complying with Clause 5.1.2.1 of ***GB/T 39276-2020***.
e) Establish standardized security testing workflows; conduct comprehensive security testing periodically or prior to major version releases, including static security testing, dynamic security testing, API testing, fuzz testing, code review and other test types.
f) Establish secure delivery workflows; implement security review and hardening prior to product shipment and major version releases, including:

1. Removal of unnecessary accounts and test accounts;
2. Elimination of all debugging code from released firmware versions;
3. Disabling redundant physical interfaces, network services, ports and network interfaces;
4. Enabling native operating system security features on camera terminals, including identity authentication, access control, data encryption and other security functions.

g) Establish security operation and maintenance workflows complying with Clause 5.2.2.3 of ***GB/T 39276-2020***.

7.5.3 Code Inspection

Manufacturers of consumer connected cameras shall satisfy the following requirements:

a) Commission qualified third-party testing institutions to conduct full code inspection of device firmware code, covering software vulnerabilities and errors, vulnerabilities embedded in third-party libraries and components, and hardcoded identity authentication credentials and critical security parameters.
b) Where dedicated mobile applications are deployed for device management, commission third-party testing institutions to inspect the management application, covering hardcoded critical security parameters, plaintext storage/transmission of critical security parameters and sensitive personal information, and unauthorized collection of sensitive personal information.

7.5.4 Penetration Testing

Manufacturers of consumer connected cameras shall satisfy the following requirements:
a) Commission qualified third-party testing institutions to conduct network security penetration testing; products shall contain no medium-risk or higher-severity vulnerabilities, and a formal penetration test report shall be issued.
b) Conduct cybersecurity crowd-sourced vulnerability testing; products shall contain no medium-risk or

higher-severity vulnerabilities, and a formal crowd-test report shall be issued.

c) Penetration testing shall satisfy the following requirements:

1. Testing duration of no less than 14 calendar days with a dedicated testing team of at least 5 personnel;
2. Execution of man-in-the-middle attack simulations;
3. Execution of privilege bypass attack simulations;
4. Execution of memory attack simulations including buffer overflow exploits;
5. Reverse engineering analysis to verify risks of sensitive information leakage;
6. For devices hosting WEB services, execution of common WEB attack simulations including SQL injection and Cross-Site Scripting (XSS).

d) Crowd-sourced vulnerability testing shall satisfy the following requirements:

7. Verify product resilience against vulnerability exploitation;
8. Testing duration of no less than 14 calendar days with a minimum of 20 participating testers possessing professional vulnerability discovery expertise and relevant project experience.

Annex A (Normative) Mandatory Security Requirements by Cybersecurity Capability Tier

Table A.1 Mandatory Security Requirements Applicable to Basic Tier, Enhanced Tier and Leading Tier Products

Security Category	Sub-item	Corresponding Clauses for Basic Tier	Corresponding Clauses for Enhanced Tier	Corresponding Clauses for Leading Tier
Physical & Hardware Security	Device Identification & Information	5.1.1	6.1.1	7.1.1
	Physical Interface Security	—	6.1.2	7.1.2
	Secure Boot	—	6.1.3	7.1.3
System & Software Security	Passphrase Security	5.2.1	6.2.1	7.2.1
	Identity Authentication	5.2.2	6.2.2	7.2.2
	Critical Security Parameter Protection	5.2.3	6.2.3	7.2.3
	Cryptography Application	5.2.4	6.2.4	7.2.4
	Access Control	—	6.2.5	7.2.5
	Log Audit	—	6.2.6	7.2.6
	Firmware Security	—	6.2.7	7.2.7
	Input Validation	—	6.2.8	7.2.8

	Secure Configuration	—	6.2.9	7.2.9
Network & Communication Security	Network Ports	—	6.3.1	7.3.1
	Communication Security	—	6.3.2	7.3.2
Data Security & Personal Information Protection	Data Security	5.3.1	6.4.1	7.4.1
	Personal Information Protection	5.3.2	6.4.2	7.4.2
Security Assurance	Vulnerability Management	5.4.1	6.5.1	7.5.1
	Product Lifecycle Management	—	—	7.5.2
	Code Inspection	—	—	7.5.3
	Penetration Testing	—	—	7.5.4

Annex B (Informative) Test Evaluation Methodologies

B.1 Basic Tier Evaluation

B.1.1 Physical & Hardware Security

B.1.1.1 Device Identification & Information

a) Test Procedures

1. Check whether the product contains specifications proving the uniqueness of the device identifier; attempt to modify the device identifier via management interfaces, interfaces and cloud platforms.
2. Check whether the device name, model and other information are clearly marked on the device exterior; cross-verify consistency between such information and the content displayed in user configuration interfaces and management mobile applications.

b) Expected Outcomes

1. The product provides specifications proving the uniqueness of the device identifier; the device identifier cannot be modified.
2. The device exterior clearly marks the device name, model and other information, which is consistent with the content displayed in user configuration interfaces and management mobile applications.

c) Judgment Criterion

Test results consistent with all expected outcomes = Compliant; all other cases = Non-compliant.

B.1.2 System & Software Security

B.1.2.1 Passphrase Security

a) Test Procedures

1. For systems adopting passphrase-based authentication, set or modify account passphrases to verify whether the system enforces checks on passphrase length and complexity, explicitly states minimum length and complexity requirements, and requires passphrases to contain at least two categories selected from numerals, lowercase letters, uppercase letters and special characters, with a minimum length of 8 characters.
2. Refer to product documentation to check factory preset initial passphrases; verify whether initial passphrases for each factory-shipped device are uniquely randomly generated, no fixed universal default passphrases are adopted, and passphrase complexity complies with Clause 5.2.1 a).
3. For products adopting an activation mechanism at factory delivery, check whether all operations other than activation are blocked before completion of activation, and no unnecessary exposed attack surfaces (such as network ports and physical interfaces) exist during pre-activation state. For products requiring users to set passphrases for activation, verify whether the system enforces passphrase complexity complying with Clause 5.2.1 a).
4. Simulate consecutive failed login attempts with invalid passphrases to verify whether the product implements anti-brute-force protection and triggers protective measures after exceeding the specified failure threshold, such as account locking, IP locking, login delay, verification code login and others.
5. Refer to product documentation to check whether the product supports physical button or other secure factory reset functions for forgotten account credentials or passphrases.

b) Expected Outcomes

1. Products adopting passphrase authentication prohibit weak passphrases, enforce a minimum passphrase length of 8 characters and require passphrases to contain at least two categories selected from numerals, lowercase letters, uppercase letters and special characters.
2. For products adopting factory preset passphrase login, each device is provisioned with a unique randomly generated initial passphrase; no fixed universal default passphrases are used, and passphrase complexity complies with Clause 5.2.1 a).
3. For products adopting an activation mechanism, all operations other than activation are blocked before completion of activation, with no unnecessary exposed network ports or physical interfaces during pre-activation state. For activation requiring passphrase setup, users are forced to set passphrases complying with Clause 5.2.1 a).
4. The product implements anti-brute-force protection and triggers protective measures after exceeding the specified number of failed login attempts.
5. The product supports physical button or other secure factory reset functions for forgotten account credentials or passphrases.

c) Judgment Criterion

Test results consistent with all expected outcomes = Compliant; all other cases = Non-compliant.

B.1.2.2 Identity Authentication

a) Test Procedures

1. Check the unique identifier generation algorithm and analyze whether protective measures against identifier tampering are deployed.
2. Refer to product documentation to check whether undisclosed accounts or login methods exist, including test accounts, operation & maintenance accounts, unused third-party software accounts and special key combination login methods.
3. Refer to product documentation to verify whether all network login channels including network ports, WEB management interfaces and management applications enforce identity authentication for accessing subjects.
4. For products adopting digital certificate authentication, refer to product documentation to verify whether the device digital certificate is bound to the device identifier.

b) Expected Outcomes

1. The product assigns a unique identifier to each user identity, with protective measures against identifier tampering deployed.
2. No undisclosed accounts or login methods exist in the product, including test accounts, operation & maintenance accounts, unused third-party software accounts and special key combination login channels.

3. All network-based device login channels enforce identity authentication for accessing subjects.
4. For products adopting digital certificate authentication, the device digital certificate is bound to the device identifier.

c) Judgment Criterion

Test results consistent with all expected outcomes = Compliant; all other cases = Non-compliant.

B.1.2.3 Critical Security Parameter Protection

a) Test Procedures

1. Check whether cryptographic technologies are adopted to protect the confidentiality of identity authentication information.
2. Review device software code to check whether hardcoded critical security parameters exist.

b) Expected Outcomes

1. The product adopts cryptographic technologies to protect the confidentiality of identity authentication information.
2. No hardcoded critical security parameters exist in the device software code.

c) Judgment Criterion

Test results consistent with all expected outcomes = Compliant; all other cases = Non-compliant.

B.1.2.4 Cryptography Application

a) Test Procedures

Refer to device design documentation to confirm whether cryptographic technologies adopted for identity authentication, security updates, network communications, data storage and secure boot comply with national cryptography administration regulations.

b) Expected Outcomes

Cryptographic technologies adopted for identity authentication, security updates, network communications, data storage and secure boot comply with national cryptography administration regulations.

c) Judgment Criterion

Test results consistent with all expected outcomes = Compliant; all other cases = Non-compliant.

B.1.3 Data Security & Personal Information Protection

B.1.3.1 Data Security

a) Test Procedures

Refer to product user manuals and management terminal operation guides to confirm whether the provider and operation path of the information erasure function are clearly marked; check whether an entry for the information erasure function exists on the product local interface or management terminal. Use professional data recovery tools to attempt recovery of data after erasure to verify whether identifiable original data remains.

b) Expected Outcomes

The product provides users with an information erasure function complying with GB 46864-2025, supporting simple and convenient data deletion from the device.

c) Judgment Criterion

Test results consistent with all expected outcomes = Compliant; all other cases = Non-compliant.

B.1.3.2 Personal Information Protection

a) Test Procedures

1. Check product management interfaces, user manuals and outer packaging boxes to confirm whether access entries or clear links for personal information processing rules are provided, and whether online review, text copying or download functions are supported; verify whether the content of processing rules complies with Clause 5.3.2 a).
2. Review the personal information collection workflow of the product to check categories of collected personal information; verify the revocability of user consent, and check whether the product silently collects personal information via background hidden channels without user consent.
3. Review personal information processing rules and privacy policy documents to verify the rationality of storage duration, security of storage methods, compliance of cross-border storage, and

compliance of transmission and storage of sensitive personal information.
4. Check whether the product performs associative analysis of individual identities captured in images and videos without separate user consent (excluding statutory scenarios).
5. Review personal information processing rules to verify whether processing of sensitive personal information complies with Chapter 5 and Clause 6.1 of GB/T 45574-2025.

b) Expected Outcomes
1. The product provides accessible personal information processing rules complying with Clause 5.3.2 a).
2. Personal information collection complies with Clauses 5.2 and 5.4 of GB/T 35273-2020.
3. Personal information storage complies with Clauses 6.1 and 6.3 of GB/T 35273-2020.
4. The product does not perform associative analysis of individual identities captured in images and videos without separate user consent.
5. Processing of sensitive personal information complies with Chapter 5 and Clause 6.1 of GB/T 45574-2025.

c) Judgment Criterion
Test results consistent with all expected outcomes = Compliant; all other cases = Non-compliant.

B.1.4 Security Assurance

B.1.4.1 Vulnerability Management

a) Test Procedures
1. Scan all vulnerabilities of the product to check whether high-risk or higher-severity vulnerabilities recorded in national vulnerability databases including CNVD, CNNVD and NVDB exist.
2. Check whether manufacturers explicitly disclose and publicize device model information; verify whether continuous security updates are provided within timeframes specified by regulations or agreed by parties; check whether tracking and emergency response mechanisms for product security defects and vulnerabilities are established and implemented to address defects and vulnerabilities identified during operation and maintenance.
3. Review manufacturer management systems and relevant documents to verify whether tracking and emergency response mechanisms for hardware, software and component security defects and vulnerabilities are established and implemented to address defects and vulnerabilities identified during operation and maintenance.
4. Review manufacturer management systems and relevant documents to verify whether manufacturers submit vulnerability information in accordance with the *Regulations on Administration of Cybersecurity Vulnerabilities of Network Products* upon discovery of device security defects or vulnerabilities, and promptly notify users of relevant security risks.

b) Expected Outcomes
1. The product contains no high-risk or higher-severity vulnerabilities recorded in national vulnerability databases including CNVD, CNNVD and NVDB.
2. Manufacturers explicitly disclose and publicize device model information, continuously provide security updates, establish and implement tracking and emergency response mechanisms for product security defects and vulnerabilities to address defects and vulnerabilities identified during operation and maintenance.
3. Manufacturers establish and implement tracking and emergency response mechanisms for hardware, software and component security defects and vulnerabilities to address defects and vulnerabilities identified during operation and maintenance.
4. Upon discovery of device security defects or vulnerabilities, manufacturers submit vulnerability information in accordance with the *Regulations on Administration of Cybersecurity Vulnerabilities of Network Products*, and promptly notify users of relevant security risks.

c) Judgment Criterion
Test results consistent with all expected outcomes = Compliant; all other cases = Non-compliant.

B.2 Enhanced Tier Evaluation

B.2.1 Physical & Hardware Security

B.2.1.1 Device Identification & Information

In addition to complying with the test procedures specified in B.1.1.1, the following test procedures, expected outcomes and judgment criteria shall also apply:

a) Test Procedures

Check whether protective measures against tampering of unique identifiers are deployed; review product design documentation to confirm the storage location and anti-tampering mechanisms of the unique device identifier.

b) Expected Outcomes

The product deploys protective measures to prevent tampering of the unique device identifier.

c) Judgment Criterion

Test results consistent with the expected outcome = Compliant; all other cases = Non-compliant.

B.2.1.2 Physical Interface Security

a) Test Procedures

1. Sort out functions and correlations of all physical interfaces and debugging interfaces of the product; verify whether all non-essential physical interfaces and debugging interfaces are disabled at factory delivery.
2. Log into the device management interface to check whether the product provides users with a function to disable debugging interfaces, and verify whether documentation explaining all physical interfaces is provided.

b) Expected Outcomes

1. All non-essential physical interfaces and debugging interfaces are disabled at factory delivery.
2. The product provides users with a function to disable debugging interfaces and complete documentation explaining all physical interfaces.

c) Judgment Criterion

Test results consistent with all expected outcomes = Compliant; all other cases = Non-compliant.

B.2.1.3 Secure Boot

a) Test Procedures

Check whether the product verifies the authenticity and integrity of firmware and boot components; verify whether the secure boot mechanism permits normal startup only after passing validation.

b) Expected Outcomes

The product implements a secure boot mechanism that verifies the authenticity and integrity of device firmware and boot components before normal startup is permitted.

c) Judgment Criterion

Test results consistent with the expected outcome = Compliant; all other cases = Non-compliant.

B.2.2 System & Software Security

B.2.2.1 Passphrase Security

Shall comply with the test procedures specified in B.1.2.1.

B.2.2.2 Identity Authentication

In addition to complying with the test procedures specified in B.1.2.2, the following test procedures, expected outcomes and judgment criteria shall also apply:

a) Test Procedures

1. Review device design documentation; attempt login via all physical interfaces to verify whether identity authentication is enforced for all accessing subjects.
2. Log into the system and attempt critical operations including modifying cybersecurity configurations and accessing sensitive personal information to verify whether an authentication factor separate from device login credentials is required, or security validation of the operating environment is enforced, including device login verification, network environment validation, operation behavior validation and other methods.

b) Expected Outcomes

1. Identity authentication is enforced for all accessing subjects logging in via physical device interfaces.
2. Critical operations including modifying cybersecurity configurations and accessing sensitive personal information require an authentication factor separate from device login credentials, or

security validation of the operating environment, including device login verification, network environment validation, operation behavior validation and other methods.

c) Judgment Criterion

Test results consistent with all expected outcomes = Compliant; all other cases = Non-compliant.

B.2.2.3 Critical Security Parameter Protection

In addition to complying with the test procedures specified in B.1.2.3, the following test procedures, expected outcomes and judgment criteria shall also apply:

a) Test Procedures

1. Review product design documentation to check whether cryptographic technologies are adopted to protect critical security parameters.
2. Review product design documentation to check whether standardized management workflows for critical security parameters are established, including key generation, key configuration, key usage, key storage, key revocation and key destruction.
3. Review product design documentation to verify whether core critical security parameters are unique for each individual device, including device root keys, keys ensuring authenticity and integrity of security updates, and keys ensuring confidentiality and integrity of network communications.

b) Expected Outcomes

1. The product adopts cryptographic technologies to protect critical security parameters.
2. Standardized management workflows for critical security parameters are established.
3. Core critical security parameters are unique for each individual device, including device root keys, keys ensuring authenticity and integrity of security updates, and keys ensuring confidentiality and integrity of network communications.

c) Judgment Criterion

Test results consistent with all expected outcomes = Compliant; all other cases = Non-compliant.

B.2.2.4 Cryptography Application

Shall comply with the test procedures specified in B.1.2.4.

B.2.2.5 Access Control

a) Test Procedures

1. For products supporting device binding functions:

(1) Review product design documentation to verify whether interactive confirmation between users and the device is required during binding.

(2) Verify whether the product only accepts control instructions originating from the bound account or its authorized sub-accounts after successful binding.

(3) Verify whether the product rejects binding requests from other accounts after successful binding unless the original bound user actively performs unbinding operations.

2. For products supporting authorization functions:

(1) Review product design documentation to check whether access control policies adhere to the principle of least privilege; attempt to access controlled resources and core functions with non-administrator accounts to verify access blocking.

(2) Attempt to access the permission sharing function with non-administrator accounts to verify access blocking.

(3) Review product design documentation to check whether protective measures for secure permission sharing are deployed.

b) Expected Outcomes

1. For products supporting device binding functions:

(1) Interactive confirmation between users and the device is required during binding.

(2) After successful binding, the product only accepts control instructions originating from the bound account or its authorized sub-accounts.

(3) After successful binding, the product rejects binding requests from other accounts unless the original bound user actively performs unbinding operations.

2. For products supporting authorization functions:

(1) Access control policies adhere to the principle of least privilege; non-administrator users are denied access to controlled resources and core functions by default.
(2) Only device administrators possess access to the permission sharing function; ordinary users cannot access this function.
(3) Protective measures for secure permission sharing are deployed on the product.
c) Judgment Criterion
Test results consistent with all expected outcomes = Compliant; all other cases = Non-compliant.

B.2.2.6 Log Audit

a) Test Procedures

1. Inspect product logs to verify whether events including power on/off, user creation, configuration modification, software installation/uninstallation, software upgrades, passphrase changes, failed login attempts and privileged user logins are recorded; verify whether audit records include event type, timestamp, triggering subject and event processing result.
2. Review design documentation to check log protection mechanisms; attempt unauthorized modification and deletion of logs to verify whether access control and protective mechanisms block such operations.
3. Inspect product logs to verify whether log storage overflow protection mechanisms are deployed to ensure continuous recording of the latest events after storage capacity thresholds are reached.
4. Check whether audit logs are stored on non-volatile storage media.

b) Expected Outcomes

1. The product records audit logs for events including power on/off, user creation, configuration modification, software installation/uninstallation, software upgrades, passphrase changes, failed login attempts and privileged user logins; audit records include event type, timestamp, triggering subject and event processing result.
2. The product deploys access control and protective mechanisms for audit logs to prevent unauthorized access, tampering and destruction of logs.
3. The product deploys log storage overflow protection mechanisms to ensure continuous recording of the latest events after storage capacity thresholds are reached.
4. Audit logs are stored on non-volatile storage media.

c) Judgment Criterion
Test results consistent with all expected outcomes = Compliant; all other cases = Non-compliant.

B.2.2.7 Firmware Security

a) Test Procedures

1. Review developer documentation to check whether authenticity and integrity validation mechanisms for firmware upgrade packages are described; perform upgrade tests with valid and tampered firmware packages to verify whether authenticity and integrity validation is enforced before upgrade execution.
2. Review product user documentation to check whether automatic and manual update functions are supported, and whether interrupted updates can be resumed.
3. Review product user documentation to check whether anti-rollback validation mechanisms are deployed; attempt unauthorized downgrade to low-version firmware to verify blocking.
4. Review product user documentation to check whether the product prompts users to perform security updates upon initial use or factory reset.

b) Expected Outcomes

1. Firmware upgrades implement security validation mechanisms to verify the authenticity and integrity of firmware packages.
2. The product supports automatic and manual security updates, and interrupted updates can be resumed.
3. Anti-rollback validation mechanisms are deployed to block unauthorized downgrade to low-version firmware.
4. The product prompts users to check and apply security updates upon initial use or factory reset.

c) Judgment Criterion
Test results consistent with all expected outcomes = Compliant; all other cases = Non-compliant.

B.2.2.8 Input Validation

a) Test Procedures

Review product design documentation to check whether security validation measures are deployed for data inputs submitted via user interfaces and APIs; submit illegal characters in user interface input boxes to verify whether the system intercepts invalid input and blocks transmission of invalid data to backend modules.

b) Expected Outcomes

Security validation measures are deployed for data inputs submitted via user interfaces and APIs, and the system intercepts all illegal input data.

c) Judgment Criterion

Test results consistent with the expected outcome = Compliant; all other cases = Non-compliant.

B.2.2.9 Secure Configuration

a) Test Procedures

Check product management interfaces and control application interfaces to verify whether the product provides a complete list of configuration items with secure default settings, and all network services and ports are minimized by default; review configuration workflows to check whether secure setting guidance is provided to users.

b) Expected Outcomes

The product ships with secure default configurations, and provides users with guidance on secure setting configuration.

c) Judgment Criterion

Test results consistent with the expected outcome = Compliant; all other cases = Non-compliant.

B.2.3 Network & Communication Security

B.2.3.1 Network Ports

a) Test Procedures

1. Check whether the product user manual clearly lists all non-essential network interfaces; use port scanning tools to identify default open ports of the product, cross-verify against manual descriptions to check whether network port exposure follows the minimization principle and all non-mandatory ports are disabled by default.
2. Check whether the product minimizes exposed port information when in an unauthenticated state.
3. Verify whether users can manually disable non-essential network services.
4. Log into the device management interface and review product documentation to verify whether complete descriptions of all network ports and corresponding services are provided.

b) Expected Outcomes

1. Network services and port exposure follow the minimization principle; all non-mandatory network services and ports are disabled by default.
2. The product minimizes exposed port information when in an unauthenticated state.
3. Users can manually disable non-essential network services.
4. Complete documentation explaining all network ports and corresponding services is provided.

c) Judgment Criterion

Test results consistent with all expected outcomes = Compliant; all other cases = Non-compliant.

B.2.3.2 Communication Security

a) Test Procedures

1. Use network packet capture tools to check whether encryption technologies are adopted for data transmission between the device and management terminals/servers.
2. Replay captured transmission data to verify whether the product can resist replay attacks.

b) Expected Outcomes

1. Encryption technologies are adopted to protect the authenticity, confidentiality and integrity of data transmission.
2. The product implements countermeasures against replay attacks.

c) Judgment Criterion

Test results consistent with all expected outcomes = Compliant; all other cases = Non-compliant.

B.2.4 Data Security & Personal Information Protection

B.2.4.1 Data Security

In addition to complying with the test procedures specified in B.1.3.1, the following test procedures, expected outcomes and judgment criteria shall also apply:

a) Test Procedures

1. Review product user manuals and management operation guides to confirm trigger conditions, notification methods and user consent workflows for fault diagnosis log uploads; simulate device fault scenarios to verify notification and consent workflows, check completeness of notification content and visibility of notification channels, and validate effectiveness of user consent mechanisms.
2. Verify whether the product provides a switch to disable user data upload functions, and confirm the switch can fully disable data uploads after activation.
3. Review product security design documentation and whitepapers to confirm specific security measures protecting confidentiality and integrity of user data; use packet capture tools to verify encryption of transmission data.

b) Expected Outcomes

1. The product clearly informs users of data collection methods, scope and purposes before uploading fault diagnosis logs, and uploads logs only after obtaining explicit user consent; notification content is complete and notification channels are prominent.
2. The product provides a switch to disable user data upload functions, which can fully block data uploads after activation.
3. Encryption and other security measures are deployed to protect the confidentiality and integrity of user data.

c) Judgment Criterion

Test results consistent with all expected outcomes = Compliant; all other cases = Non-compliant.

B.2.4.2 Personal Information Protection

In addition to complying with the test procedures specified in B.1.3.2, the following test procedures, expected outcomes and judgment criteria shall also apply:

a) Test Procedures

1. Review personal information processing rules to verify whether purposes, methods, categories of shared personal information and recipient entities are listed in a clear inventory.
2. Verify whether convenient channels (setting pages, customer service entries and others) are provided via management terminals for users to exercise personal information rights, and no unreasonable restrictions are imposed on legitimate user requests.

b) Expected Outcomes

1. All content related to provision of personal information to third parties is listed in a clear inventory within personal information processing rules.
2. Convenient channels are provided via management terminals for users to exercise personal information rights, with no unreasonable restrictions on legitimate user requests.

c) Judgment Criterion

Test results consistent with all expected outcomes = Compliant; all other cases = Non-compliant.

B.2.5 Security Assurance

B.2.5.1 Vulnerability Management

Shall comply with the test procedures specified in B.1.4.1.

B.3 Leading Tier Evaluation

B.3.1 Physical & Hardware Security

B.3.1.1 Device Identification & Information

Shall comply with the test procedures specified in B.2.1.1.

B.3.1.2 Physical Interface Security
Shall comply with the test procedures specified in B.2.1.2.

B.3.1.3 Secure Boot
Shall comply with the test procedures specified in B.2.1.3.

B.3.2 System & Software Security
B.3.2.1 Passphrase Security
Shall comply with the test procedures specified in B.2.2.1.

B.3.2.2 Identity Authentication
In addition to complying with the test procedures specified in B.2.2.2, the following test procedures, expected outcomes and judgment criteria shall also apply:
a) Test Procedures
Log into the system and attempt critical operations including modifying cybersecurity configurations and accessing sensitive personal information to verify whether an authentication factor separate from device login credentials is required, or security validation of the operating environment is enforced, including device login verification, network environment validation, operation behavior validation and other methods.
b) Expected Outcomes
Critical operations including modifying cybersecurity configurations and accessing sensitive personal information require an authentication factor separate from device login credentials, or security validation of the operating environment, including device login verification, network environment validation, operation behavior validation and other methods.
c) Judgment Criterion
Test results consistent with the expected outcome = Compliant; all other cases = Non-compliant.

B.3.2.3 Critical Security Parameter Protection
In addition to complying with the test procedures specified in B.2.2.3, the following test procedures, expected outcomes and judgment criteria shall also apply:
a) Test Procedures
Review product user documentation to check whether hardware security modules such as secure chips are adopted for key storage and usage.
b) Expected Outcomes
Hardware-based protection mechanisms including secure chips are adopted to store and use device root keys.
c) Judgment Criterion
Test results consistent with the expected outcome = Compliant; all other cases = Non-compliant.

B.3.2.4 Cryptography Application
Shall comply with the test procedures specified in B.2.2.4.

B.3.2.5 Access Control
Shall comply with the test procedures specified in B.2.2.5.

B.3.2.6 Log Audit
In addition to complying with the test procedures specified in B.2.2.6, the following test procedures, expected outcomes and judgment criteria shall also apply:
a) Test Procedures
For devices deployed via cloud network platforms, check whether audit logs are retained for a minimum of 180 consecutive days.
b) Expected Outcomes
For devices deployed via cloud network platforms, audit logs are retained for a minimum of 180 consecutive days.

c) Judgment Criterion
Test results consistent with the expected outcome = Compliant; all other cases = Non-compliant.

B.3.2.7 Firmware Security
Shall comply with the test procedures specified in B.2.2.7.

B.3.2.8 Input Validation
Shall comply with the test procedures specified in B.2.2.8.

B.3.2.9 Secure Configuration
Shall comply with the test procedures specified in B.2.2.9.

B.3.3 Network & Communication Security
B.3.3.1 Network Ports
Shall comply with the test procedures specified in B.2.3.1.

B.3.3.2 Communication Security
Shall comply with the test procedures specified in B.2.3.2.

B.3.4 Data Security & Personal Information Protection
B.3.4.1 Data Security
Shall comply with the test procedures specified in B.2.4.1.

B.3.4.2 Personal Information Protection
In addition to complying with the test procedures specified in B.2.4.2, the following recommended test procedures, expected outcomes and judgment criteria shall also apply:
a) Test Procedures
1. Review product documentation related to sensitive personal information processing to confirm whether the scope, methods and technical standards of sensitive personal information desensitization are clearly specified.
2. Verify whether at least one desensitization method is specified in product documentation, and supplementary desensitization methods and detailed implementation specifications are provided.
3. Perform actual operation tests on the camera under normal shooting scenarios to check whether real-time desensitization processing is applied to sensitive personal information in preview and recorded video streams.
4. Inspect video storage files and transmission data to verify whether desensitization status is maintained throughout storage and transmission without desensitization failure or leakage of sensitive personal information.
5. Review technical parameter documentation and test records of desensitization mechanisms to verify the stability and effectiveness of desensitization technologies, with no obvious vulnerabilities.
6. Verify whether the product supports adjustment of desensitization parameters, and desensitization effects remain compliant after parameter modification.

b) Expected Outcomes
1. Manufacturers formulate complete documentation for sensitive personal information desensitization, clearly specifying desensitization scope, methods and technical standards covering full links of shooting, preview, storage and transmission.
2. At least one desensitization method is deployed, with reasonable and operable supplementary desensitization solutions.
3. The product performs real-time desensitization processing on sensitive personal information captured in shooting scenarios, such that sensitive personal information cannot be identified in preview and recorded video streams.
4. Desensitization status remains stable throughout storage and transmission of video data, with no desensitization failure or leakage of sensitive personal information.
5. Desensitization technologies are stable and effective, with complete test records proving

sustainable and reliable desensitization performance with no obvious vulnerabilities.

6. The product supports reasonable adjustment of desensitization parameters, and desensitization effects remain compliant after parameter modification.

c) Judgment Criterion

Test results consistent with all expected outcomes = Compliant; all other cases = Non-compliant.

B.3.5 Security Assurance

B.3.5.1 Vulnerability Management

Shall comply with the test procedures specified in B.2.5.1.

B.3.5.2 Product Lifecycle Management

a) Test Procedures

1. Review product management documentation to confirm whether a full-lifecycle cybersecurity management mechanism covering design, development, testing, delivery and operation & maintenance phases is established.
2. Review security design documentation to verify whether threat modeling is performed in accordance with Clause 5.1.2.1 of GB/T 39276-2020, including threat identification, analysis and mitigation measures.
3. Review secure development documentation to verify whether mechanisms and workflows ensuring confidentiality and integrity of data storage and transmission during device design and development are described in full.
4. Review secure development mechanism documentation to verify compliance with Clause 5.1.2.1 of GB/T 39276-2020.
5. Review security testing mechanism documentation and test records to verify whether periodic security testing or pre-major-release security testing is performed, including static security testing, dynamic security testing, API testing, fuzz testing, code review and other test types.
6. Review secure delivery mechanism documentation and delivery records to verify whether security review and hardening are performed prior to product shipment and major version releases.
7. Review security operation and maintenance workflow documentation to verify compliance with Clause 5.2.2.3 of GB/T 39276-2020.

b) Expected Outcomes

1. Manufacturers establish a full-lifecycle cybersecurity management mechanism covering design, development, testing, delivery and operation & maintenance phases.
2. Manufacturers establish product security design workflows and conduct threat modeling in accordance with Clause 5.1.2.1 of GB/T 39276-2020 to identify, analyze and mitigate device security threats.
3. Manufacturers compile secure development documentation fully describing mechanisms and workflows ensuring confidentiality and integrity of data storage and transmission during device design and development.
4. Manufacturers establish secure product development workflows complying with Clause 5.1.2.1 of GB/T 39276-2020.
5. Manufacturers establish standardized security testing workflows, conducting periodic security testing or pre-major-release security testing including static security testing, dynamic security testing, API testing, fuzz testing, code review and other test types.
6. Manufacturers establish secure delivery workflows, implementing security review and hardening prior to product shipment and major version releases.
7. Manufacturers establish security operation and maintenance workflows complying with Clause 5.2.2.3 of GB/T 39276-2020.

c) Judgment Criterion

Test results consistent with all expected outcomes = Compliant; all other cases = Non-compliant.

B.3.5.3 Code Inspection

a) Test Procedures

1. Conduct code inspection or review third-party code inspection reports issued by qualified testing institutions; inspection targets include source code or binary programs, covering software

vulnerabilities and errors, vulnerabilities embedded in third-party libraries and components, and hardcoded identity authentication credentials and critical security parameters. Verify testing institutions hold valid corresponding qualifications and test workflows comply with specifications.

2. Check whether dedicated mobile applications are deployed for device management; if yes, conduct inspection of management applications or review third-party inspection reports, covering hardcoded critical security parameters, plaintext storage/transmission of critical security parameters and sensitive personal information, and unauthorized collection of sensitive personal information. Verify testing institutions hold valid corresponding qualifications.
3. Review inspection reports to verify completeness of test records, raw data and test conclusions; confirm no omission of test items, scientific and reasonable test methodologies, and authentic and valid test results.

b) Expected Outcomes

1. Manufacturers commission qualified third-party institutions to conduct full device code inspection covering software vulnerabilities and errors, vulnerabilities embedded in third-party libraries and components, and hardcoded identity authentication credentials and critical security parameters; inspection conclusions confirm no medium-risk or higher-severity vulnerabilities.
2. Where dedicated mobile applications are deployed for device management, manufacturers commission qualified third-party institutions to inspect the management application, covering hardcoded critical security parameters, plaintext storage/transmission of critical security parameters and sensitive personal information, and unauthorized collection of sensitive personal information; all identified non-compliant items are fully rectified.
3. Inspection reports are complete and standardized, containing qualification certificates, test workflows, test items, raw test data and formal test conclusions, with test procedures fully compliant with relevant standard specifications.

c) Judgment Criterion

Test results consistent with all expected outcomes = Compliant; all other cases = Non-compliant.

Annex C (Normative) Competency Requirements for Third-Party Testing Institutions

C.1 Institutional Requirements

Third-party testing institutions shall hold CNAS and CMA accreditations, with recognized accreditation scopes covering cybersecurity testing services.

C.2 Personnel Requirements

Third-party testing institutions undertaking penetration testing shall employ a minimum of five full-time penetration testing specialists, each satisfying at least one of the following criteria:

a) Possession of penetration testing professional certifications including CISP-PTE, CISP-PTS and other equivalent certificates;

b) Documented project experience delivering penetration testing services;

c) Record of legally discovered security vulnerabilities submitted to national authoritative vulnerability databases within the preceding five years;

d) Award recipient at national or provincial-level cybersecurity competitions.

Introduction of SESEC Project

The Seconded European Standardization Expert in China (SESEC) is a visibility project co-financed by the European Commission (EC), the European Free Trade Association (EFTA) secretariat and the three European Standardization organizations (CEN, CENELEC and ETSI). Since 2006, there has been four SESEC projects in China, SESEC I (2006-2009). SESEC II (2009- 2012), SESEC III (2014-2017), SESEC IV (2018- 2022) and SESEC V (2022-2025). Dr. Betty XU is nominated as the SESEC expert and will spend the next 36 months on promoting EU-China standardization information exchange and EU-China standardization cooperation.

The SESEC project supports the strategic objectives of the European Union, EFTA and the European Standardization organizations (ESOs). The purpose of SESEC project is to:

- **Promote European and international standards in China;**
- **Improve contacts with different levels of the Chinese administration, industry and standardization bodies;**
- **Improve the visibility and understanding of the European Standardization System (ESS) in China;**
- **Gather regulatory and standardization intelligence.**

The following areas have been identified as sectoral project priorities by the SESEC project partners: Internet of Things (IoT) & Machine-to-Machine(M2M) communication, communication networks & services, cybersecurity & digital identity, Smart Cities (including transport, power grids & metering), electrical & electronic products, general product safety, medical devices, cosmetics, energy management & environmental protection (including eco-design & labeling, as well as environmental performance of buildings).