附件 2

网络安全标识 消费类网联摄像头安全要求

1 范围

本文件规定了消费类网联摄像头的安全技术要求和安全保障要求，规定了基础级、增强级、领先级三个等级的安全能力要求。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB 46864—2025 数据安全技术 电子产品信息清除技术要求

GB/T 25069—2022 信息安全技术 术语

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 38674—2020 信息安全技术 应用软件安全编程指南

GB/T 39276—2020 信息安全技术 网络产品和服务安全通用要求

GB/T 45574—2025 数据安全技术 敏感个人信息处理安全要求

3 术语和定义

3.1

消费类网联摄像头 consumer connected camera

消费者个人或组织购买、使用，为个人或组织提供音视频信息采集和处理服务、具有互联网联网功能的独立摄像头。

注：不适用于公共安全领域的摄像头。

3.2

关键安全参数 critical security parameter；CSP

与安全有关，其泄露或修改会危及密码模块安全的信息。

示例：秘密和私有密码密钥、口令之类的鉴别数据、个人标识码（PIN）、证书或其他信任锚。

注：消费类网联摄像头中重点保护的关键安全参数包括设备根密钥、用户身份鉴别信息、设备鉴别信息、保证安全更新真实性和完整性的密钥、保证网络通信机密性和完整性的密钥。

[来源：GB/T 25069—2022，有修改]

3.3

固件 firmware

功能上独立于主存储器，通常存储在只读存储器（ROM）中的指令和相关数据的有序集。

[来源：GB/T 25069—2022]

3.4

设备绑定　device binding

建立用户账号与消费类网联摄像头设备间唯一权属关系的过程。

3.5

***硬编码*　hardcode**

在编码过程中将可变变量用一个固定数值表示。

[来源：GB/T 38674—2020]

4　概述

本文件从物理与硬件安全、系统与软件安全、网络与通信安全、数据安全与个人信息保护和安全保障5个方面构建消费类网联摄像头安全框架（见图1）。

消费类网联摄像头安全能力划分为三级，从基础级、增强级、领先级逐级提升。基础级要求产品网络安全能力达到基本的网络安全水平，增强级要求产品网络安全能力达到同类产品先进水平，领先级要求产品网络安全能力达到同类产品领先水平。满足同一等级的所有单项要求，方可获得该网络安全能力等级。各安全能力等级的产品应符合的安全要求见附录A，测试评价方法参考附录B。

开展基础级、增强级产品检测的第三方检测机构应满足附录 C.1 的要求；开展领先级产品检测的第三方检测机构应满足附录 C.1、C.2 的要求。

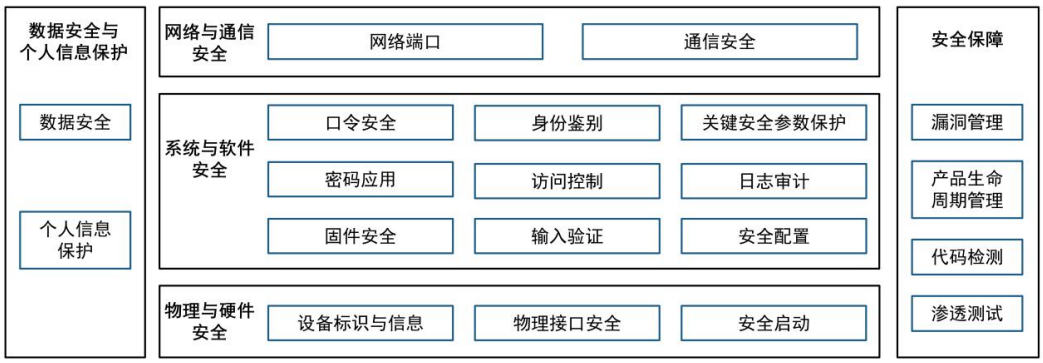

图1 消费类网联摄像头安全框架

5 基础级要求

5.1 物理与硬件安全

5.1.1 设备标识与信息

消费类网联摄像头应满足如下要求:

a）具有唯一设备标识;

注：设备标识指用于识别或验证设备身份合法性的唯一标识符号。

b）在设备外观清晰标识出设备型号、设备名称等信息。

5.2 系统与软件安全

5.2.1 口令安全

消费类网联摄像头应满足如下要求:

a）使用口令进行身份鉴别的，禁止使用弱口令，口令不应少于8个字符，至少包含数字、小写字母、大写字母以及特殊字符中的2类字符;

注：包括但不限于初始随机口令、用户初始设置的口令、用户激活设备时配置的口令、用户使用设备过程中设置或修改的口令。

b）出厂配置时采用初始口令登录设备的，每台设备的初始口令应为唯一随机生成，不得使用固定或通用默认口令，复杂度应符合5.2.1a）的要求;

c）出厂配置时采用激活机制的，在设备完成激活前拒绝激活以外的其他操作。通过用户设置口令进行设备激活的，要求用户设置复杂度符合5.2.1a）要求的口令;

注：激活指设备第一次使用时由用户采取相关操作才能使用设备的机制，包括设置口令、扫描二维码等。

d）具备口令防暴力破解功能，对错误登录尝试超过设定次数后采取保护措施;

注：如锁定账号、锁定IP、登录延时、验证码登录等方式，错误登录尝试次数宜为10次以下。

e）在忘记账号或者口令的情况下，通过物理按键或其他安全方式将设备恢复到出厂设置状态。

5.2.2 身份鉴别

消费类网联摄像头应满足如下要求:

a）对用户身份进行唯一标识，并采取防护措施防止标识被篡改;

b）不存在未公开的账号和登录方式;

注：未公开的账号包括但不限于测试账号、运维账号、第三方软件中不使用的账号。

c）通过网络登录设备，对访问主体进行身份鉴别;

注：登录设备方式包括但不限于网络端口、WEB 管理界面、管理应用程序等。

d）使用数字证书进行身份鉴别的，设备的数字证书应和设备标识绑定。

5.2.3 关键安全参数保护

消费类网联摄像头应满足如下要求:

a）使用密码技术保护身份鉴别信息的机密性;

b）不在设备软件代码中硬编码关键安全参数。

5.2.4 密码应用

消费类网联摄像头中用于身份鉴别、安全更新、网络通信、数据存储、安全启动等场景的加密技术应符合国家密码管理相关规定。

5.3 数据安全与个人信息保护

5.3.1 数据安全

数据销毁应为用户提供符合 GB 46864—2025 要求的信息清除功能。

注：功能由产品或其管理端提供，用户自行使用。

5.3.2 个人信息保护

消费类网联摄像头应满足如下要求:

a）处理个人信息的，在产品管理相关界面、说明书等提供的链接页面公开展示个人信息处理规则，供用户查阅、复制或下载后查阅，规则内容包括但不限于:

1）个人信息处理者的名称和联系方式;

2）处理个人信息的种类和对应的处理目的、方式;

3）明确个人信息是否存储在境内，以及存储的期限和到期后的处理方式;

4）处理个人信息的必要性、对用户个人权益的影响和所采取安全措施的说明;

5）查阅、复制、转移、更正、补充、删除用户个人信息，以及注销账号、撤回同意的方法和途径。

b）个人信息收集符合 GB/T 35273—2020 中 5.2、5.4 的要求;

c）个人信息存储符合 GB/T 35273—2020 中 6.1、6.3 的要求;

d）未经用户同意，不对所收集图片、视频中个人的身份进行关联分析，履行法定义务和法律法规另有规定的除外;

e）处理用户敏感个人信息符合 GB/T 45574—2025 中第 5 章及 6.1 的要求。

5.4 安全保障

5.4.1 漏洞管理

消费类网联摄像头生产者应满足如下要求:

a）确保设备不存在已知的高危及以上等级的漏洞;

注：已知高危漏洞参考 CNVD、CNNVD、NVDB 等国家漏洞库。

b）应明确并公示设备的型号，在规定或当事人约定期限内，持续进行安全更新;

c）建立和执行产品的软硬件及相关组件的安全缺陷、漏洞的跟踪和应急响应机制，对产品在运行和维护阶段发现的安全缺陷、漏洞进行响应;

d）发现设备存在安全缺陷、漏洞时，按照《网络产品安全漏洞管理规定》报送相关漏洞信息，并及时告知用户安全风险。

6 增强级要求

6.1 物理与硬件安全

6.1.1 设备标识与信息

在满足 5.1.1 的要求的同时，还应满足如下要求：

采取防护措施保护唯一设备标识不被篡改。

6.1.2 物理接口安全

消费类网联摄像头应满足如下要求：

a）在出厂时关闭非必要物理接口和调试接口；

b）向用户提供调试接口关闭功能，并提供物理接口说明文档。

6.1.3 安全启动

消费类网联摄像头应实现安全启动机制，对设备固件和启动组件的真实性和完整性进行校验通过后方可正常启动。

6.2 系统与软件安全

6.2.1 口令安全

应满足 5.2.1 的要求。

6.2.2 身份鉴别

在满足 5.2.2 的要求的同时，还需满足如下要求:

a）通过物理接口登录设备，应对访问主体进行身份鉴别;

b）修改网络安全配置、访问敏感个人信息等重要操作，宜使用与设备登录不同的因子进行认证，或对操作环境进行安全校验。

注：安全校验方式包括但不限于登录设备校验、网络环境、操作行为。

6.2.3 关键安全参数保护

在满足 5.2.3 的要求的同时，还应满足如下要求：

a）采用密码技术对关键安全参数进行机密性和完整性保护；

b）建立规范的关键安全参数的安全管理流程；

注 1：管理对象包括但不限于根密钥，以及用于通信安全保护、安全更新保护、敏感个人信息保护的关键安全参数。

注 2：管理流程包括但不限于密钥生成、密钥配置、密钥使用、密钥存储、密钥吊销、密钥销毁等。

c）保证设备重要的关键安全参数对每个设备是唯一的。

注：设备重要的关键安全参数包括但不限于设备根密钥、保证安全更新真实性和完整性的密钥、保证网络通信机密性和完整性的密钥。

6.2.4 密码应用

应满足 5.2.4 的要求。

6.2.5 访问控制

消费类网联摄像头应满足如下要求：

a）具有设备绑定功能的：

1）在用户绑定设备时，与设备进行交互确认；

注：交互方式包括但不限于按键、蓝牙或无线网络配对、声波、二维码等，防止非设备所属用户绑定。

2）已完成设备绑定的，仅接受来自绑定账号或其授权账号的控制指令;

3）已完成设备绑定的，不再接受其它账号绑定，除非原设备绑定用户主动解除绑定。

b）具有授权功能的:

1）设备访问控制策略应满足最小授权原则，默认不允许设备管理员以外的用户访问受控资源或使用关键功能;

注：仅允许设备管理员更改访问控制策略。

2）只能由设备管理员具备访问权限分享功能，其它用户不具备权限分享功能;

3）采取防护措施保障分享的安全性。

注：保障分享的安全性防护措施包括但不限于分享权限即时回收、设置被分享者查看权限，宜设置分享有效期、被分享者水印等措施。

6.2.6 日志审计

消费类网联摄像头应满足如下要求:

a）能对开关机、创建用户、更改配置、软件升级、修改口令、登录失败、特权用户登录等事件进行记录，

审计记录应包括事件类型、事件发生时间、触发事件的主体、事件处理结果等信息;

b）具备对日志记录的访问权限控制等保护机制，使其免遭非法访问、篡改及破坏;

c）具备审计日志存储保护机制，保障日志存储量超过阈值后审计日志正常记录最新事件;

d）日志保存于非易失性存储介质。

6.2.7 固件安全

消费类网联摄像头应满足如下要求:

a）固件升级具备安全校验机制，验证更新固件的真实性和完整性;

b）具备新的固件版本时，提示用户通过自动、人工方式进行安全更新，更新中止后能重新更新;

c）具备非授权固件版本防回退校验机制;

d）设备在第一次使用或恢复出厂设置后检查并提示进行安全更新。

6.2.8 输入验证

消费类网联摄像头应对通过用户界面输入、应用程序编程接口输入的数据进行安全验证，以避免数据处理过程中出现意外行为。

注: 数据处理过程中出现的意外行为包括但不限于SQL注入、操作系统命令注入和路径遍历等。

6.2.9 安全配置

消费类网联摄像头应默认提供安全的配置，并向用户提供安全设置的指导。

6.3 网络与通信安全

6.3.1 网络端口

消费类网联摄像头应满足如下要求:

a）网络服务和网络端口开放遵循最小化原则，默认关闭非必须使用的网络服务和网络端口;

b）未认证状态下减少网络端口暴露信息;

c）用户可关闭非必要的网络服务;

d）提供文档说明所有网络端口和服务。

6.3.2 通信安全

消费类网联摄像头应满足如下要求:

a）使用加密技术保护关键安全参数和敏感个人信息传输的真实性、机密性、完整性;

b）具有抵抗重放攻击的能力。

6.4 数据安全与个人信息保护

6.4.1 数据安全

在满足 5.3.1 的要求的同时，还应满足如下要求:

a）通过上传设备日志进行故障诊断时，明确告知用户数据采集方式、范围、目的，经用户同意后上传;

b）具备用户关闭上传用户数据的相关功能;

c）采取加密等安全措施保护用户数据的机密性和完整性。

6.4.2 个人信息保护

在满足 5.3.2 的要求的同时，还应满足如下要求:

a）个人信息处理规则中涉及收集和向其他个人信息处理者提供个人信息的目的、方式、种类以及接收方信息的，以清单等形式予以列明;

b）用户通过管理端交互界面等便捷通道行使个人信息权利的，不得设置不合理条件限制用户的合理请求。

6.5 安全保障

6.5.1 漏洞管理

应满足 5.4.1 的要求。

7 领先级要求

7.1 物理与硬件安全

7.1.1 设备标识与信息

应满足 6.1.1 的要求。

7.1.2 物理接口安全

应满足 6.1.2 的要求。

7.1.3 安全启动

应满足 6.1.3 的要求。

7.2 系统与软件安全

7.2.1 口令安全

应满足 6.2.1 的要求。

7.2.2 身份鉴别

在满足 6.2.2 的要求的同时，还应满足如下要求:

修改网络安全配置、访问敏感个人信息等重要操作，使用与设备登录不同的因子进行认证，或对操作环境进行安全校验。

注：安全校验方式包括但不限于登录设备校验、网络环境、操作行为。

7.2.3 关键安全参数保护

在满足 6.2.3 的要求的同时，还应满足如下要求:

采用硬件方式保护设备根密钥。

注：硬件方式包括但不限于使用安全芯片、芯片的安全存储区等。

7.2.4 密码应用

应满足 6.2.4 的要求。

7.2.5 访问控制

应满足 6.2.5 的要求。

7.2.6 日志审计

在满足 6.2.6 的要求的同时，还应满足如下要求:

通过网络平台部署的，审计日志记录的期限为 180 天及以上。

7.2.7 固件安全

应满足 6.2.7 的要求。

7.2.8 输入验证

应满足 6.2.8 的要求。

7.2.9 安全配置

应满足 6.2.9 的要求。

7.3 网络与通信安全

7.3.1 网络端口

应满足 6.3.1 的要求。

7.3.2 通信安全

应满足 6.3.2 的要求。

7.4 数据安全与个人信息保护

7.4.1 数据安全

应满足 6.4.1 的要求。

7.4.2 个人信息保护

在满足 6.4.2 的要求的同时，还宜满足如下要求:

对敏感个人信息进行脱敏。

注：对敏感个人信息进行脱敏的方式包括但不限于对敏感区域进行打码、使用安全视频编码等。

7.5 安全保障

7.5.1 漏洞管理

应满足 6.5.1 的要求。

7.5.2 产品生命周期管理

消费类网联摄像头生产者应满足如下要求:

a）建立产品全生命周期网络安全管理机制，覆盖设计、开发、测试、交付、运维等环节;

b）建立产品安全设计机制，参考 GB/T 39276—2020 第 5.1.2.1 项相关要求进行威胁建模，以识别、分析和缓解对设备的安全威胁;

c）编制开发安全文档，描述设备设计和开发过程中实现数据存储和传输的机密性和完整性的机制和流程;

d）建立产品安全开发机制，满足 GB/T 39276—2020 第 5.1.2.1 项相关要求;

e）建立安全测试机制，定期或在重要版本发布前进行安全测试，包括但不限于：静态安全测试、动态安全测试、API 测试、模糊测试、代码审查等;

f）建立安全交付机制，在产品交付和重要版本发布前进行安全审查和加固，包括但不限于:

1）删除非必要的账号、测试账号;

2）从发布的版本中删除所有调试代码;

3）禁用不必要的物理接口、网络服务、网络端口、网络接口;

4）启用摄像头终端侧操作系统的安全功能，包括身

份鉴别、访问控制、数据加密等功能。

g）建立安全运维机制和流程，满足 GB/T 39276—2020 第 5.2.2.3 项相关要求。

7.5.3 代码检测

消费类网联摄像头生产者应满足如下要求:

a）委托第三方检测机构针对设备自身代码进行检测，包括但不限于软件安全漏洞和错误、第三方库和第三方组件中的安全漏洞、硬编码身份鉴别信息和关键安全参数;

b）使用应用程序对设备进行管理的，委托第三方检测机构针对设备管理应用程序进行检测，包括但不限于硬编码关键安全参数、通过明文存储或传输关键安全参数和敏感个人信息、违规收集敏感个人信息。

7.5.4 渗透测试

消费类网联摄像头生产者应满足如下要求:

a）委托第三方检测机构开展网络安全渗透性测试，不存在中危及以上级别漏洞，并获得渗透测试报告;

b）通过网络安全众测方式进行网络安全众测，不存在中危及以上级别漏洞，并获得网络安全众测报告;

c）开展网络安全渗透性测试应满足如下要求:

1）测试时间不少于 14 天，参与人数不少于 5 人;

2）进行中间人攻击;

3）进行权限绕过;

4）进行内存攻击，包括但不限于缓冲区溢出等;

5）进行逆向攻击，验证是否泄露敏感信息;

6）提供 WEB 服务的，进行 SQL 注入、跨站脚本攻击等常见的 WEB 攻击。

d）开展网络安全众测应满足如下要求:

1）验证产品对抗漏洞利用的安全能力;

2）测试时间不少于 14 天，众测人数不少于 20 人，参与人员具备相关领域漏洞发掘能力，以及相关领域漏洞发掘项目经验。

附录 A

（规范性）

不同安全能力等级的产品应符合的安全要求

表A.1列出了消费类网联摄像头基础级、增强级和领先级应符合的安全要求。

表A.1 不同安全能力等级的产品应符合的安全要求

技术要求		基础级要求对应章条号	增强级要求对应章条号	领先级要求对应章条号
物理与硬件安全	设备标识与信息	5.1.1	6.1.1	7.1.1
	物理接口安全	—	6.1.2	7.1.2
	安全启动	—	6.1.3	7.1.3
系统与软件安全	口令安全	5.2.1	6.2.1	7.2.1
	身份鉴别	5.2.2	6.2.2	7.2.2
	关键安全参数保护	5.2.3	6.2.3	7.2.3
	密码应用	5.2.4	6.2.4	7.2.4
	访问控制	—	6.2.5	7.2.5

	日志审计	—	6.2.6	7.2.6
	固件安全	—	6.2.7	7.2.7
	输入验证	—	6.2.8	7.2.8
	安全配置	—	6.2.9	7.2.9
网络与通信安全	网络端口	—	6.3.1	7.3.1
	通信安全	—	6.3.2	7.3.2
数据安全与个人信息保护	数据安全	5.3.1	6.4.1	7.4.1
	个人信息保护	5.3.2	6.4.2	7.4.2
安全保障	漏洞管理	5.4.1	6.5.1	7.5.1
	产品生命周期管理	—	—	7.5.2
	代码检测	—	—	7.5.3
	渗透测试	—	—	7.5.4

附录 B

（资料性）

测试评价方法

B.1 基础级测评

B.1.1 物理与硬件安全

B.1.1.1 设备标识与信息

设备标识与信息的测评方法如下:

a）测试方法:

1）检查设备标识是否具有保证设备标识唯一性的说明；尝试通过管理界面、接口、平台等对设备标识进行修改;

2）检查设备外观的名称、型号等信息是否清晰；核查用户配置界面、管理 APP 等位置的相关信息是否与外观一致。

b）预期结果:

1）设备具有保证设备标识唯一性的说明;

2）设备外观清晰标识出设备的名称、型号等信息，并且与用户配置界面、管理 APP 等位置的信息一致；无法对唯一性标识进行修改。

c）结果判定:

实际测试结果与预期结果一致则判定为“符合”,其他情况判定为“不符合”。

B.1.2 系统与软件安全

B.1.2.1 口令安全

口令安全的测评方法如下:

a）测试方法:

1）对采用基于口令作为鉴别信息的系统，通过设置或修改账户口令，检验系统是否对设置的口令进行复杂度、长度检查，是否明示口令长度要求、复杂度要求，是否要求至少包含：数字、小写字母、大写字母、特殊字符中的 2 类，口令长度至少 8 位;

2）根据产品说明文档，查看出厂设备的初始口令。检查出厂设备的初始口令是否为唯一随机生成，是否使用固定或通用默认口令，复杂度是否符合 5.2.1a）的要求;

3）检查出厂配置时采用激活机制的产品，是否在设备完成激活前拒绝激活以外的其他操作，是否存在与激活无关的暴露面，如网络端口、物理接口等。通过用户设置口令进行设备激活的产品，是否要求用户设置复杂度符合 5.2.1a）要求的口令;

4）使用错误的口令连续登录设备，检查产品是否具

备口令防暴力破解功能，对错误登录尝试超过设定次数后是否采取保护措施，例如：锁定账号、锁定IP、登录延时、验证码登录等方式等;

5）根据产品说明文档，检查产品是否在忘记账号或者口令的情况下，通过物理按键或其他安全方式重新设置口令，或将设备恢复到出厂设置状态。

b）预期结果:

1）使用口令进行身份鉴别的产品，未使用弱口令，口令长度不少于8个字符，包含数字、小写字母、大写字母以及特殊字符中的2类字符;

2）出厂配置时采用初始口令登录的产品，每台设备的初始口令为唯一随机生成，未使用固定或通用默认口令，复杂度符合5.2.1a）的要求;

3）出厂配置时采用激活机制的产品，在完成激活前拒绝激活以外的其他操作，不存在与激活无关的暴露面，如网络端口、物理接口等。通过用户设置口令进行设备激活的产品，要求用户设置复杂度符合5.2.1a）要求的口令;

4）设备具备口令防暴力破解功能，对错误登录尝试超过设定次数后采取保护措施;

5）设备在忘记账号或者口令的情况下，通过物理按键或其他安全方式重新设置口令，或将设备恢复

到出厂设置状态。

c）结果判定:

实际测试结果与预期结果一致则判定为“符合”,其他情况判定为“不符合”。

B.1.2.2 身份鉴别

身份鉴别的测评方法如下:

a）测试方法:

1）检查唯一标识生成算法，分析是否存在防止标识被篡改的防护措施;

2）查阅产品说明文档，检查产品中是否存在未公开的账号和登录方式，账号包括但不限于测试账号、运维账号、第三方软件中不使用的账号，登录方式包括但不限于特殊组合键;

3）查阅产品说明文档,检查核对设备所有网络端口、WEB 管理界面、管理应用程序等网络登录方式,是否都需要身份鉴别;

4）使用数字证书进行身份鉴别的，查阅产品说明文档，设备的数字证书是否和设备标识绑定。

b）预期结果:

1）产品对用户身份进行唯一标识，并采取防护措施防止标识被篡改;

2）产品中不存在未公开的账号和登录方式，账号包

括但不限于测试账号、运维账号、第三方软件中不使用的账号，登录方式包括但不限于特殊组合键;

3）所有通过网络登录设备的方式，都对访问主体进行身份鉴别;

4）使用数字证书进行身份鉴别的，设备的数字证书和设备标识绑定。

c）结果判定:

实际测试结果与预期结果一致则判定为“符合”,其他情况判定为“不符合”。

B.1.2.3 关键安全参数保护

关键安全参数保护的测评方法如下:

a）测试方法:

1）检查是否采用了密码技术保障鉴别信息的保密性;

2）查看设备软件代码，检查代码中是否存在硬编码的关键安全参数。

b）预期结果:

1）产品使用了密码技术保护身份鉴别信息的机密性;

2）设备软件代码中不存在硬编码的关键安全参数。

c）结果判定:

实际测试结果与预期结果一致则判定为“符合”,其他情况判定为“不符合”。

B.1.2.4 密码应用

密码应用的测评方法如下:

a）测试方法:

查阅设备设计文档，确认身份鉴别、安全更新、网络通信、数据存储和安全启动等场景使用的加密技术是否符合国家密码管理相关规定。

b）预期结果:

身份鉴别、安全更新、网络通信、数据存储和安全启动等场景使用的加密技术符合国家密码管理相关规定。

c）结果判定:

实际测试结果与预期结果一致则判定为“符合”,其他情况判定为“不符合”。

B.1.3 数据安全与个人信息保护

B.1.3.1 数据安全

数据安全的测评方法如下:

a）测试方法:

查阅产品说明书、管理端操作指南等文档，确认是否明确标注信息清除功能的提供主体及操作路径，检查产品本地界面或管理端是否存在信息清除功能

入口，使用专业数据恢复工具对清除后的存储介质进行数据恢复尝试，验证是否残留可识别的原始数据。

b）预期结果:

产品的数据销毁为用户提供符合GB 46864—2025要求的信息清除功能，以简单便捷的方式从设备中删除数据。

c）结果判定:

实际测试结果与预期结果一致则判定为“符合”,其他情况判定为“不符合”。

B.1.3.2　个人信息保护

个人信息保护的测评方法如下:

a）测试方法:

1）检查产品管理相关界面、说明书、外包装盒等载体确认是否提供个人信息处理规则的访问入口或明确链接，验证是否提供在线查阅、复制文本或下载功能；核查处理规则内容是否符合5.3.2a）的要求;

2）审查产品的个人信息收集流程，核查收集的个人信息种类；验证同意的可撤回性，审查产品是否存在未经用户同意，通过隐蔽方式（如后台静默收集）获取个人信息的情况;

3）审查产品个人信息处理规则、隐私政策等文档，核查存储期限的合理性，检查存储方式的安全性，验证跨境存储合规性，敏感个人信息的传输和存储的合规性;

4）检查是否存在未经用户同意，对图片、视频中个人身份进行关联分析的情况（法定情形除外）;

5）审查产品个人信息处理规则，处理用户敏感个人信息是否符合 GB/T 45574—2025 中第 5 章及 6.1 的要求。

b）预期结果:

1）产品提供了个人信息处理规则并符合 5.3.2a）的要求;

2)产品个人信息收集符合 GB/T 35273—2020 中 5.2、5.4 的要求;

3)产品个人信息存储符合 GB/T 35273—2020 中 6.1、6.3 的要求;

4）设备不存在未经用户单独同意对所收集图片、视频中个人的身份进行关联分析行为;

5）处理用户敏感个人信息符合 GB/T 45574—2025 中第 5 章及 6.1 的要求。

c）结果判定:

实际测试结果与预期结果一致则判定为“符合”,其他

情况判为“不符合”。

B.1.4 安全保障

B.1.4.1 漏洞管理

漏洞管理的测评方法如下:

a）测试方法:

1）检查产品的所有漏洞，核查产品是否存在 CNVD、CNNVD、NVDB 等国家漏洞库已公布的高危及以上级别漏洞;

2）检查产品生产者是否明确并公示设备的型号，验证产品是否在规定或当事人约定期限内持续进行安全更新，核查产品是否建立和执行产品安全缺陷、漏洞的应急响应机制和流程，并对在运行和维护阶段发现的安全缺陷、漏洞进行响应;

3）检查产品生产者管理制度和相关文件，是否建立和执行产品的软硬件及相关组件的安全缺陷、漏洞的跟踪和应急响应机制，对产品在运行和维护阶段发现的安全缺陷、漏洞进行响应;

4）检查产品生产者管理制度和相关文件，是否在发现设备存在安全缺陷、漏洞时，按照《网络产品安全漏洞管理规定》报送相关漏洞信息，并及时告知用户安全风险。

b）预期结果:

1）产品不存在 CNVD、CNNVD、NVDB 等国家漏洞库已公布的高危及高危以上级别漏洞;

2）产品明确并公示设备的型号，持续进行安全更新，建立和执行产品安全缺陷、漏洞的应急响应机制和流程，对产品在运行和维护阶段发现的安全缺陷、漏洞进行响应;

3）建立和执行产品的软硬件及相关组件的安全缺陷、漏洞的跟踪和应急响应机制，对产品在运行和维护阶段发现的安全缺陷、漏洞进行响应;

4）发现设备存在安全缺陷、漏洞时，按照《网络产品安全漏洞管理规定》报送相关漏洞信息，并及时告知用户安全风险。

c）结果判定:

实际测试结果与预期结果一致则判定为“符合”,其他情况判定为“不符合”。

B.2 增强级测评

B.2.1 物理与硬件安全

B.2.1.1 设备标识与信息

在满足 B.1.1.1 的测评方法的同时,还应满足如下测试方法、预期结果和结果判定:

a）测试方法:

检查产品是否采取防护措施保护唯一标识不被篡

改，审查产品设计文档，确认唯一设备标识的存储位置及防篡改机制。

b）预期结果:

产品采取防护措施保护唯一标识不被篡改。

c）结果判定:

实际测试结果与预期结果一致则判定为“符合”,其他情况判定为“不符合”。

B.2.1.2 物理接口安全

物理接口安全的测评方法如下:

a）测试方法:

1）检查产品哪些物理接口与调试接口的功能和相关性，核查非相关的物理接口与调试接口出厂时是否全部关闭;

2）登录设备管理界面，检查产品是否向用户提供调试接口关闭功能，核查产品是否提供物理接口的说明文档。

b）预期结果:

1）产品在出厂时关闭非必要物理接口和调试接口;

2）产品能向用户提供调试接口的关闭功能和物理接口的说明文档。

c）结果判定:

实际测试结果与预期结果一致则判定为“符合”,其他

情况判定为“不符合”。

B.2.1.3 安全启动

安全启动的测评方法如下:

a）测试方法:

检查产品是否对固件和启动组件的真实性和完整性进行校验；核查校验后产品的安全启动机制能否正常启动。

b）预期结果:

产品实现安全启动机制，对设备固件和启动组件的真实性和完整性进行校验通过后方可正常启动。

c）结果判定:

实际测试结果与预期结果一致则判定为“符合”,其他情况判定为“不符合”。

B.2.2 系统与软件安全

B.2.2.1 口令安全

应满足 B.1.2.1 的测评方法。

B.2.2.2 身份鉴别

在满足 B.1.2.2 的测评方法的同时,还需满足如下测试方法、预期结果和结果判定:

a）测试方法:

1）核对设备设计文档，对所有物理接口尝试登录，验证是否对访问主体进行身份鉴别;

2）登录系统尝试进行修改网络安全配置、访问敏感个人信息等操作，验证是否使用与设备登录不同的因子进行认证，或对操作环境进行安全校验，安全校验方式包括但不限于登录设备校验、网络环境、操作行为。

b）预期结果:

1）所有通过物理接口登录设备，都对访问主体进行身份鉴别;

2）进行修改网络安全配置、访问敏感个人信息等重要操作使用与设备登录不同的因子进行认证，或对操作环境进行安全校验，安全校验方式包括但不限于登录设备校验、网络环境、操作行为。

c）结果判定:

实际测试结果与预期结果一致则判定为“符合”,其他情况判定为“不符合”。

B.2.2.3　关键安全参数保护

在满足 B.1.2.3 的测评方法的同时,还应满足如下测试方法、预期结果和结果判定:

a）测试方法:

1）查阅产品设计文档，检查是否采用了密码技术对关键安全参数进行保护;

2）查阅产品设计文档，检查是否建立了规范的关键

安全参数的安全管理流程，例如密钥生成、密钥配置、密钥使用、密钥存储、密钥吊销、密钥销毁等;

3）查阅产品设计文档，检查是否保证设备重要的关键安全参数对每个设备是唯一的，设备重要的关键安全参数包括但不限于设备根密钥、保证安全更新真实性和完整性的密钥、保证网络通信机密性和完整性的密钥。

b）预期结果:

1）产品采用了密码技术对关键安全参数进行保护;

2）建立了规范的关键安全参数的安全管理流程;

3）设备重要的关键安全参数对每个设备是唯一的，设备重要的关键安全参数包括但不限于设备根密钥、保证安全更新真实性和完整性的密钥、保证网络通信机密性和完整性的密钥。

c）结果判定:

实际测试结果与预期结果一致则判定为“符合”,其他情况判定为“不符合”。

B.2.2.4 密码应用

应满足 B.1.2.4 的测评方法。

B.2.2.5 访问控制

访问控制的测评方法如下:

a）测试方法:

1）具有设备绑定功能的产品:

（1）查阅产品设计文档，核验用户在绑定设备时，是否与设备进行交互确认;

（2）核验已完成设备绑定的产品，是否可以接受来自绑定账号或其授权账号的控制指令;

（3）核验已完成设备绑定的产品，是否可以在原设备绑定用户未主动解除绑定的情况下，接受其它账号的绑定。

2）具有授权功能的产品:

（1）查阅产品设计文档，检查访问控制策略是否满足最小授权原则，尝试用设备管理员以外的用户访问受控资源或使用关键功能验证是否成功;

（2）尝试用设备管理员以外的用户访问权限分享功能，验证是否能访问成功;

（3）查阅产品设计文档，检查是否采取防护措施保障分享的安全性。

b）预期结果:

1）具有设备绑定功能的产品:

（1）在用户绑定设备时，与设备进行交互确认;

（2）已完成设备绑定的产品，仅接受来自绑定账号或其授权账号的控制指令;

（3）已完成设备绑定的，不再接受其它账号绑定，除非原设备绑定用户主动解除绑定。

2）具有授权功能的产品:

（1）设备访问控制策略满足最小授权原则，不允许设备管理员以外的用户访问受控资源或使用关键功能;

（2）只能由设备管理员具备访问权限分享功能，其它用户不具备权限分享功能;

（3）产品具备防护措施保障分享的安全性。

c）结果判定:

实际测试结果与预期结果一致则判定为“符合”,其他情况判定为“不符合”。

B.2.2.6 日志审计

日志审计的测评方法如下:

a）测试方法:

1）检测产品日志，是否对开关机、创建用户、更改配置、安装与卸载软件、软件升级、修改口令、登录失败、特权用户登录等事件进行记录，审计记录应包括事件类型、事件发生时间、触发事件的主体、事件处理结果等信息;

2）查阅设计文档，对于审计日志有哪些保护机制，检查产品是否具备对日志记录的访问权限控制等保护机制，使其免遭非法访问、篡改及破坏。尝试对日志进行非授权修改和删除;

3）检测产品日志，检查产品是否具备审计日志存储保护机制，日志存储量超过阈值后是否正常记录最新事件;

4）检查日志是否存储于非易失性存储介质。

b）预期结果:

1）能对开关机、创建用户、更改配置、软件升级、修改口令、登录失败、特权用户登录等事件进行记录，审计记录应包括事件类型、事件发生时间、触发事件的主体、事件处理结果等信息;

2）产品具备对日志记录的访问权限控制等保护机制，使其免遭非法访问、篡改及破坏;

3）产品具备审计日志存储保护机制，日志存储量超过阈值后正常记录最新事件;

4）日志保存于非易失性存储介质。

c）结果判定:

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.2.2.7 固件安全

固件安全的测评方法如下:

a）测试方法:

1）查阅开发者文档是否具有对固件升级包进行完整性校验和真实性校验的方法说明；分别使用满足完整性和真实性的固件升级包和不满足完整性和真实性的固件升级包进行验证，查看是否具有完整性和真实性校验过程和结果，查看升级是否成功;

2）查阅设备说明文档，检查系统是否具备自动或人工更新、更新中止后重新更新的功能;

3）查阅设备说明文档，检查系统更新是否具备防非授权回退校验机制；尝试非授权更新低版本固件，验证是否成功;

4）查阅设备说明文档，检查设备第一次使用或恢复出厂设置后是否提示进行安全更新。

b）预期结果:

1）固件升级具备安全校验机制，会验证更新固件的真实性和完整性;

2）设备可通过自动、人工方式进行安全更新，更新中止后可重新更新;

3）系统更新具备防非授权回退校验机制，无法通过

非授权方式更新低版本固件;

4）设备在第一次使用或恢复出厂设置后会检查并提示进行安全更新。

c）结果判定:

实际测试结果与预期结果一致则判定为“符合”,其他情况判定为“不符合”。

B.2.2.8　输入验证

输入验证的测评方法如下:

a）测试方法:

查阅设备设计文档，检查是否存在对通过用户界面输入、应用程序编程接口输入的数据的安全校验措施。在用户界面输入框中提交非法字符，验证系统是否拦截非法输入，且未向后端传输无效数据。

b）预期结果:

存在对通过用户界面输入、应用程序编程接口输入的数据的安全校验措施，系统可以拦截非法输入。

c）结果判定:

实际测试结果与预期结果一致则判定为“符合”,其他情况判定为“不符合”。

B.2.2.9　安全配置

安全配置的测评方法如下:

a）测试方法:

查看设备管理操作界面或控制应用程序界面，核查设备是否提供设备配置项列表，是否默认为安全的，所有网络服务、端口为默认最小化的；查看设备配置过程，核查设备是否向用户进行安全设置的指导。

b）预期结果:

设备提供默认安全的配置，向用户提供安全设置的指导。

c）结果判定:

实际测试结果与预期结果一致则判定为“符合”,其他情况判定为“不符合”。

B.2.3 网络与通信安全

B.2.3.1 网络端口

网络端口的测评方法如下:

a）测试方法:

1）查看摄像头设备说明书中是否明确声明公开的不必要的网络接口。使用端口扫描工具识别设备在默认状态下开放的端口情况，与设备说明书中说明情况进行比对，检查设备网络端口开放是否遵循最小化原则，是否默认关闭非必须使用及未使用的网络端口;

2）未登录认证时，查看网络端口暴露的信息是否简化;

3）验证是否可手动关闭非必要的网络服务;

4）进入设备管理界面，查阅设备文档，确认是否完整说明所有网络端口的用途及对应服务。

b）预期结果:

1）设备网络服务和网络端口开放遵循最小化原则，默认关闭非必须使用的网络服务和网络端口;

2）设备未认证状态下未暴露网络端口信息;

3）用户可关闭非必要的网络服务;

4）设备提供了文档并说明所有网络端口和服务。

c）结果判定:

实际测试结果与预期结果一致则判定为“符合”,其他情况判定为“不符合”。

B.2.3.2 通信安全

通信安全的测评方法如下:

a）测试方法:

1）使用网络抓包工具查看数据传输（如设备与管理端、设备与服务器交互）是否采用加密技术;

2）尝试重复发送已捕获的传输数据，验证是否能抵抗重放攻击。

b）预期结果:

1）设备使用了加密技术保护数据传输的真实性、机密性、完整性;

2）设备具有抵抗重放攻击的能力。

c）结果判定:

实际测试结果与预期结果一致则判定为“符合”,其他情况判定为“不符合”。

B.2.4 数据安全与个人信息保护

B.2.4.1 数据安全

在满足 B.1.3.1 的测评方法的同时,还应满足如下测试方法、预期结果和结果判定:

a）测试方法:

1）查阅设备说明书、管理端操作指南等文档，确认是否明确说明故障诊断日志上传的触发条件、告知方式及用户同意流程；模拟设备故障场景，观察是否触发日志上传告知流程；核查告知内容的完整性；验证告知方式的显著性；核查同意机制的有效性;

2）核验设备是否提供了用户关闭上传用户数据的相关功能；验证是否能关闭上传用户数据功能;

3）查阅设备安全设计文档、技术白皮书，确认是否明确说明保护用户数据机密性和完整性的具体安全措施；用抓包工具捕获数据包，验证传输是否采用加密技术。

b）预期结果:

1）设备告知用户数据采集方式、范围、目的，并经用户同意后上传，告知内容完整，告知方式显著；

2）设备具备用户关闭上传用户数据的相关功能；

3）设备采取加密等安全措施保护用户数据的机密性和完整性。

c）结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.2.4.2　个人信息保护

在满足 B.1.3.2 的测评方法的同时，还应满足如下测试方法、预期结果和结果判定：

a）测试方法：

1）查阅个人信息处理规则，确认对外提供个人信息的目的、方式、种类及接收方是否以清单形式列明；

2）验证管理端是否有便捷通道（如设置页、客服入口）供用户行使个人信息权利，是否设置不合理限制条件。

b）预期结果：

1）设备对外提供个人信息相关内容以清单形式清晰列明；

2）设备有便捷通道（如设置页、客服入口）供用户

行使个人信息权利，无不合理限制条件。

c）结果判定:

实际测试结果与预期结果一致则判定为“符合”,其他情况判定为“不符合”。

B.2.5 安全保障

B.2.5.1 漏洞管理

应满足 B.1.4.1 的测评方法。

B.3 领先级测评

B.3.1 物理与硬件安全

B.3.1.1 设备标识与信息

应满足 B.2.1.1 的测评方法。

B.3.1.2 物理接口安全

应满足 B.2.1.2 的测评方法。

B.3.1.3 安全启动

应满足 B.2.1.3 的测评方法。

B.3.2 系统与软件安全

B.3.2.1 口令安全

应满足 B.2.2.1 的测评方法。

B.3.2.2 身份鉴别

在满足 B.2.2.2 的测评方法的同时,还应满足如下测试方法、预期结果和结果判定:

a）测试方法:

登录系统尝试进行修改网络安全配置、访问敏感个人信息等操作，验证是否使用与设备登录不同的因子进行认证，或对操作环境进行安全校验，安全校验方式包括但不限于登录设备校验、网络环境、操作行为。

b）预期结果:

进行修改网络安全配置、访问敏感个人信息等重要操作使用与设备登录不同的因子进行认证，或对操作环境进行安全校验，安全校验方式包括但不限于登录设备校验、网络环境、操作行为。

c）结果判定:

实际测试结果与预期结果一致则判定为“符合”,其他情况判定为“不符合”。

B.3.2.3 关键安全参数保护

在满足 B.2.2.3 的测评方法的同时,还应满足如下测试方法、预期结果和结果判定:

a）测试方法:

查阅设备说明文档，检查是否采用安全芯片等硬件方式保护和使用密钥。

b）预期结果:

设备采用安全芯片等硬件方式保护和使用密钥。

c）结果判定:

实际测试结果与预期结果一致则判定为“符合”,其他情况判定为“不符合”。

B.3.2.4 密码应用

应满足 B.2.2.4 的测评方法。

B.3.2.5 访问控制

应满足 B.2.2.5 的测评方法。

B.3.2.6 日志审计

在满足 B.2.2.6 的测评方法的同时,还应满足如下测试方法、预期结果和结果判定:

a）测试方法:

通过网络平台部署的，检查审计日志记录的期限是否为 180 天及以上。

b）预期结果:

通过网络平台部署的，审计日志记录的期限为 180 天及以上。

c）结果判定:

实际测试结果与预期结果一致则判定为“符合”,其他情况判定为“不符合”。

B.3.2.7 固件安全

应满足 B.2.2.7 的测评方法。

B.3.2.8 输入验证

应满足 B.2.2.8 的测评方法。

B.3.2.9 安全配置

应满足 B.2.2.9 的测评方法。

B.3.3 网络与通信安全

B.3.3.1 网络端口

应满足 B.2.3.1 的测评方法。

B.3.3.2 通信安全

应满足 B.2.3.2 的测评方法。

B.3.4 数据安全与个人信息保护

B.3.4.1 数据安全

应满足 B.2.4.1 的测评方法。

B.3.4.2 个人信息保护

在满足 B.2.4.2 的测评方法的同时，还宜满足如下测试方法、预期结果和结果判定：

a）测试方法：

1）查阅消费类网联摄像头的敏感个人信息处理相关文档，确认是否明确规定敏感个人信息脱敏处理的范围、方式及相关技术标准；

2）核查文档中明确的脱敏方式，确认是否包含至少一种及以上脱敏方式，同时确认是否有其他补充脱敏方式及具体实施说明；

3）对消费类网联摄像头进行实际操作测试，模拟正常拍摄场景，查看实时预览、录制存储的视频内

容，验证是否对敏感个人信息进行了脱敏处理；

4）核查视频存储文件及传输过程中的数据，确认脱敏处理后的视频数据在存储、传输环节，敏感个人信息仍处于脱敏状态，未出现脱敏失效、敏感个人信息泄露的情况；

5）查阅脱敏处理相关的技术参数文档及测试记录，确认脱敏方式的有效性、稳定性，是否能持续对敏感个人信息进行可靠脱敏，无明显漏洞；

6）核查产品是否具备脱敏参数调整机制，且调整后仍能满足敏感个人信息脱敏要求。

b）预期结果：

1）消费类网联摄像头生产者已制定完善的敏感个人信息脱敏处理相关文档，明确脱敏范围、方式及技术标准，覆盖拍摄、预览、存储、传输全环节；

2）脱敏方式符合要求，至少包含一种及以上脱敏方式，补充脱敏方式合理且具备可操作性；

3）实际测试中，摄像头拍摄包含敏感个人信息的场景时，能实时对敏感个人信息进行脱敏处理，预览、录制的视频中敏感个人信息无法识别；

4）脱敏后的视频数据在存储、传输过程中，脱敏状态保持稳定，无敏感个人信息泄露、脱敏失效的情况；

5）脱敏处理技术稳定有效，相关测试记录完整，能证明脱敏机制可持续、可靠运行;

6）产品具备合理的脱敏参数调整机制，调整后仍能有效实现敏感个人信息脱敏，满足隐私保护要求。

c）结果判定:

实际测试结果与预期结果一致则判定为“符合”,其他情况判定为“不符合”。

B.3.5 安全保障

B.3.5.1 漏洞管理

应满足 B.2.5.1 的测评方法。

B.3.5.2 产品生命周期管理

产品生命周期管理的测评方法如下:

a）测试方法:

1）查阅产品管理文档，确认是否建立覆盖设计、开发、测试、交付、运维等环节的全生命周期网络安全管理机制;

2）核查安全设计机制文档，是否参考 GB/T 39276—2020 第 5.1.2.1 项进行威胁建模，包含威胁识别、分析及缓解措施;

3）查看开发安全文档，是否描述设计和开发过程中保障数据存储与传输机密性、完整性的机制和流

程;

4）核查安全开发机制相关文件，是否满足 GB/T 39276—2020 第 5.1.2.1 项要求;

5）查阅安全测试机制文档及测试记录，确认定期或在重要版本发布前是否开展静态安全测试、动态安全测试等规定测试类型;

6）检查安全交付机制文档及交付记录，确认产品交付和重要版本发布前是否执行安全审查和加固;

7）核查安全运维机制和流程文档，是否满足 GB/T 39276—2020 第 5.2.2.3 项要求。

b）预期结果:

1）产品生产者建立了产品全生命周期网络安全管理机制，覆盖设计、开发、测试、交付、运维等环节;

2）产品生产者建立了产品安全设计机制，参考 GB/T 39276—2020 第 5.1.2.1 项相关要求进行威胁建模，以识别、分析和缓解对设备的安全威胁;

3）产品生产者编制了开发安全文档，描述设备设计和开发过程中实现数据存储和传输的机密性和完整性的机制和流程;

4）产品生产者建立了产品安全开发机制，应满足 GB/T 39276—2020 第 5.1.2.1 项相关要求;

5）产品生产者建立了安全测试机制，定期或在重要版本发布前进行安全测试，包括但不限于：静态安全测试、动态安全测试、API 测试、模糊测试、代码审查等;

6）产品生产者建立了安全交付机制，在产品交付和重要版本发布前进行安全审查和加固;

7）产品生产者建立安全运维机制和流程，应满足 GB/T 39276—2020 第 5.2.2.3 项相关要求。

c）结果判定:

实际测试结果与预期结果一致则判定为“符合”,其他情况判定为“不符合”。

B.3.5.3 代码检测

代码检测的测评方法如下:

a）测试方法:

1）进行代码检测，或查阅第三方检测机构出具的代码检测报告，检测对象为源代码或二进制程序，覆盖以下检测内容：是否存在软件安全漏洞和错误、第三方库和第三方组件中的安全漏洞、硬编码身份鉴别信息和关键安全参数；确认检测机构具备相应检测资质，检测流程符合规范;

2）核查产品是否存在使用应用程序进行设备管理的情况；若存在，进行管理应用程序检测，或查阅

第三方检测机构出具的设备管理应用程序检测报告，检测对象为源代码或二进制程序，覆盖以下检测内容：是否存在硬编码关键安全参数、通过明文存储或传输关键安全参数和敏感个人信息、违规传输敏感个人信息；确认检测机构具备相应检测资质，检测流程符合规范；

3）核查检测报告中的检测过程记录、原始数据及检测结论，确认检测内容无遗漏、检测方法科学合理，检测结果真实有效。

b）预期结果：

1）委托第三方检测的，检测机构具备相应资质；对设备自身代码进行全面检测，检测内容覆盖软件安全漏洞和错误、第三方库和第三方组件中的安全漏洞、硬编码身份鉴别信息和关键安全参数，检测结论为合格（无中风险及以上漏洞）；

2）使用应用程序对设备进行管理的，如委托第三方检测，检测机构具备相应资质；对设备管理应用程序进行全面检测，检测内容覆盖硬编码关键安全参数、通过明文存储或传输关键安全参数和敏感个人信息、违规传输敏感个人信息，检测结论为合格（无相关违规问题，或发现的问题已完成整改）；

3）检测报告完整规范，包含检测资质证明、检测流程、检测内容、检测数据、检测结论等核心要素，检测过程符合相关标准要求。

c）结果判定:

实际测试结果与预期结果一致则判定为“符合”,其他情况判定为“不符合”。

附录 C

（规范性）

第三方检测机构能力要求

C.1 机构要求

第三方检测机构应满足如下要求：具有 CNAS、CMA 资质，认可能力范围覆盖网络安全检测相关内容。

C.2 人员要求

进行渗透测试的第三方检测机构应至少有 5 人专职从事渗透测试相关工作，相关人员应至少满足下列章条中的任意 1 项要求:

a）具有 CISP-PTE、CISP-PTS 等渗透测试相关证书;

b）具有渗透测试相关项目经历;

c）具有 5 年内通过合法方式挖掘安全漏洞并向国家权威漏洞库报送的经历;

d）在国家级、省部级网络安全赛事获得奖励的人员。