ICS 13.310

A 91

GA

中华人民共和国公共安全行业标准

GA/T XXXX.1—XXXX

公安视频图像信息系统安全技术要求 第1部分：通用要求

Security technical requirements for video and image information system for public security —Part 1: General requirements

（报批稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国公安部　　发布

目　次

目次 I
前言 II
1 范围 1
2 规范性引用文件 1
3 术语和定义、缩略语 1
3.1 术语和定义 1
3.2 缩略语 2
4 总体技术要求 2
4.1 基本要求 2
4.2 安全技术功能组成 3
5 前端接入区安全技术要求 4
5.1 前端设备接入安全 4
5.2 前端设备安全 4
6 安全交互区安全技术要求 4
6.1 横向边界安全技术要求 4
6.2 纵向防护安全技术要求 6
6.3 其他安全技术要求 7
7 系统应用区安全技术要求 7
7.1 视频图像信息应用安全 7
7.2 视频图像信息数据安全 8
7.3 运行环境安全 8
8 安全管理区安全技术要求 9
8.1 安全基础设施 9
8.2 安全管理平台 10

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

GA/T XXXX《公安视频图像信息系统安全技术要求》分为4个部分：

——第1部分：通用要求；

——第2部分：前端设备；

——第3部分：安全交互；

——第4部分：安全管理平台。

本文件是 GA/T XXXX的第1部分。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由公安部科技信息化局提出。

本文件由全国安全防范报警系统标准化技术委员会（SAC/TC100）归口。

本文件起草单位：公安部第一研究所、公安部科技信息化局、视频图像信息智能分析与共享应用技术国家工程实验室、杭州熙菱信息技术有限公司、北京天防安全科技有限公司、奇安信科技集团股份有限公司、格尔软件股份有限公司、苏州科达科技股份有限公司、公安部安全与警用电子产品质量检测中心、北京市公安局、河南省公安厅、浙江宇视科技有限公司、北京明朝万达科技股份有限公司、浙江大华技术股份有限公司、华为技术有限公司、深信服科技服份有限公司。

本文件主要起草人：王建勇、赵源、闫雪、崔云红、栗红梅、周群、张震宇、段伟恒、邬怡、杨学军、陈建华、卢玉华、解丹、余新康、王连朝、喻波、邓志吉、孟凡辉、邱慎奋。

本文件于202x年首次发布。

公安视频图像信息系统安全技术要求
第1部分：通用要求

1 范围

本文件规定了公安视频图像信息系统安全的总体技术要求，以及前端接入区、安全交互区、系统应用区、安全管理区的安全技术要求。

本文件适用于基于公安视频传输网建设的视频图像信息系统安全的总体规划、方案设计、工程建设、运维管理、检验验收，以及与之相关的系统设备研发、生产和质量控制。其他视频图像信息系统可参照执行。

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/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 28181 公共安全视频监控联网系统信息传输、交换、控制技术要求

GB 35114 公共安全视频监控联网信息安全技术要求

GA/T 1400.4 公安视频图像信息应用系统 第4部分：接口协议要求

GA/T XXXX.2—XXXX 公安视频图像信息系统安全技术要求 第2部分：前端设备

GA/T XXXX.3—XXXX 公安视频图像信息系统安全技术要求 第3部分：安全交互

GA/T XXXX.4—XXXX 公安视频图像信息系统安全技术要求 第4部分：安全管理平台

3 术语和定义、缩略语

3.1 术语和定义

GB/T 22239、GB/T 28181、GB 35114界定的以及下列术语和定义适用于本文件。

3.1.1

视频图像信息 video and image information

视频流、视频片段、图像、与视频片段和图像相关的文件，以及相关描述信息。

3.1.2

公安视频图像信息系统 video and image information system for public security

以维护公共安全为目的，提供视频图像信息采集、传输、存储、分析、处理、应用、联网共享、安全保护等功能的系统。

3.1.3

公安视频传输网 video transmission network for public security

建设在公安信息网之外，采用专线方式或虚拟专用网方式，主要用于传输视频图像、汇接各层级公安视频图像信息系统、支撑公安视频图像信息服务的非涉密网络,包括主干网、城域网和接入网等部分。

注：公安视频传输网可以根据需要按照管理要求传输视频图像之外的其他相关公安业务数据。

3.1.4

前端设备 front-end device

公安视频图像信息系统中应用于现场、具备视频图像等安防信息采集、编/解码、存储、传输、安全控制等功能的设备或其设备组合。

3.1.5

横向边界区 region of horizontal border

公安视频传输网与其他网络进行信息交换的区域。

注：其他网络主要包括公安信息网、公安移动信息网、电子政务外网及其他行业专网、互联网等网络。

3.1.6

纵向防护区 region of vertical border

公安视频传输网的本级与上下级主干网、主干网与接入网进行连接的区域。

3.1.7

安全交互系统 security interaction system

公安视频传输网的上下级主干网络间、主干网与接入网间，以及公安视频传输网与其他网络互联时，实现网络间信息安全交互的系统。安全交互系统包括纵向安全防护系统和横向边界安全交互系统。

3.1.8

横向边界安全交互系统 horizontal border security interaction system

公安视频传输网与其他网络互联时，实现在边界上建立网络间信息交互安全的系统。

3.1.9

纵向安全防护系统 vertical security interaction system

公安视频传输网的本级与上下级主干网、主干网与接入网间建立信息交互安全的系统。

3.2 缩略语

下列缩略语适用于本文件。

API：应用程序接口（Application Programing Interface）

DDoS：分布式拒绝服务（Distributed Denial of Service）

DVR：硬盘录像机（Digital Video Recorder）

IP：因特网协议（Internet Protocol）

IPC：网络摄像机（Internet Protocol Camera）

NVR：网络硬盘录像机（Network Video Recorder）

SSH：安全外壳（Security Shell）

4 总体技术要求

4.1 基本要求

4.1.1 公安视频图像信息系统应具有发现和修复重要安全漏洞的技术措施。

4.1.2 公安视频图像信息系统应具有及时发现、检测攻击行为和处置安全事件的技术措施。

4.1.3　公安视频图像信息系统应具有防护恶意攻击的技术措施。

4.1.4　公安视频图像信息系统应具有在自身遭到损害时较快恢复绝大部分功能的技术措施。

4.1.5　公安视频图像信息系统的物理安全和公安视频传输网网内安全应符合 GB/T 22239 的相关规定。

4.1.6　公安视频图像信息系统的安全技术防护措施应与相应安全管理措施配合实现对公安视频图像信息系统的安全防护。

4.2　安全技术功能组成

4.2.1　公安视频图像信息系统应从前端安全、边界/接入安全（包括横向边界安全和纵向防护安全）、运行环境安全、视频图像数据安全、视频图像应用安全、安全管理平台、安全基础设施等维度构建安全技术总体框架。公安视频图像信息系统安全技术功能组成见图 1。

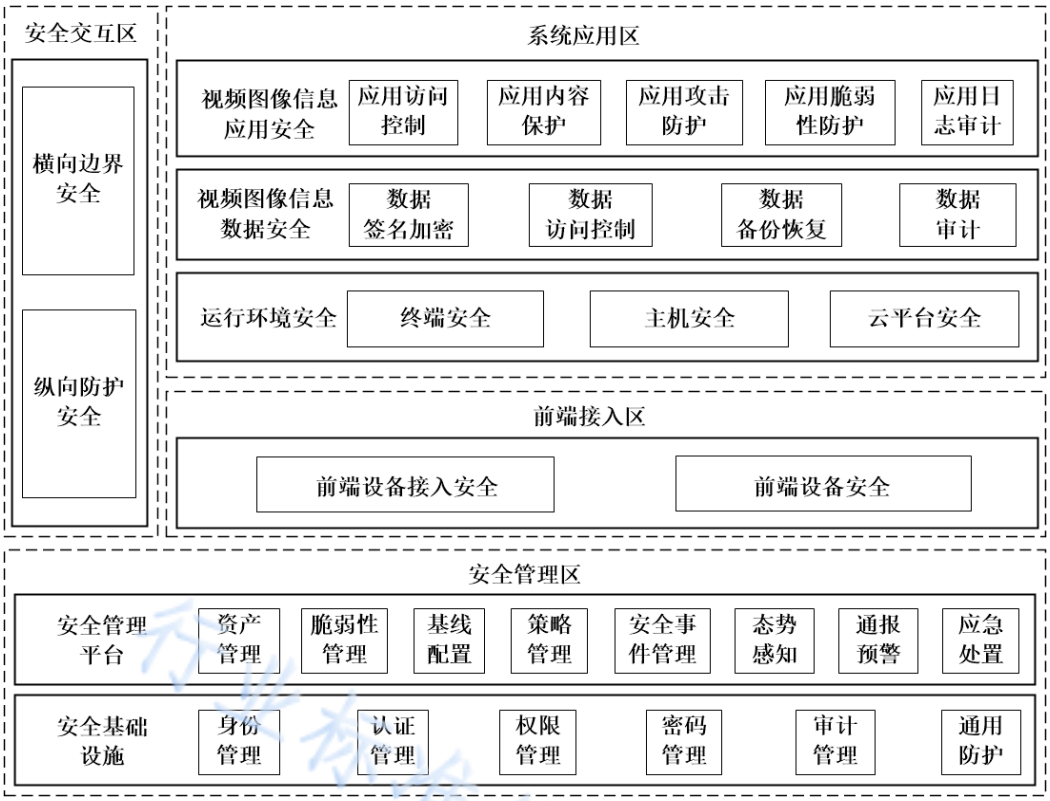

图1　公安视频图像信息系统安全技术功能组成图

4.2.2　公安视频图像信息系统安全域分为前端接入区、安全交互区、系统应用区和安全管理区。

4.2.3　前端接入区指部署公安视频图像信息系统的各类前端设备、相关网络设备及链路的区域。前端接入区安全包括前端设备接入安全和前端设备安全。

4.2.4　安全交互区包括横向边界区和纵向防护区，横向边界区通过部署横向边界安全交互系统实现横向边界安全防护，纵向防护区通过部署纵向安全防护系统实现纵向安全防护。

4.2.5　系统应用区指部署各类中心端视频图像信息系统的区域。系统应用区安全防护包括视频图像信息应用安全、视频图像信息数据安全、运行环境安全。

4.2.6　安全管理区指公安视频图像信息系统中实现安全基础设施服务和安全运行管理的区域，包括安全管理平台和安全基础设施。

5 前端接入区安全技术要求

5.1 前端设备接入安全

5.1.1 前端设备接入公安视频传输网时，应采用虚拟专线或物理专线方式。
5.1.2 应对前端设备进行安全准入管理，对于未通过准入管理的前端设备应及时阻断、告警。
5.1.3 宜对前端接入流量进行分析，阻断异常流量或阻断流量异常设备的网络通信。
5.1.4 无线前端设备接入公安视频传输网应符合 GA/T XXXX.3—XXXX 的规定。

5.2 前端设备安全

5.2.1 前端设备安全包括物理安全、身份鉴别、访问控制、入侵防范、数据安全、证书和密钥管理、日志安全、无线交互类前端设备管控、无线前端设备承载业务等，前端设备安全应符合 GA/T XXXX.2—XXXX 的规定。
5.2.2 前端设备分类与分级应符合 GA/T XXXX.2—XXXX 的规定。

6 安全交互区安全技术要求

6.1 横向边界安全技术要求

6.1.1 基本安全要求

6.1.1.1 公安视频传输网应通过横向边界安全交互系统与公安移动信息网、电子政务外网及其他行业专网、互联网等网络实现视频图像信息的交互；公安视频传输网与公安移动信息网、电子政务外网及其他行业专网之间应为双向数据传输，公安视频传输网与互联网之间应为双单向数据传输。
6.1.1.2 横向边界安全交互系统包括视频交换链路和数据交换链路。视频交换链路用于视音频流的传输，数据交换链路用于视频图像（如视频片段、图像数据等）、其他数据（如文件、数据库记录等）、视频图像信息数据库请求（如采用 JSON 格式的 API 请求）的传输；视频交换链路和数据交换链路均应采用数据交换前置服务、安全隔离设备和数据交换后置服务方式搭建。
6.1.1.3 横向边界安全交互系统应根据连接区域的安全要求划分安全等级，并应符合 GA/T XXXX.3—XXXX 的规定。
6.1.1.4 公安视频传输网与公安信息网之间进行视频图像信息和数据交换时，应满足公安信息网边界接入的相关规定。

6.1.2 视频交换链路安全技术要求

6.1.2.1 设备认证

应对所有接入视频交换链路的设备进行身份认证，身份认证应基于公安机关颁发的数字身份证书，认证协议应采用符合GB/T 28181或GB 35114的认证协议。

6.1.2.2 访问控制

6.1.2.2.1 应禁止未通过身份认证的接入设备进入视频交换链路。
6.1.2.2.2 通过身份认证的接入设备只能访问视频交换链路内的指定设备，且只能进行已被授权的操作，非授权的访问应被阻断。

6.1.2.3 流向控制

视频流与视频控制信令应按照不同的安全策略分别进行处理和传输，其中视频流应根据业务需求采用单向或双向传输模式。

6.1.2.4 协议限制

其他网络的视频图像信息系统应通过视频交换链路以符合GB/T 28181、GB 35114或公安移动信息网专用协议与公安视频传输网进行视频信息的共享与交互。

6.1.2.5 交换服务策略

宜根据预先设置或动态下发的交换服务策略实现视频交换链路的全部或部分服务启停，并支持视频交换任务优先级设置。

6.1.2.6 格式检查

应按照预先注册的视频控制信令和视频数据的类型、格式和内容对控制信令和视频数据进行“白名单”方式的格式检查，仅允许符合格式要求的控制信令数据和视频数据通过，对不符合格式要求的数据进行阻断和告警。

6.1.2.7 内容过滤

宜采取安全技术措施防止视频数据夹杂恶意代码进入公安视频传输网。

6.1.2.8 安全审计

应采集并审计视频信息交换过程中的视频交换链路应用日志和流量日志。

6.1.3 数据交换链路安全技术要求

6.1.3.1 设备认证

应对所有连接数据交换链路的设备进行身份认证。身份认证应基于公安机关颁发的数字身份证书，认证协议应采用带有安全机制的认证协议。

6.1.3.2 访问控制

6.1.3.2.1 应禁止未通过身份认证的接入设备进入数据交换链路。

6.1.3.2.2 通过身份认证的接入设备只能访问数据交换链路内的指定设备，且只能进行已被授权的操作，非授权的访问应被阻断。

6.1.3.3 数据交换

其他网络的非视频图像类数据（文件、通用数据库等）应通过数据交换链路以文件交换、数据库交换方式与公安视频传输网进行信息共享与交换。

6.1.3.4 接口服务

其他网络的视频图像数据（如视频片段、图像数据等）应通过数据交换链路以接口服务（如符合GA/T 1400.4的视频图像信息数据库请求）调用方式与公安视频传输网进行信息共享与交互。接口服务提供方应提供接口技术规范，包括调用方式、参数、封装格式、合法性校验等内容。

6.1.3.5 交换服务策略

宜根据预先设置和动态下发的交换服务策略实现交换链路的全部、部分服务启停，并支持设置任务优先级。

6.1.3.6 格式检查

应按照预先注册的数据交换或接口服务的类型、格式和内容对数据交换或接口服务进行格式检查，仅允许符合格式要求的数据交换或接口服务通过，对不符合格式的数据进行阻断和告警。

6.1.3.7 内容过滤

宜采取安全技术措施防止交换数据中夹杂恶意代码进入公安视频传输网。针对接口服务中的文件、图像等数据内容，宜采用图文转换、图像二次渲染等方式防止数据泄露。

6.1.3.8 验签服务

应采用密码技术保证重要数据在传输过程中的完整性，包括交换的文件、数据库记录、API请求应答等，数据交换链路应提供验签服务。

6.1.3.9 安全审计

应采集交换过程中数据交换链路的应用日志和流量日志。

6.2 纵向防护安全技术要求

6.2.1 基本安全要求

应在纵向防护区部署纵向安全防护系统实现公安视频传输网的纵向安全防护。

6.2.2 纵向安全防护系统安全等级划分

纵向安全防护系统应根据连接区域的安全要求划分不同的安全等级，并应符合GA/T XXXX.3—XXXX的规定。

6.2.3 纵向安全防护系统安全技术要求

6.2.3.1 网络访问控制

应按照最小访问控制原则限制网络访问权限。

6.2.3.2 网络入侵防范

6.2.3.2.1 应支持对网络入侵威胁进行防范，阻止或限制针对公安视频传输网的网络攻击和异常行为。

6.2.3.2.2 宜支持对网络流量进行还原取证、分析和统计。

6.2.3.3 流量过滤

宜支持采集、记录、分析网络流量，为符合GB/T 28181、GB 35114、GA/T 1400.4和其他必要的远程访问、运维和安全服务等技术接口协议建立白名单规则，对不符合规则的流量进行清洗过滤。

6.2.3.4 流量审计

宜支持捕获网络流量或导入其他网络流量，提供网络审计功能，审计记录保存不少于180d，并支持事后追溯和审计结果导出。

6.3 其他安全技术要求

应符合GA/T XXXX.3—XXXX的规定。

7 系统应用区安全技术要求

7.1 视频图像信息应用安全

7.1.1 应用访问控制

7.1.1.1 应对登录公安视频图像信息系统的用户进行身份鉴别，用户身份管理和认证管理由安全基础设施统一提供。

7.1.1.2 应对用户访问进行授权，并根据用户的不同角色、级别、所属机构、任务和场景进行鉴权、授权，实现功能级访问控制。

7.1.2 应用内容保护

7.1.2.1 应根据业务需求对公安视频图像信息系统展示和导出的敏感视频图像、数据等信息进行脱敏处理。

7.1.2.2 应对应用内容的完整性进行保护，防止非授权修改。

7.1.2.3 应对公安视频图像信息系统应用内容进行安全防护，防止自动化工具攻击和数据爬取。

7.1.3 应用攻击防护

7.1.3.1 应对视频图像应用服务进行 Web 攻击防护，识别、防御恶意用户针对 Web 应用发起的攻击。

7.1.3.2 应对视频图像应用服务进行 API 攻击防护，检测、识别、拦截针对 API 接口的攻击。

7.1.3.3 应对视频图像应用服务进行应用层 DDoS 攻击防护，阻断恶意发送大量合理请求、消耗目标系统服务资源的 DDoS 攻击行为。

7.1.4 应用脆弱性防护

7.1.4.1 应对应用程序的安全漏洞、编码隐患进行安全扫描检测，发现潜在的安全问题和架构缺陷。

7.1.4.2 应对已经发现的应用漏洞通过修补程序或软件版本升级进行漏洞修复。

7.1.5 应用日志审计

7.1.5.1 应记录视频图像业务应用的操作日志，操作日志应包含操作人、操作时间、操作终端、操作对象、操作条件、返回结果等。

7.1.5.2 应能够基于业务日志的行为发生 IP、行为发生时间范围、行为发生时间周期、行为结果等进行分析，发现用户异常行为。

7.1.5.3 应支持对异常应用行为进行告警，告警信息的内容包括但不限于告警类型、告警级别、事件时间、告警明细信息、处理建议等。支持对审计日志以及告警信息进行人工和自动处置。

7.1.5.4 应由审计管理员查阅审计日志信息，审计管理员的查阅和审计操作需记录日志。

7.1.5.5 应提供应用日志存储能力，日志保存时间不少于 180d。

7.1.6 其他应用安全措施

应具备根据需求增加其他应用安全技术措施的能力。

7.2 视频图像信息数据安全

7.2.1 数据签名和加密

7.2.1.1 重要视频数据的签名和加密应符合 GB 35114 的规定。

7.2.1.2 应对其他重要的非视频数据在传输和存储过程中通过签名、加密等措施进行完整性和机密性保护。

7.2.2 数据访问控制

7.2.2.1 应根据用户属性、数据属性、数据操作行为按最小权限原则配置数据访问权限策略。

7.2.2.2 结构化数据访问权限宜实现记录级权限管控。

7.2.3 数据备份恢复

7.2.3.1 应支持重要数据的本地备份与恢复。

7.2.3.2 应支持重要数据处理系统的热冗余。

7.2.3.3 宜支持异地备份。

7.2.4 数据审计

7.2.4.1 应支持对公安视频图像信息系统中数据库和数据文件系统的操作行为进行审计，审计记录应包括日期、时间、用户、事件类型、操作是否成功及其他与审计相关的信息。

7.2.4.2 应支持发现并记录异常数据操作、数据删除操作、敏感数据操作等。

7.2.4.3 应对视频图像信息的存储位置、使用交换过程、访问控制权限进行审计。

7.2.5 其他数据安全措施

应具备根据需求增加其他数据安全技术措施的能力。

7.3 运行环境安全

7.3.1 终端安全

7.3.1.1 应对恶意代码进行实时检测、查杀或隔离。

7.3.1.2 应及时安装系统补丁，修复系统漏洞。

7.3.1.3 应对终端网络连接的端口、协议类型等进行有效管理，关闭高危端口，阻断未知协议。

7.3.1.4 应采用数字水印等方式对拍照、转发等视频图像数据泄露行为进行追踪溯源。

7.3.1.5 应对接入视频传输网的终端进行身份认证。

7.3.1.6 应对违规内/外联行为进行及时发现、阻断。

7.3.1.7 应通过采集、分析终端数据，发现存在风险和威胁的终端。

7.3.2 主机安全

7.3.2.1 应能检查并调整物理主机操作系统的安全策略和配置。

7.3.2.2 应能扫描、分析物理主机上存在的安全漏洞，并提供修复建议。

7.3.2.3 应实时监控、识别针对物理主机的入侵和病毒攻击行为并阻断。

7.3.2.4 宜能通过裁剪物理主机操作系统内核、禁用不必要的系统服务等方式加固物理主机操作系统。

7.3.3 云平台安全

7.3.3.1 物理网络安全

应提供物理网络的安全访问控制，通过物理网络的安全威胁检测能力，保护云平台出口的物理网络。

7.3.3.2 虚拟化安全

应针对虚拟化漏洞的逃逸攻击进行检测和保护，对云计算资源进行隔离，保护宿主机和虚拟机的安全。

7.3.3.3 容器安全

应通过镜像完整性校验、资源安全隔离、文件访问控制、容器漏洞扫描、容器防逃逸、容器加固配置等机制，保障容器资源安全，降低容器运行风险。

7.3.3.4 云主机安全

应通过对云主机进行基线核查、漏洞扫描、入侵检测、安全加固、安全迁移、恶意代码查杀，对镜像进行安全加固、漏洞扫描、访问控制、安全备份，提高云主机安全防护能力，保障镜像数据安全。

7.3.3.5 云网络安全

应对云平台流量进行安全访问控制，构建隔离的虚拟网络环境，针对网络流量进行威胁检测，及时阻断网络中存在的恶意威胁行为。

7.3.3.6 云存储安全

宜利用多副本冗余、数据一致性保障、虚拟化隔离等机制保障云存储安全可靠；宜对存储数据进行加密，防止存储数据泄露。

8 安全管理区安全技术要求

8.1 安全基础设施

8.1.1 身份管理

8.1.1.1 身份管理对象包括用户、设备、应用、服务。
8.1.1.2 应对身份管理对象的身份进行唯一标识。
8.1.1.3 应对身份管理对象实施全生命周期身份管理，确保身份信息准确、及时更新。
8.1.1.4 宜建立统一的身份管理服务，实现各类应用间身份信息的统一。
8.1.1.5 宜对身份信息的变更进行审计。

8.1.2 认证管理

8.1.2.1 应在设备接入、网络互联、系统访问时进行身份认证。
8.1.2.2 认证技术宜采用数字证书、口令、生物特征、物理特征等进行双因子认证。
8.1.2.3 采用数字证书认证时，应采用国家商用密码算法及产品实现。
8.1.2.4 采用物理特征认证时，物理特征至少应包含 IP/MAC 地址或硬件唯一标识等特征信息。

8.1.2.5 前端设备认证应符合 GA/T XXXX.2—XXXX 的规定。
8.1.2.6 用户访问系统应用区的视频图像应用及其他服务时，用户认证应采用基于数字证书的方式；访问前端设备时应采用 GA/T XXXX.2—XXXX 要求的方式；用户认证可根据具体业务要求采用数字证书和生物特征的方式。
8.1.2.7 应用系统间通过接口互联时，宜基于物理特征或数字证书的方式进行身份认证。
8.1.2.8 应对身份认证结果进行审计。

8.1.3 权限管理

8.1.3.1 权限管理对象包括用户、设备、应用、服务。
8.1.3.2 权限管理资源类型包括应用功能权限、数据权限、接口权限。
8.1.3.3 权限授予应包括分级授权、自动授权、权限主动申请、权限委托等方式。
8.1.3.4 宜建立统一的授权管理服务，实现应用间权限管理的统一。
8.1.3.5 应对权限的使用进行审计。

8.1.4 密码管理

8.1.4.1 密码算法应使用国家商用密码算法。
8.1.4.2 应使用符合 GB 35114 规定的证书及密钥，并统一管理。

8.1.5 审计管理

8.1.5.1 系统管理员、审计管理员、安全管理员应通过特定的命令或界面进行操作，并对其操作内容进行审计。
8.1.5.2 应对公安视频图像信息系统的运行状况、网络流量、用户访问操作行为等进行日志审计记录。审计记录应涵盖访问的日期、时间、用户、事件类型、事件是否成功及其他与审计相关的信息。
8.1.5.3 应提供综合审计能力，对公安视频图像信息系统中的应用、终端、主机、数据库、网络流量进行综合审计。
8.1.5.4 应提供日志的存储能力，日志存储时间不少于 180d。

8.1.6 通用防护

8.1.6.1 应提供针对公安视频图像信息系统的基础安全防护能力，包括安全识别、安全防护、安全检测、安全响应等。
8.1.6.2 安全识别能力包括但不限于资产发现、漏洞扫描、基线核查等能力。
8.1.6.3 安全防护能力包括但不限于网络访问控制、隔离交换、网络准入、网络入侵防御、恶意代码查杀、补丁管理、应用安全防护等能力。
8.1.6.4 安全检测能力包括但不限于网络威胁检测、恶意代码检测、数据泄露检测等能力。
8.1.6.5 安全响应能力包括但不限于攻击溯源、调查取证、响应恢复等能力。

8.2 安全管理平台

8.2.1 资产管理

应对公安视频图像信息系统的资产信息进行统一管理，包括资产信息的导入、导出、新建、删除、修改、查询与统计等。支持从外部设备/系统获取资产管理数据，并能结合资产信息、漏洞信息、基线信息等进行多维度分析和展示。

8.2.2 脆弱性管理

8.2.2.1 应支持对前端设备、用户终端设备、网络设备、服务器、操作系统、应用软件等IT资产进行检测，发现安全漏洞，并提供修补建议。
8.2.2.2 应支持检测识别前端设备、应用系统等的弱口令问题，并对发现的弱口令进行评估、分析。
8.2.2.3 应定期进行脆弱性检测，对发现的安全隐患及风险进行处置。
8.2.2.4 宜对前端设备的特权账号（如SSH账号）进行统一管理，当特权行为采用口令密码进行身份鉴别时，应定期修改特权账号的密码。

8.2.3 基线配置

应建立公安视频图像信息系统的安全基线，对前端设备、网络设备、安全设备、主机、数据库、中间件、应用等进行安全合规性检查并提供评估、分析报告。支持从外部设备/系统获取基线配置核查数据，并能够结合配置核查信息进行多维度分析和展示。

8.2.4 策略管理

应支持采集策略、安全事件告警策略、监控策略等安全策略的集中管理，支持从外部设备/系统获取相关数据，结合安全风险、告警、威胁情报等信息实现安全策略的优化。

8.2.5 安全事件管理

8.2.5.1 安全事件应包含发生时间、IP地址、区域、事件类型、数量和危害等级等信息。
8.2.5.2 应支持对安全事件信息进行清洗、分类、合并整理形成统一的安全事件库。
8.2.5.3 应支持对安全事件的告警。

8.2.6 态势感知

8.2.6.1 应支持对公安视频图像信息系统内资产、安全事件、安全风险、安全威胁等信息进行采集、分析、展示。
8.2.6.2 应支持对公安视频图像信息系统的资产数据、安全数据等进行分析研判，并根据不同的安全风险、安全事件提供可视化态势分析展示，包括全网资产态势、风险威胁态势、违规行为态势、安全事件态势、脆弱性态势等。
8.2.6.3 宜支持建立威胁情报库。

8.2.7 通报预警

8.2.7.1 应对公安视频图像信息系统的安全事件、安全风险进行通报预警。
8.2.7.2 应将接收到的预警信息按照重要程度、影响范围等进行分级，支持进一步的预警处理。

8.2.8 应急处置

应对公安视频图像信息系统内安全事件进行及时响应和处置，支持按照应急处置事件等级、类型、影响范围、处置结果等进行分类、归档，并形成应急处置报告文档。

8.2.9 其他安全技术要求

应符合GA/T XXXX.4—XXXX的规定。