上海市安防视频图像系统信息安全产品技术基本要求（试行）

1. 应用范围

为进一步规范本市技防行业中安防视频图像系统的信息安全建设，根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《网络数据安全管理条例》、《公共安全视频图像信息系统管理条例》等法律法规，加强对安防视频图像系统的防攻击、防入侵、防病毒、防篡改、防泄露和隐私保护等信息安全防护，制定本要求。

本要求规定了对本市安防视频图像系统信息安全产品（以下简称“信息安全产品”）的总体要求、组成和基本功能，是相关产品选型、产品检测、工程设计、评审、验收和运行的主要依据。

2. 术语及定义

2.1. 安防视频图像系统

应用于安全防范领域的视频图像信息收集、传输、显示、存储的系统。

2.2. 视频融合安全网关

对安防视频图像系统提供防攻击、防入侵、防病毒、防篡改、防泄露、隐私保护等安全技术措施的安全设备。

2.3. 用户终端视频安全软件

运行在用户终端，与视频融合安全网关相配合，对从安防视频图像系统中获取的视频数据进行防泄露、防篡改保护的软件。

2.4. 视频水印

通过在视频内容中嵌入特定信息的技术，实现追踪溯源、完整性保护和版权标识的信息安全技术。视频水印包括视频显式水印和视频隐式水印。

2.5. 视频显式水印

在视频内容中嵌入使用者可察觉、可辨识的视频水印。

2.6. 视频隐式水印

在视频内容中嵌入对使用者隐蔽（肉眼不可察觉）、不可辨识且位置不固定的视频水印。

2.7. 视频水印安全网关

提供对安防视频图像系统中的视频码流实时嵌入视频显式水印和视频隐式水印，对用户终端调阅、监控大屏显示和视频共享等场景提供视频泄露追溯的安全设备。

2.8. 大屏显示安全网关

对监控大屏显示画面实时嵌入视频显式水印，对屏幕拍摄提供视频泄露追溯的安全设备。

2.9. 引流

通过调整路由器或者交换机的路由策略，改变 IP 报文的转发路径，引导 IP 报文经过特定设备。

3. 总体要求

3.1. 本市安全技术防范工程领域所涉及的安防视频图像系统应配置信息安全产品。

3.2. 信息安全产品应适用于符合《安全防范工程技术标准》（GB 50348）、《安全防范工程通用规范》（GB 55029）等标准中规定的安防视频图像系统。

3.3. 信息安全产品应符合《公共安全视频图像信息系统管理条例》中的技术要求。

3.4. 信息安全产品应符合《网络安全技术 网络攻击和网络攻击事件判定准则》（GB/T 37027）、《公安视频图像信息系统安全技术要求》（GA/T 1788.1）等标准的相关技术要求。

3.5. 信息安全产品应能有效防止安防视频图像系统的安全缺陷、漏洞等风险暴露，对新暴露的安全缺陷、漏洞等应在 48 小时内消除风险。信息安全产品对自身的安全缺陷、漏洞等风险应具有更高的防护能力，对新暴露的安全缺陷、漏洞等应在 24 小时内消除风险。

3.6. 用户终端应安装用户终端视频安全软件和病毒防护软件，两款软件应开机自动运行，且功能应处于开启状态。

3.7. 宜具备必要接口，配合自动化检测工具实现设备信息、工作状态、报警等信息的上报和检测工作。

3.8. 应符合用户授权要求，建立实名账号管理机制，结合岗位职能分配操作权限，账号专人专用，禁止共用、转借、冒用账号，杜绝越权查阅、处理视频图像信息。

3.9. 应实现分级分类管理，对系统用户、视频图像资源实行分级分类管控，按权限等级划定访问、查阅、调取、处置范围，不同级别用户不得跨权限访问非授权资源。

4. 系统组成

4.1. 信息安全产品的组成如下：

a. 基本配置由视频融合安全网关、用户终端视频安全软件和病毒防护软件组成。

b. 使用单位对视频显示防泄露有较高要求的，应配置视频水印安全网关，对监控大屏、终端调阅、视频共享等场景，提供视频隐式水印防护；其他单位宜配置视频水印安全网关。视频水印安全网关应使用商用密码技术对视频水印安全网关的用户认证和视频水印信息进行机密性和完整性保护，防止关键信息被非法泄露、篡改。

c. 在配置监控大屏且未配置视频水印安全网关的情况下，应配置大屏显示安全网关，提供视频显式水印防护，应支持文字水印、图片水印、滚动水印和点阵水印。

4.2. 视频融合安全网关通过交换机/路由器接入到安防视频图像系统中，应同时支持引流方式和直连方式，优先选择引流方式。视频融合安全网关应支持快速链路检测和切换能力，检测和切换时延小于200ms。

4.3. 大屏显示安全网关与监控大屏直连。

4.4. 视频水印安全网关通过交换机/路由器接入到安防视频图像系统中，应支持标准 API 接口提供视频显式水印和视频隐式水印。

4.5. 用户终端视频安全软件和病毒防护软件部署在用户终端上，其标准配置运行环境要求如下：

a. CPU：1.8GHz 及以上

b. 内存：8G 及以上

c. 操作系统：Windows10、麒麟 V10 和统信 V20 及以上操作系统

5. 技术要求

5.1. 防攻击

a. 网络防攻击：应支持发现网络层（IP 层、UDP 层、TCP 层和 TLS 层）攻击行为，并及时阻断和报警。

b. 通用协议防攻击：应支持发现通用应用协议（FTP、HTTP、SNMP、SSH 等）的攻击行为，并及时阻断和报警。

c. 视频专有协议防攻击：应支持发现视频专有协议（SIP、ONVIF、RTSP 等）的攻击行为，并及时阻断和报警。

5.2. 防入侵

a. 防嗅探：应支持实时发现黑客扫描探测安全缺陷、漏洞的行为，支持通过干扰和修改黑客收集信息，在不影响资产数量的情况下，对安防视频图像系统、特别是信息安全产品自身的安全缺陷、漏洞进行屏蔽。

b. 视频准入：应支持基于设备属性、数字证书、应用协议、流量行为的设备身份识别、认证和网络访问控制。应支持全流量逐包检测和实时阻断。

c. 应用层防护：应支持应用层协议解析能力，有效检测并防御应用层入侵行为。特征库应支持及时更新。

5.3. 防病毒

应支持对本地文件和HTTP、FTP等协议中的病毒进行识别和防御，特征库应支持及时更新。

5.4. 防篡改

应支持采用校验技术对安防视频图像系统导出视频文件的完整性进行校验，有效识别文件篡改。

应支持采用访问控制策略对安防视频图像系统导出视频文件进行防护。

5.5. 防泄露

a. 视频导出防泄露：应支持采用密码技术对安防视频图像系统导出的视频文件进行保密性和完整性保护；应支持依据安全策略，限制导出视频文件的使用环境。

b. 视频显示防泄露：应支持嵌入视频水印，实现对监控大屏、终端调阅的屏幕拍摄防护；使用单位对视频显示防泄露有较高要求的，应使用视频隐式水印，其鲁棒性应达到IEEE 3361中定义的3级；其他单位宜使用视频隐式水印。

c. 视频外发防泄露。

1）应支持通过授权，在用户终端将视频文件制作成外发数据，并应具有设置密码、时效、编辑、自删除等修改、调整功能；

2）应支持所制作的外发数据，在时效和权限许可范围内，无需安装专用软件即可使用；

3）应支持在外发文件中嵌入视频水印进行防护。使用单位对视频显示防泄露有较高要求的，应使用视频隐式水印，其鲁棒性应达到 IEEE 3361 中定义的 3 级；其他单位宜使用视频隐式水印。时长 10 分钟的视频文件，嵌入水印耗时不应超过 1 分钟。

4）不超过 5G 的外发文件在标准配置计算机上：打开时间比原始视频文件增加不应超过 10 秒钟。

5.6. 隐私保护

对于依法用于公开传播的视频信息，应支持对涉及的人脸、机动车号牌等敏感个人信息，以及法人、非法人组织的名称、营业执照等信息，采用遮挡等脱敏方式处理至无法识别。

1）人脸信息检出率和人脸信息误检率应达到 GB/T 41772《信息技术 生物特征识别 人脸识别系统技术要求》7.2 章节的要求；

2）机动车号牌、法人/非法人组织的名称、营业执照等信息检出率应>=90%，误检率应 <=10%；

3）应支持对单帧图像中多个敏感信息同时进行脱敏；

4）应支持 mp4、avi 格式的视频文件格式、支持 H.264、H.265 视频编解码格式、支持 JPEG、BMP、PNG 图像文件格式；

5）时长 10 分钟的视频文件，脱敏耗时不应超过 1 分钟。

5.7. 安全审计

应支持对重要安全事件的审计，包括视频文件的所有操作事件、用户身份鉴别事件、网络访问控制事件、防攻击事件、防入侵事件、防病毒事件、防篡改事件、防泄露事件等。

操作日志不得删除、篡改。

5.8. 视频水印规格性能

应包含机构/操作用户标识符(ID)、设备信息(IP 地址、MAC 地址、设备 ID 等)、当前时间信息等。其中，视频显式水印包含文字水印、图片水印、二维码水印、滚动水印、点阵水印、图像块水印等；视频隐式水印应符合《网络安全技术 数字水印技术实现指南》（GB/T 45909）。

6. 实施日期

本要求自发布之日起实施。

《上海市视频安防监控数据导出防泄密系统基本技术要求（试行）》（2014 年 3 号文）同时废止。