

附件 2

团体标准《视频安全防护系统》编制说明

一、工作简况

1. 任务来源

深圳市博通智能技术有限公司会根据行业发展，于 2024 年 5 月向深圳市网络与信息安全行业协会提出《视频安全防护系统》团体标准立项申请。深圳市网络与信息安全行业协会按程序批准该团体标准立项并发布公告。来自深圳市博通智能技术有限公司、中兴通讯股份有限公司、华测检测认证集团股份有限公司、深圳市安络科技有限公司、广东省信息安全测评中心等单位的专家参与了标准的制定。

2. 编制目的

经过多年的努力，我国已经建成世界上最大的视频监控网络，初步覆盖了公共区域重点单位和关键点位。目前在大规模联网、云计算和人工智能等新技术普及应用的背景下，视频监控系统面临严重的安全威胁和视频数据泄露风险。

本标准的目的是确保视频安全产品的质量和性能符合一定要求，以保障视频监控系统的网络安全和视频流数据安全。通过制定统一的技术要求和测试方法，有效减少不符合安全要求的视频防护系统流入市场，降低视频系统安全和数据泄露事故的风险。

二、标准的属性

本标准由深圳市网络与信息安全行业协会制定发布的团体标准。

三、标准制定原则

按照 GB/T1.1-2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的要求和规定编写本标准内容。

本标准具有先进性、系统性、普适性、可操作性。

三、确定标准主要内容的依据

《视频安全防护系统》团体标准为首次制定，确定主要内容的依据具体如下：

1. 法律法规要求

公共视频监控网络属于《中华人民共和国网络安全法》（网络安全法）、《中华人民共和国数据安全法》（数据安全法）定义的“关键信息基础设施”。《网络安全法》、《数据安全法》、《个人信息保护法》均对公共视频数据的安全防护、隐私保护、防泄漏做出了要求。另一方面，《关于加强公共安全视频监控建设联网应用工作的若干意见》（996 号）文件明确要求实现视频图像数据的全程可控。

本标准契合上述法律法规要求，对视频安全防护系统做出技术规定。

2. 行业最佳实践

本标准充分参考视频监控安全防护行业内广泛认可、经过验证并被证明为高效、可靠和安全的操作方式、技术选择、系统设计和策略。这些实践经验基于行业内多年知识积累，对于视频监控防护的规划、设计、实施和管理都具有重要的指导意义。

3. 技术发展趋势

随着视频监控系统在各个领域的应用越来越广泛，视频网络安全和视频数据加密也成为了重要的技术发展趋势。通过采用先进的网络安全技术和数据加密算法，可以确保视频数据在传输和存储过程中的安全性和可靠性。同时，加强系统的访问控制和身份认证机制也可以有效防止未经授权的访问和数据泄露事件的发生。本标准在技术要求中将视频网络、数据安全融入标准之中，确保标准的先进性和前瞻性。

4. 专家意见和学术研究

标准制订单位广泛征求视频安全防护行业专家的意见，从提升行业规范性、增强系统安全性、促进技术创新、便于系统集成和兼容性、提升行业国际竞争力等多个角度，确认标准具体内容。另一方面，标准制订单位通过搜索引擎、图书馆等渠道查阅视频安全防护领域的学术研究成果，了解最新研究动态，将其融入标准之中。

五、国内外现有相关标准情况

视频监控联网安全相关的国际标准组织包括 IEC、ISO、PSIA、ETSI、ONVIF 等，其中的 ONVIF 组织最具有代表性。该组织主要研究全球性的系统开放接口标准，所提出的 ONVIF 规范有效提升了国际上各类监控设备的连通性，使得系统具有兼容性。

在国内，目前国家标准化管理委员会推出三项相关的国家标准：GB/T25724-2017

主要对视频和音频数据的编解码方案做出了流程化的技术规定，提倡使用国密算法来保护数据安全；GB35114-2017 适用于监控系统内部的信息安全方案设计，规定了安全系统结构和基本功能要求，包括设备与平台之间的授权和访问控制、视频数据的加密与完整性校验；GB/T28181-2016 规定了监控系统内部的主要信令控制协议以及信息传输、控制、交互的互联结构，并且统一了信息传输流程和协议接口设置方案，克服了系统中数据格式规范和标准信令控制等问题。国内诸多安防领域的厂商均以上述三项标准为基础来展开产品设计与开发工作。

目前上述现有标准均没有在视频安全防护系统的系统结构、接口要求、功能要求、性能要求、安全要求、实验方法等方面做出具体规定，本标准填补这个空白。

六、重大分歧意见的处理经过和依据

本标准在制定过程中未出现重大分歧意见。

七、作为强制性标准或推荐性标准的建议

本标准建议作为推荐性标准发布实施。

八、其他应予说明的情况

无。