ICS 35.240
CCS L 80

团　体　标　准

T/CFEII 0009—2023

人脸识别应用安全评估指南

Guide to security evaluation for face recognition application

2023 - 08 - 21 发布　　2023 - 08 - 21 实施

中国电子信息行业联合会　发布

目　　次

前　言

本标准按照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。

本标准由中国电子信息行业联合会提出并归口。

请注意本标准的某些内容可能涉及专利，本标准的发布机构不承担识别专利的责任。

本标准起草单位：国家工业信息安全发展研究中心、国家语音及图像识别产品质量检验检测中心、小视科技（江苏）股份有限公司、杭州海康威视数字技术股份有限公司、上海依图网络科技有限公司、上海商汤智能科技有限公司、深信服科技股份有限公司、北京智游网安科技有限公司、蚂蚁科技集团股份有限公司、北京百度网讯科技有限公司、罗克佳华科技集团股份有限公司、大同市数字政府服务中心、北京信源电子信息技术有限公司大同分公司、北京信源电子信息技术有限公司吉安分公司。

本标准主要起草人：朱倩倩、汪慕峰、刘永东、李美桃、杨帆、李双、王晶晶、王升国、种国双、高云龙、倪邦杰、乔思渊、赵春昊、成瑾、鲍旭华、马红丽、韩云、林冠辰、郭建领、李世勇、薛学琴、周永修、 韩杰、马国斌。

引　　言

人脸识别是一种基于人的面部特征信息进行身份识别的生物识别技术。在应用人脸识别技术后，采集到的人脸图像经过算法的处理得到人脸识别数据，进而实现更加准确高效的身份识别，提升应用单位的管理能力和业务水平。人脸识别应用场景广泛，但人脸识别应用安全制度还不完善，使应用单位人员的人脸识别数据和可能关联单位业务的系统面临安全风险。当政府部门、高新企业、科研院所等重点单位应用人脸识别技术时，建议特别关注安全问题。

政府部门、高新企业、科研院所等重点单位可参考本文件对人脸识别应用采取相应的安全技术和管理措施，保障人脸识别应用安全。

人脸识别应用安全评估指南

1 范围

本文件给出了评估人脸识别应用安全时涉及应用单位、人员安全、数据安全、系统安全和服务安全方面的建议。

本文件适用于人脸识别应用单位对人脸识别应用进行安全评估，也适用于人脸识别系统的规划、设计、建设和使用。

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 25069—2022 信息安全技术 术语

GB/T 38671—2020 信息安全技术 远程人脸识别系统技术要求

GB/T 41772—2022 信息技术 生物特征识别 人脸识别系统技术要求

GB/T 41819—2022 信息安全技术 人脸识别数据安全要求

3 术语和定义

GB/T 25069—2022、GB/T 41772—2022、GB/T 41819—2022 界定的以及下列术语和定义适用于本文件。

3.1

人脸图像 face image

自然人脸部信息的模拟表示或数字表示，也称人脸样本。

[来源:GB/T 41819—2022，3.1，有修改]

3.2

人脸特征 face feature

从人脸图像提取的反映对应数据主体特征，用于比对的数值或标记。

[来源:GB/T 41819—2022，3.2，有修改]

3.3

人脸识别数据 face recognition data

可识别自然人身份的人脸图像或人脸特征。

[来源:GB/T 41819—2022，3.3]

3.4

人脸识别数据控制者 data controller

有能力决定人脸识别数据处理目的、方式等的组织或个人。

3.5

人脸识别应用 face recognition application

使用人脸识别技术来确认特定自然人或特定自然人身份的过程。

3.6

应用单位 application unit

使用、控制人脸识别系统的组织。

3.7

用户 user

使用人脸识别产品或服务不具备特殊权限的个体，特指人脸识别数据主体。

3.8

系统用户 system user

能够对人脸识别系统进行特定操作，实现特定功能的人员。

注：系统用户指系统管理员、数据操作员和审计员等。

3.9

服务商 service provider

直接为应用单位提供或维护人脸识别产品/服务的组织。

注：服务商指供应商或集成商等。

4 人脸识别数据处理流程

人脸识别系统通常要经过采集人脸图像、提取人脸特征和存储人脸识别数据，人脸识别数据处理流程见图 1。最终，通过人脸识别数据的比对实现人脸识别功能。

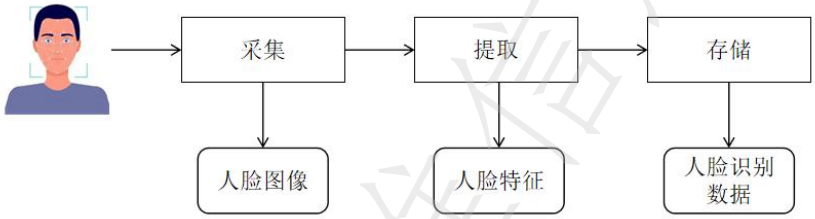

图 1 人脸识别数据处理流程

5 人脸识别应用安全评估内容

5.1 概述

人脸识别应用场景广泛，其安全风险主要源自人员、数据、系统和服务四个方面，应用单位需根据自身单位性质和业务特点，配备相应管理措施和技术手段。本文件主要为政府部门、高新企业、科研院所等应用单位的人脸识别应用开展安全评估提供指导，具体评估要点见参考附录 A。

5.2 应用单位

5.2.1 单位情况

明确应用单位的类型，可分为政府部门、高新企业、科研院所等。

设立安全管理部门，并明确组织架构、岗位和岗位人员数量，以用于防范和响应安全事件。

5.2.2 应用系统

记录应用单位范围内已部署的人脸识别系统数量及业务信息，能够独立部署运行且包含多个人脸识别相关业务的系统为 1 套。

明确每个人脸识别系统关联业务重要程度，可分为关键业务、重要业务、一般业务等。关键业务指涉及国家秘密的场所出入、人员授权验证等；重要业务指不涉及国家秘密，但与国家安全、经济发展、社会稳定，以及单位和公众利益密切相关的场所出入、人员授权验证等；一般业务不涉及国家秘密且不涉及敏感信息的相关场所出入、人员授权验证等。

明确人脸识别系统的应用场景，可分为单位管理、社会管理、行业应用等。单位管理指实现人员管理、安全防范等目的的应用场景，如签到打卡、智能监控、门禁闸机等；社会管理指政务、公共服务、交通等具有社会管理属性的应用场景；行业应用指利用人脸识别系统辅助金融、医疗、教育、娱乐等行业的应用场景。

5.2.3 应用人员

记录用户和系统用户重要程度，可分为重要人员、敏感人员和一般人员等。重要人员指涉及国家秘密的人员；敏感人员不涉及国家秘密，但与国家安全、经济发展、社会稳定，以及单位和公众利益密切相关的人员；一般人员不涉及国家秘密且不涉及敏感信息的人员。

记录授权同意使用人脸识别系统的用户数量，及用户同意使用人脸识别数据的目的、方式、范围等，公共安全等特殊场景除外。用户数量超过一定数量的，符合政府监管部门安全管理规定。

5.2.4 服务信息

记录已提供产品或服务的服务商数量、名称及服务期限。

5.2.5 管理制度

在人员分类和业务分类的基础上评估人脸识别应用优先级，可分为宜采用、可采用、不采用。宜采用指一般人员与一般业务；可采用指敏感人员与重要业务；不采用指重要人员与关键业务。

建立人脸识别应用安全管理制度，包括但不限于人员管理制度、数据管理制度、系统管理制度、服务管理制度。

5.3 人员安全

5.3.1 相关人员信息

应记录系统用户的相关信息，包括但不限于姓名、工号、部门、岗位。

5.3.2 人员安全管理措施

具备系统用户上岗培训安全管理措施，包括但不限于新员工符合岗位能力要求、签署安全责任书。

具备系统用户岗位交接安全管理措施，包括但不限于岗位交接材料范围。

具备系统用户离岗离职安全管理措施，包括但不限于终止访问权限、删除人脸识别数据、签署保密协议。

5.4 数据安全

5.4.1 人脸识别数据管理

明确人脸识别数据管理方式，可分为指定专门部门管理、委托服务商代管等。

明确用户提供的人脸识别数据关联个人信息的类型和数量。

5.4.2 人脸识别数据存储

明确人脸识别数据是否必要留存，如需留存，经数据主体单独同意或书面同意，并明确不同用户留存期限。

在使用人脸识别数据时，将人脸识别数据与其数据主体的其他个人信息去标识化和加密处理，并采用物理或逻辑隔离方式分别存储。在终止使用人脸识别数据时，将人脸识别数据与其数据主体的其他个人信息匿名化或删除处理。

明确应用单位人脸识别数据存储位置及运行方式，禁止人脸识别数据存储基础设施设在境外。存储位置及运行方式可分为单位所在地数据中心（单位自运行）、单位所在地数据中心（服务商运行）、远程数据中心（单位自运行）、远程专用数据中心（服务商运行）、远程公用数据中心（服务商运行）等。

明确人脸识别数据存储者、人脸识别数据控制者、人脸识别数据存储介质管理者等关键人员，并加强访问和权限管理。

5.4.3 人脸识别数据安全防护方式

明确人脸识别数据在采集、传输、存储等环节采取的安全防护方式，包括但不限于数据加密、数字签名、校验技术、脱敏技术。

5.5 系统安全

5.5.1 系统配置

根据业务功能需求，明确人脸识别系统的技术要求，包括但不限于识别精度、响应时间、识别阈值、活体检测阈值、使用距离和环境光线。

5.5.2 系统功能

除人脸识别方式外，系统宜有其他非人脸识别方式供选择来实现业务功能，并且不存在诱导用户选择倾向性。

系统具备查询、更正、删除人脸识别数据的功能，并提供必要的监管接口或日志查询功能。

系统在超出留存期限、用户离职、用户撤回同意授权等情况下，宜具备自动删除人脸识别数据的功能。

5.5.3 网络环境

明确人脸识别系统网络环境，特别是连接互联网情况。在连接互联网的情况下，人脸识别系统具备网络安全保护措施，包括但不限于访问控制、安全审计、边界完整性检查、入侵检测、恶意代码防护。

5.5.4 操作权限

明确服务商和系统用户的操作权限，并对系统用户进行技术培训，宜由系统用户对人脸识别数据进行操作。

5.5.5 安全检测

先依据 GB/T 41772、GB/T 38671 等相关标准检测评估后，再上线运行人脸识别系统。

5.5.6 使用审核记录

明确本单位人员和外单位人员使用人脸识别系统的审核制度，明确操作过程事前有审批、事中有监督、事后有归档。

建立系统上线部署、使用、更新升级、维修维护、废止（或终止）等审核制度，且记录完整，包括但不限于人员姓名、人员单位、使用开始时间、使用结束时间、使用目的。

5.6 服务安全

5.6.1 服务商能力

宜在计划应用人脸识别技术前评估服务商的相关能力，包括但不限于该技术的同类型成功应用案例、具备管理体系认证（如 ISO9001、ISO20000、ISO27000 等）、技术/产品规定的系统开发与供应链安全能力相关认证(如国家信息安全产品认证)、人脸识别相关的检验检测报告。

5.6.2 服务商责任/义务

在签署服务合同时，与服务商签署保密协议，明确保密事项、责任与义务。

宜明确其下级供应商采取必要的安全措施。

为应用单位提供有关安全措施的文档和信息，配合应用单位完成对数据和业务系统的管理。

宜对人脸识别系统进行配置管理，在系统生命周期内建立和维护人脸识别硬件、软件、文档等的基线配置和详细清单，并设置安全配置参数。

建立有效的审查和检查机制，实现对人脸识别服务的有效监管。

5.6.3 服务商现场服务记录

服务商在提供人脸识别系统安装、升级、维护等服务时，记录服务商现场服务内容。

5.6.4 退出服务/更换服务商

在退出服务或更换服务商时，服务商交还的材料范围，包括但不限于人脸识别数据、服务中产生和收集的数据/文件、程序代码、技术资料、运行日志。

附 录 A
（资料性）
人脸识别应用安全评估表格

人脸识别应用安全评估具体评估要点可参考表 A.1 至表 A.9。

表 A.1 应用单位基本情况记录表

应用单位情况	1. 单位类型： ☐政府部门 ☐高新企业 ☐科研院所 ☐其他 2. 是否设立人脸识别应用管理部门： ☐是 ☐否 3. 是否明确组织架构、岗位和岗位人员数量： ☐是 ☐否 4. 单位范围内应用人脸识别系统的数量：____套，每套人脸识别系统情况见表 A.2 5. 业务重要程度及数量：_____. 6. 应用场景及数量：_____. 7. 用户重要程度及数量：_____. 8. 系统用户重要程度及数量：_____. 9. 授权使用人脸识别系统的用户数量：_____. 10. 用户同意使用人脸识别数据的目的、方式和范围： _____. 11. 服务商数量：____家 12. 服务商名称及服务期限：_____. 13. 是否建立人脸识别应用安全管理制度： ☐是 ☐否

表 A.2　人脸识别系统记录表

系统编号	
系统名称	
版本号	
数据规模	
主管部门	
应用场景	
业务重要程度及数量	
用户重要程度及数量	
系统用户重要程度及数量	
系统部署位置	
数据存储位置	
网络环境	
服务商名称	
上线运行时间	
系统软件升级频率	
系统硬件升级频率	
系统软件操作 时间、人员及方式	
系统硬件操作 时间、人员及方式	

表 A.3　人员安全记录表

人员安全	1.　是否记录系统用户的学历、专业信息、证书、项目和培训经历： ☐是，人员信息情况见表 A.4 ☐否 2.　是否明确系统用户上岗培训安全管理措施： ☐是，采取的管理措施：_____. ☐否 3.　是否明确系统用户岗位交接安全管理措施： ☐是，采取的管理措施：_____. ☐否 4.　是否明确系统用户离岗离职安全管理措施： ☐是，采取的管理措施：_____. ☐否

表 A.4 人员信息记录表

员工姓名	
工号	
部门	
岗位	
学历	
专业	
证书	
职称	
入职时间	
离职时间	
项目经历	
培训经历	

表 A.5　数据安全记录表

数据安全	1.　人脸识别数据管理方式： ☐指定专门部门管理 ☐委托服务商代管 ☐其他 2.　人脸识别数据关联个人信息的类型和数量：_____.　　. 3.　是否需要留存人脸识别数据： ☐是，数据主体是否单独同意或书面同意：_____.不同用户留存期限：_____. ☐否 4.　在使用人脸识别数据时，是否将人脸识别数据与其数据主体的其他个人信息去标识化和加密 处理，并采用物理或逻辑隔离方式分别存储： ☐是 ☐否 5.　在终止使用人脸识别数据时，是否将人脸识别数据与其数据主体的其他个人信息匿名化或删 除处理： ☐是 ☐否 6.　人脸识别数据存储位置及运行方式（可多选）： ☐单位所在地数据中心（单位自运行） ☐单位所在地数据中心（服务商运行） ☐远程数据中心（单位自运行） ☐远程专用数据中心（服务商运行） ☐远程公用数据中心（服务商运行） ☐其他　. 7.　是否明确人脸识别数据存储者、人脸识别数据控制者、人脸识别数据存储介质管理人员，并 加强访问和权限管理： ☐是 ☐否 8.　是否明确人脸识别数据安全防护方式： ☐是，人脸识别数据安全防护方式：_____. ☐否

表 A.6　系统安全记录表

系统安全	1.　是否明确人脸识别系统技术要求： ☐是，技术要求：_____. ☐否 2.　除人脸识别方式外，系统是否可选择其他非人脸识别方式供选择来实现业务功能，并且不存 在诱导用户选择倾向性： ☐是 ☐否 3.　系统是否具备查询、更正、删除人脸识别数据的功能，并提供必要的监管接口或日志查询功 能： ☐是 ☐否 4.　在超出留存期限、用户离职、用户撤回同意授权等情况，系统是否具备及时删除人脸识别数 据的功能： ☐是 ☐否 5.　系统是否连接互联网： ☐是，网络安全保护措施：_____. ☐否 6.　是否明确服务商和系统用户的操作权限： ☐是 ☐否 7.　系统上线前是否经过 GB/T 41772，GB/T 38671 等相关标准检测评估： ☐是 ☐否 8.　是否明确本单位人员使用人脸识别系统的审核制度： ☐是，人脸识别系统使用记录见表 A.7 ☐否 9.　是否明确外单位人员使用人脸识别系统的审批制度： ☐是 ☐否 10.　是否建立人脸识别系统上线部署、使用、更新升级、维护维修、废止（或终止）等审核制度： ☐是 ☐否

表 A.7　人脸识别系统使用记录表

系统编号	
系统名称	
主管部门	
使用人员姓名	
人员单位	
使用开始时间	
使用结束时间	
使用内容	

表 A.8　服务安全记录表

服务安全	1.　是否明确服务商及服务商的基本信息： □是，　服务商情况见表 A.9 □否 2.　是否在应用人脸识别系统前评估服务商的相关能力： □是 □否 3.　是否明确服务商针对提供的服务签署保密协议： □是 □否 4.　是否明确下级供应商采取必要的安全措施： □是 □否 5.　是否为应用单位提供有关安全措施的文档和信息，配合应用单位完成对数据和业务系统的管 理： □是 □否 6.　是否对人脸识别系统进行配置管理，在系统生命周期内建立和维护人脸识别硬件、软件、文 档等的基线配置和详细清单，并设置安全配置参数： □是 □否 7.　是否建立有效的审查、检查机制，实现对人脸识别服务的有效监管： □是 □否 8.　服务商在提供人脸识别系统安装、升级、维护等服务时，是否有服务商现场服务记录： □是 □否 9.　在退出服务或更换服务商时，服务商应该移交的材料范围（可多选）： □人脸识别数据 □服务中产生和收集的数据、文件 □程序代码 □技术资料 □运行日志 □其他___.

表 A.9　服务商信息记录表

服务商名称	
合同编号	
服务内容	
服务记录	
服务商能力	