ICS 35.240.01
I6440

T/WHCSA 009—2026

团 体 标 准

网络安全产品和服务认定规范

Specifications for the Recognition of Network Security Products and Services

2026-7-22 发布 2026-7-31 实施

武汉市网络安全协会 发布

目录

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》起草。

本标准旨在规范武汉市行政区域内网络安全产品的技术合规性与服务的专业能力认定，明确产品质量底线与服务交付标准，为企业选择网络安全解决方案、政府开展产业监管提供依据，推动网络安全产业从 “合规驱动” 向 “价值驱动 + 技术驱动” 升级。

编制过程中，严格遵循《团体标准管理规定》（国标委联〔2019〕1号）、《中华人民共和国标准化法》《中华人民共和国网络安全法》等法规，参考 GB/T 25067-2020《信息技术 安全技术 信息安全管理体系审核和认证机构要求》、GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》、中国网络安全审查技术与认证中心（CCRC）信息安全服务资质认证规范等标准，吸纳网络安全产品研发企业、服务提供商、检测机构、终端用户及政府监管部门意见，确保技术要求不低于强制性国家标准，兼顾产业前沿性与落地可操作性。

本标准与现有国家标准、行业标准无冲突，可作为武汉市网络安全产品入市合规审查、服务能力评估的核心依据。

本标准由武汉市网络安全协会提出并归口。

主要起草单位：武汉市网络安全协会、武汉市企业科技创新服务中心、湖北省双新融合成果转化中心、武汉企业信息化促进会、武汉大学国家网络安全学院、华中科技大学网络空间安全学院、网络空间安全学院、湖北大学网络空间安全学院、武汉轻工大学、武汉软件工程职业学院（武汉开放大学）、中金数据（武汉）超算技术有限公司、中国电信股份有限公司武汉分公司、武汉市德发电子信息有限责任公司、武汉地铁桥隧管理有限公司、武汉安天信息技术有限责任公司、奇安信网神信息技术（北京）股份有限公司、深信服科技股份有限公司、武汉安恒信息科技有限公司、神州绿盟武汉科技有限公司、北京启明星辰信息安全技术有限公司、智网安云（武汉）信息技术有限公司、武汉光谷信息技术股份有限公司、武汉数安科技发展有限公司、武汉汉融通数智科技有限公司、武汉网络安全技术有限公司、武汉金信润天信息技术有限公司、上海三零卫士信息安全有限公司、武汉武创通科技服务有限公司、武汉云视科技技术有限公司、中国联合网络通信有限公司湖北省分公司、武汉世跃专利代理事务所（普通合伙）等。

主要起草人：刘悦恒、乔奇、张玉萍、祝志华、陈曼、刁雪晨、赵波、徐笛、李可、何鹏、张帆、王文博、李亚妨、王俊华、顾达强、孟懿璐、杨杭杭、潘宣辰、李迎雪、卢雨、崔镇麒、张吉浩、聂良金、毕非凡、朱琪、宋齐伟、蔡志鹏、李振瑞、丁勇、邓方鸣、张杰、蔡镝、李英、林千帆、万仲达、赵文祥、严媛、周怡、何溪山等。

网络安全产品和服务认定规范

1 范围

本标准规定了网络安全产品与服务的分类、认定条件、评估方法、认定流程及后续监督管理要求。

本标准适用于中国境内从事网络安全产品研发、生产、销售的企业，以及提供网络安全服务的机构（含在武汉市设有分支机构的外地企业/机构）所涉产品与服务的认定。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件；凡是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 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

GB/T 25067-2020 信息技术 安全技术 信息安全管理体系审核和认证机构要求

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求

GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 25066-2020 信息安全技术 信息安全产品类别与代码

GB/T 4754-2017 国民经济行业分类（含第1号修改单）

CCRC《信息安全服务资质认证规范》（2024版）

GA/T 2182-2024 关键信息基础设施安全测评要求

3 术语和定义

下列术语和定义适用于本文件。

3.1 网络安全产品

具备网络安全防护、检测、响应、恢复等核心功能，用于保障网络设施、数据、应用安全的硬件设备、软件系统或软硬一体化解决方案，通过防火墙、入侵检测、数据加密等技术手段，构建"预防-监测-响应-恢复"的动态防护体系，包括但不限于防火墙、数据防泄漏（DLP）系统、入侵检测/防御系统（IDS/IPS）等。

3.2 网络安全服务

通过技术与管理手段，系统性地保护网络系统的硬件、软件及数据免受攻击、破坏或泄露的一系列措施，核心目标是保障信息的机密性、完整性、可用性，确保网络服务连续可靠运行。不仅应对黑客入侵、病毒传播等传统威胁，也涵盖数据防泄露、合规审计、应急响应等现代安全需求，包括但不限于安全集成、风险评估、渗透测试、应急响应、安全运维等。

3.3 产品认定

依据本标准，对网络安全产品的技术合规性、功能完整性、性能稳定性及兼容性进行评估，确认其

是否符合安全标准的活动。

3.4 服务认定

依据本标准，对网络安全服务的流程规范性、人员专业性、交付质量及风险管控能力进行评估，确认其服务能力的活动。

3.5 认定证书

由武汉市网络安全协会颁发，证明网络安全产品符合技术标准或服务达到相应能力的规范性文件。

4 网络安全产品与服务分类

网络安全产品与服务分类					
大类	**一级分类**	**二级分类**	**三级分类**	**代码**	**形态**
产品	P1 物理环境安全	P1.1 环境安全	区域防护	P1.1.1	产品
			灾难防范与恢复	P1.1.2	产品
			容灾恢复计划辅助支持	P1.1.3	产品
			电磁干扰	P1.1.4	产品
			抗电磁干扰	P1.1.5	产品
			电磁泄漏防护	P1.1.6	产品
		P1.2 物理安全	防盗	P1.2.1	产品
			防毁	P1.2.2	产品
			防线路截获	P1.2.3	产品
			电源保护	P1.2.4	产品
			介质安全	P1.2.5	产品
			物理访问控制（门禁/生物识别）	P1.2.6	产品
			安防监控与入侵报警	P1.2.7	产品
	P2 通信网络安全	P2.1 通信安全	虚拟专用网（VPN）	P2.1.1	产品
			通信加密（含密码模块）	P2.1.2	产品
		P2.2 网络监测与控制	网络入侵检测（IDS）	P2.2.1	产品
			网络活动监测与分析	P2.2.2	产品
			流量控制	P2.2.3	产品
			上网行为管理	P2.2.4	产品
			反垃圾邮件	P2.2.5	产品
			信息过滤	P2.2.6	产品
			网络检测与响应（NDR/NTA）	P2.2.7	产品
	P3 区域边界安全	P3.1 隔离	终端隔离	P3.1.1	产品
			网络隔离	P3.1.2	产品
			网络单向导入	P3.1.3	产品
			安全隔离与信息交换系统（网闸，含高性能）	P3.1.4	产品
		P3.2 入侵防范	网络入侵防御（IPS）	P3.2.1	产品
			网络恶意代码防范	P3.2.2	产品
			抗拒绝服务攻击（Anti-DDoS）	P3.2.3	产品
		P3.3 边界访问控制	防火墙	P3.3.1	产品
			安全路由器	P3.3.2	产品

网络安全产品与服务分类					
大类	**一级分类**	**二级分类**	**三级分类**	**代码**	**形态**
			安全交换机	P3.3.3	产品
			下一代防火墙（NGFW）/防水墙	P3.3.4	产品
			统一威胁管理（UTM）	P3.3.5	产品
		P3.4 接入安全	终端接入控制（NAC）	P3.4.1	产品
			零信任访问（ZTA）	P3.4.2	产品
	P4 计算环境安全	P4.1 计算环境防护	可信计算	P4.1.1	产品
			身份鉴别（主机）	P4.1.2	产品
			主机入侵检测	P4.1.3	产品
			主机访问控制	P4.1.4	产品
			主机型防火墙	P4.1.5	产品
			终端使用安全	P4.1.6	产品
			移动存储设备安全管理	P4.1.7	产品
		P4.2 防恶意代码	主机恶意代码防治（防病毒软件）	P4.2.1	产品
			防病毒网关（含高性能）	P4.2.2	产品
			网络病毒监控（VDS）	P4.2.3	产品
			终端检测与响应（EDR）	P4.2.4	产品
		P4.3 操作系统安全	安全操作系统	P4.3.1	产品
			操作系统安全部件	P4.3.2	产品
		P4.4 应用安全防护	身份鉴别（应用）	P4.4.1	产品
			WEB 应用防火墙（WAF）	P4.4.2	产品
			邮件安全防护	P4.4.3	产品
			网站恢复	P4.4.4	产品
			应用安全加固	P4.4.5	产品
			API 安全	P4.4.6	产品
			内容安全（违法信息及行为监测管理）	P4.4.7	产品
		P4.5 应用安全支持	业务流程监控	P4.5.1	产品
			源代码审计	P4.5.2	产品
			网站监测	P4.5.3	产品
			应用软件安全管理	P4.5.4	产品
			应用代理	P4.5.5	产品
			负载均衡	P4.5.6	产品
			数字签名	P4.5.7	产品
		P4.6 数据安全防护	数据加密	P4.6.1	产品
			数据泄露防护（DLP）	P4.6.2	产品
			数据脱敏	P4.6.3	产品
			数据清除	P4.6.4	产品
			数据备份与恢复	P4.6.5	产品
			数据防拷贝	P4.6.6	产品
		P4.7 数据平台安全	安全数据库	P4.7.1	产品
			数据库安全部件	P4.7.2	产品
			数据库防火墙	P4.7.3	产品

网络安全产品与服务分类					
大类	**一级分类**	**二级分类**	**三级分类**	**代码**	**形态**
			数据库审计	P4.7.4	产品
	P5 安全管理支持	P5.1 综合审计	安全审计	P5.1.1	产品
			日志审计	P5.1.2	产品
			网络审计	P5.1.3	产品
		P5.2 应急响应支持	应急响应辅助系统	P5.2.1	产品
		P5.3 密码管理	密码设备（密码机/密码模块）	P5.3.1	产品
			公钥基础设施（PKI）	P5.3.2	产品
			签名验签服务器与电子签章	P5.3.3	产品
			密钥管理系统	P5.3.4	产品
			安全智能卡与认证令牌	P5.3.5	产品
		P5.4 风险评估与处置	系统风险评估	P5.4.1	产品
			安全性检测分析（含安全测试仪表）	P5.4.2	产品
			配置核查	P5.4.3	产品
			漏洞挖掘	P5.4.4	产品
			态势感知	P5.4.5	产品
			高级持续威胁检测（APT）	P5.4.6	产品
			舆情分析	P5.4.7	产品
			漏洞扫描与补丁管理	P5.4.8	产品
		P5.5 安全管理	安全管理平台（SOC）	P5.5.1	产品
			安全监控	P5.5.2	产品
			运维安全管理（堡垒机）	P5.5.3	产品
			统一身份鉴别与授权（4A）	P5.5.4	产品
			安全编排自动化与响应（SOAR）	P5.5.5	产品
			威胁情报平台（TIP）	P5.5.6	产品
	P6 其他网络安全产品	P6.1 工业控制系统安全产品	工控防火墙/工控 IDS/PLC 安全	P6.1.1	产品
		P6.2 移动安全产品	移动设备/应用管理与威胁防御（MDM/MAM/MTD）	P6.2.1	产品
		P6.3 办公与外设安全产品	打印/刻录安全、安全数据摆渡	P6.3.1	产品
		P6.4 其他未列明产品	其他网络安全专用产品（动态维护）	P6.4.1	产品
服务	S1 安全运维与监测服务	S1.1 网络安全运维服务		S1.1	服务
		S1.2 网络安全监测服务（安全托管/MSS）		S1.2	服务
	S2 安全应急与恢复服务	S2.1 应急响应服务		S2.1	服务
		S2.2 灾难备份与恢复服务		S2.2	服务
	S3 安全评估与审计服务	S3.1 风险评估服务		S3.1	服务
		S3.2 安全测试服务（渗透测试/等级测评）		S3.2	服务
		S3.3 安全配置核查服务		S3.3	服务
		S3.4 安全审计服务		S3.4	服务

网络安全产品与服务分类					
大类	**一级分类**	**二级分类**	**三级分类**	**代码**	**形态**
	S4 安全咨询与规划服务	S4.1 安全管理咨询		S4.1	服务
		S4.2 安全规划服务		S4.2	服务
	S5 安全培训服务	S5.1 安全意识培训		S5.1	服务
		S5.2 安全技能培训		S5.2	服务
	S6 安全集成服务	S6.1 安全集成总包		S6.1	服务
		S6.2 安全集成实施（安全防护系统集成）		S6.2	服务
	S7 数据安全与个人信息保护服务	S7.1 数据安全评估与治理服务		S7.1	服务
		S7.2 个人信息保护合规服务（PIPL）		S7.2	服务
	S8 软件安全开发服务	S8.1 安全开发生命周期（SDL）与代码安全服务		S8.1	服务
		S8.2 安全软件外包服务		S8.2	服务
	S9 网络安全众测与攻防演练服务	S9.1 安全众测		S9.1	服务
		S9.2 红蓝对抗与攻防演练		S9.2	服务
	S10 网络安全产品流通服务	S10.1 总代理与分销		S10.1	服务
		S10.2 批发		S10.2	服务
		S10.3 零售		S10.3	服务
	S11 其他网络安全服务	S11.1 其他未列明网络安全服务（动态维护）		S11.1	服务
新兴融合	E1 人工智能安全	E1.1 人工智能系统自身安全（算法/模型/数据/生成内容安全）		E1.1	产品/服务（双形态）
		E1.2 人工智能赋能安全（安全大模型/智能威胁检测）		E1.2	产品/服务（双形态）
		E1.3 人工智能基础设施安全（算力/训练框架/模型仓库）		E1.3	产品/服务（双形态）
	E2 云计算与边缘计算安全	E2.1 云工作负载保护（CWPP）		E2.1	产品/服务（双形态）
		E2.2 云安全态势管理（CSPM）		E2.2	产品/服务（双形态）
		E2.3 云身份与访问管理（CIAM）		E2.3	产品/服务（双形态）
		E2.4 边缘计算安全		E2.4	产品/服务（双形态）
	E3 大数据安全与隐私计算	E3.1 数据脱敏与隐私计算（联邦学习/可信执行环境/多方安全计算）		E3.1	产品/服务（双形态）
		E3.2 数据流通安全（数据共享/交易/出境）		E3.2	产品/服务（双形态）
	E4 物联网安全	E4.1 物联网设备/终端安全		E4.1	产品/服务（双形态）
		E4.2 物联网通信与平台安全		E4.2	产品/服务（双形态）

网络安全产品与服务分类					
大类	**一级分类**	**二级分类**	**三级分类**	**代码**	**形态**
	E5 工业互联网安全（工控安全）	E5.1 工业控制系统安全		E5.1	产品/服务（双形态）
		E5.2 工业互联网平台与数据安全		E5.2	产品/服务（双形态）
	E6 车联网（智能网联汽车）安全	E6.1 车端（车载系统）安全		E6.1	产品/服务（双形态）
		E6.2 V2X 通信安全		E6.2	产品/服务（双形态）
		E6.3 车联网平台安全		E6.3	产品/服务（双形态）
		E6.4 自动驾驶数据安全		E6.4	产品/服务（双形态）
	E7 区块链安全	E7.1 区块链平台安全		E7.1	产品/服务（双形态）
		E7.2 智能合约与应用安全		E7.2	产品/服务（双形态）
	E8 卫星互联网（低轨星座）安全	E8.1 星地/星间通信安全		E8.1	产品/服务（双形态）
		E8.2 星载系统与地面站（测控）安全		E8.2	产品/服务（双形态）
	E9 5G/6G 与新型通信网络安全	E9.1 网络切片/边缘计算/Open RAN 安全		E9.1	产品/服务（双形态）
	E10 量子安全	E10.1 量子密钥分发（QKD）安全		E10.1	产品/服务（双形态）
		E10.2 抗量子密码（PQC）迁移		E10.2	产品/服务（双形态）
	E11 网络安全公共服务	E11.1 威胁情报与漏洞共享平台		E11.1	产品/服务（双形态）
		E11.2 安全众测/靶场/实训平台		E11.2	产品/服务（双形态）
		E11.3 态势感知公共服务平台		E11.3	产品/服务（双形态）
		E11.4 互联网公共安全服务平台		E11.4	产品/服务（双形态）
	E12 其他新兴融合安全	E12.1 其他未列明新兴融合安全（动态维护）		E12.1	产品/服务（双形态）

5 产品认定条件

5.1 基本条件（所有类别产品通用）

5.1.1 合规性要求

列入《网络安全专用产品目录》的产品，需已取得安全专用产品销售许可或完成国家网信办备案认

证；未列入目录的产品，需提供具备 CMA/CNAS 资质的机构出具的安全检测报告。

涉及个人信息处理的产品，需符合 GB/T 35273-2020《个人信息安全规范》，不违规收集、存储用户信息。

5.1.2 知识产权要求

产品核心技术拥有自主知识产权（发明专利、实用新型专利或软件著作权），无知识产权纠纷。

若包含开源组件，需提供开源协议合规说明，确保无开源许可冲突。

5.1.3 测试验证要求

提供具备相关资质的机构出具的产品测试报告，报告需涵盖功能、性能、兼容性及安全性检测。

测试报告关键指标（如吞吐量、时延、误报率）应达到对应分类的技术要求。

6 服务认定条件

6.1 基本条件（所有类型服务通用）

6.1.1 资质要求

服务提供方需为依法设立的企业法人，注册地在武汉市或在武汉市设有分支机构（分支机构需提供总公司或全资子公司授权书）；外地企业在武汉设立的分支机构，持总公司授权书及武汉本地经营场所证明，可申请认定。

营业执照经营范围需包含网络安全相关服务内容，并具备对应服务类别的基础资质。

6.1.2 人员资质要求

本标准所称相关资质，指注册信息安全专业人员（CISP）、网络安全等级测评师、CCRC 信息安全服务资质认证人员等行业公认的网络安全类职业资格证书。

6.1.3 流程要求

建立标准化的服务流程文档，包括服务方案设计、实施计划、质量管控、交付验收、售后支持等环节。

服务流程需符合 CCRC《信息安全服务资质认证规范》或对应行业服务标准，关键环节（如渗透测试、应急响应）需有明确操作规范。

6.1.4 工具与资源要求

配备服务所需的专业工具（如渗透测试工具、漏洞扫描工具、应急响应设备），工具需经第三方验证或具备厂商授权。

开源安全工具不受厂商授权限制，但服务提供方需确保所用版本稳定、无已知高危漏洞，且具备自主研判工具结果的技术能力。

建立服务资源池（如威胁情报库、漏洞库、应急响应预案模板），且资源定期更新。

6.2 核心条件（按服务类型）

6.2.1 安全运维与监测服务

人员要求：运维/监测团队实行 7×24 小时服务制，团队中持相关资质的人员占比不低于 30%或不少于 5 人，运维工程师需具备 2 年以上安全设备运维经验。

响应能力：常规运维问题响应时间不超过 1 小时，故障修复时间不超过 4 小时。

运营质量：安全事件检出率不低于 95%、误报率不超过 5%，每月出具安全运维/监测报告。

6.2.2 安全应急与恢复服务

人员要求：核心成员需持相关资质，且参与过不少于 2 次重大安全事件处置。

响应速度：本地应急响应 1 小时内抵达现场，远程应急响应 30 分钟内启动，重大事件（如数据泄露、勒索病毒）处置方案在 2 小时内出具。

处置效果：事件溯源准确率不低于 90%，系统恢复时间不超过 24 小时，处置后 3 个月内无同类事件复发，提供完整的处置报告与加固建议。

6.2.3 安全评估与审计服务

人员要求：评估/审计团队中，持相关资质的人员占比不低于 30%或不少于 5 人，核心评估人员需具备 3 年以上安全评估经验。

技术能力：风险评估需覆盖资产识别、威胁分析、脆弱性扫描、风险计算全流程；安全测试需支持 Web、移动应用、内网等多场景；安全审计需覆盖配置核查、合规审计等。

报告要求：评估/审计报告需包含详细问题描述、风险等级划分、修复建议及验证方案，用户无重大异议。

6.2.4 安全咨询与规划服务

人员要求：咨询顾问需持相关资质，且具备 3 年以上安全咨询或安全管理经验。

方案能力：能根据用户业务场景（如政府、金融、工业）定制安全规划方案，方案需包含风险评估、架构设计、实施路径及预算，提供 2 个及以上定制方案案例。

交付要求：咨询项目验收合格率 100%，交付文档完整率 100%。

6.2.5 安全培训服务

人员要求：培训讲师需持 CISP（注册信息安全专业人员）或同等级别网络安全类职业资格证书，且具备至少 1 年网络安全培训授课经验。

课程要求：培训内容需覆盖安全意识、安全技能等模块，具备标准化的课程体系、教材和考核方案。

培训效果：学员考核通过率不低于 85%，提供培训效果评估报告。

7 评估方法

7.1 通则

本认定为符合性基础认定。申请材料真实有效，满足本标准全部基本条件及对应类别核心要求的，即认定通过，认定结论为"通过"或"不通过"，不设等级、不做打分评估。

7.2 产品评估方法

文档审查（10 个工作日）：协会组织专家核查申请材料，包括产品技术手册、测试报告、知识产权证明、应用案例等，确认是否符合认定条件。

现场验证（5 个工作日）：材料存疑、收到实名举报或属于重点监管品类的产品，可组织专家赴用户现场核查产品部署与使用情况。

检测报告采信规则：申请方已提供具备 CMA/CNAS 资质的第三方机构出具的有效测试报告，且产品型号、版本与申请事项一致的，原则上不重复开展实验室测试；仅对材料存疑、有投诉举报或属于重点监管品类的产品，开展抽样复测。

综合评估（5 个工作日）：专家结合文档审查、现场验证（如有）及第三方检测报告采信结果，形成最终评估结论。

7.3 服务评估方法

材料审查（10 个工作日）：协会组织服务专家核查申请材料，确认流程规范性与资质有效性。

客户回访（1 个工作日）：提供 3 至 5 个过往服务客户所填写的服务满意度调查（含交付及时性、问题解决效果等）。

现场核查（5 个工作日）：材料存疑、收到实名举报或属于重点监管的服务类型，可赴服务提供方现场核查流程运行情况。

综合评估（5 个工作日）：专家结合上述材料综合评定，形成最终评估结论。

8 认定流程

8.1 申请受理

8.1.1 申请材料（产品认定）

a）《网络安全产品认定申请书》（附录 A）；

b）企业营业执照副本复印件（加盖公章），分支机构附总公司授权书；

c）产品技术手册（含功能说明、性能参数、部署要求）；

d）第三方检测机构出具的产品测试报告（CMA/CNAS 资质）；

e）产品知识产权证明（专利证书、软件著作权登记证书）；

f）产品安全专用产品认证/备案证明（如适用）；

g）产品应用案例（含合同关键页、用户使用报告）；

h）其他补充材料（如产品获奖证明、标准参编证明）。

8.1.2 申请材料（服务认定）

a）《网络安全服务认定申请书》（附录 B）；

b）企业营业执照副本复印件（加盖公章），分支机构附总公司授权书；

c）服务资质证书复印件（如 CCRC、等保测评等资质）；

d）服务流程文档（含服务规范、操作手册、质量管控方案）；

e）服务团队人员名单及人员资质证书复印件；

f）过往服务项目合同关键页、交付报告、用户满意度证明；

g）服务工具清单及授权证明（如厂商授权书、工具检测报告）；

h）其他补充材料（如服务获奖证明、标准参编证明）。

8.1.3 受理时限

武汉市网络安全协会常年受理申请，企业按认定通知要求报送纸质及电子版材料至协会秘书处。

收到材料后 5 个工作日内完成形式审查：材料齐全且符合要求的，出具《受理通知书》；材料不齐的，一次性告知需补正内容；材料不符合基本要求的，出具《不予受理通知书》。

8.2 评估实施

8.2.1 产品评估流程

a）文档审查（10 个工作日）：协会组织技术专家核查申请材料，确认技术合规性与材料完整性，出具《文档审查意见》；

b）现场验证（5 个工作日）：对材料存疑、收到实名举报或重点监管的产品，组织专家赴用户现场核查产品部署与使用情况，出具《现场验证报告》；

c）综合评估（5 个工作日）：专家结合文档审查、现场验证结果，形成《产品评估报告》。

8.2.2 服务评估流程

a）材料审查（10 个工作日）：协会组织服务专家核查申请材料，确认流程规范性与资质有效性，出具《文档审查意见》；

b）客户回访（1 个工作日）：提供过往客户满意度反馈；

c）现场核查（5 个工作日）：对材料存疑、收到实名举报或重点监管的服务，赴服务提供方现场核查流程运行情况，出具《现场核查报告》；

d）综合评估（5 个工作日）：专家结合上述材料综合评定，形成《服务评估报告》。

8.3 认定决定与公示

8.3.1 认定审议

协会组织评审委员会（技术专家不少于 3 人、服务专家不少于 2 人），审议《产品评估报告》或《服务评估报告》，确定初步认定结果。

8.3.2 公示

初步认定结果在协会官网公示 7 个工作日，公示内容包括申请企业名称、产品/服务名称。公示期内接受异议，异议人需提交书面异议材料及相关证明。

8.3.3 异议处理

协会在收到异议后 5 个工作日内受理，组织专家核查异议内容。

15 个工作日内出具《异议处理结果》：异议成立的，重新评估；异议不成立的，维持初步认定结果。涉及复杂技术核查的异议，可延长 10 个工作日。

8.4 证书颁发

8.4.1 证书内容

产品认定证书：含企业名称、产品名称、产品类别、证书编号（武网安协产认〔年份〕第 XX 号）、有效期、发证机构，格式见附录 C-1。

服务认定证书：含企业名称、服务类别、证书编号（武网安协服认〔年份〕第 XX 号）、有效期、发证机构，格式见附录 C-2。

8.4.2 证书有效期

认定证书有效期为 2 年，有效期满前 3 个月，企业可申请复评。

产品/服务核心信息（如产品型号、服务范围）变更的，需在变更后 30 日内申请证书变更。

9 监督管理

9.1 年度核查

9.1.1 核查对象

所有持有有效认定证书的产品与服务提供方。

9.1.2 核查内容

产品核查：产品技术指标是否持续符合标准、是否存在安全漏洞未修复、用户投诉情况。

服务核查：服务流程是否持续规范、人员资质是否有效、交付质量是否达标、用户满意度情况。

9.1.3 核查方式

按自然年度开展年度核查。持证企业每年 4 月 30 日前提交《年度核查报告》（含产品更新情况/服务项目总结、用户反馈、合规证明）。逾期未提交年度报告的，责令 15 日内补报。

协会随机抽取 20%的认定对象进行现场核查，或委托第三方机构进行抽样测试。

9.1.4 核查结果

合格：持续符合认定条件，保留认定。

整改：存在轻微不符合项，责令 3 个月内整改，整改合格保留认定。

不合格：存在重大不符合项（如产品出现高危漏洞未修复、服务出现重大质量问题），暂停认定资格。逾期仍未补报年度报告或年度检查不合格的，暂停认定资格，责令 3 个月内整改；连续两年未参加年度检查或整改后仍不合格的，撤销认定证书。

9.2 复评

9.2.1 复评申请

证书有效期满前 3 个月，企业提交复评申请及最新材料（同初次申请，新增"有效期内产品/服务运行总结"）。有效期内无违规、无重大变更的企业，复评时可简化材料、免于现场核查。

9.2.2 复评流程

同初次认定流程（申请受理→评估实施→认定决定→公示），复评重点核查产品/服务的持续改进情况与合规性。

9.2.3 复评结果

通过：换发新证书，有效期重新计算 2 年。

未通过：撤销认定资格，收回原证书。

9.3 证书撤销

出现下列情形之一的，协会撤销认定证书并公告：

a）申请认定时提供虚假材料（如伪造测试报告、资质证书）的，撤销证书，3 年内不得重新申请；

b）产品出现重大安全漏洞，未在规定时间内修复，造成用户损失的，撤销证书，3 年内不得重新申请；

c）服务出现重大质量问题，引发用户投诉且未妥善处理，造成恶劣影响的，撤销证书，3 年内不得重新申请；

d）连续 2 年未参加年度核查或年度核查不合格的，撤销证书，3 年内不得重新申请；

e）违反《网络安全法》《数据安全法》等法律法规，被监管部门处罚的，撤销证书，3 年内不得重新申请；

f）企业主动申请撤销认定的，撤销证书；

g）一般违规整改后再犯的，撤销证书。

附录 A

（规范性附录）

网络安全产品认定申请书格式

网络安全产品认定申请书

填 写 须 知

1. 本申请书填写应准确、完整，不得涂改。
2. 所有材料均需加盖申请单位公章。
3. 申请材料以 A4 纸打印并装订成册。
4. 申请书及相关材料不予退还，请自行留存底稿。

一、企业基本信息

项　目	内　容
企业名称	
统一社会信用代码	
注册地址	
经营地址	
法定代表人	姓名：_____　职务：_____　办公电话：_____　手机：_____　邮箱：_____
申报联系人	姓名：_____　职务：_____　办公电话：_____　手机：_____　邮箱：_____
成立日期	_____年____月____日
企业类型	□国有企业　□民营企业　□外资企业　□合资企业　□其他（请注明_____）
是否上市	□是　□否
股票代码	
分支机构情况	□有　□无（如有，填写武汉分支机构的名称及经营地址：_____，_____）

二、产品基本信息

项　目	内　容
产品名称	
产品型号	
产品版本	
研发完成时间	
是否取得安全专用产品认证/备案	□是　□否
产品核心功能描述	

三、知识产权与测试情况

项　目	内　容	备　注
知识产权类型	专利（☐实用新型　☐发明　☐外观）　☐软件著作权　☐其他证书：_____	
知识产权名称		
知识产权编号/登记号		
第三方检测机构名称(须具备相关资质）		
第三方检测报告编号		
测试结论	☐合格　☐不合格　☐未进行第三方检测（请说明原因：_____）	
测试完成时间		
关键安全指标	（示例：漏洞类核心指标、安全合规类指标、访问控制类指标、攻防对抗类指标、数据与传输安全类指标、运行安全类指标、测试过程质量指标）	
提供知识产权的名称,证书附后	（例如测评证书、著作权证书、专利证书等）	
产品密码检测证书（如适用）		/

四、申请认定类型（单选）

☐物理环境安全：_____（如：区域防护、电磁泄漏防护等）

☐通信网络安全：_____（如：虚拟专用网、网络入侵检测等）

☐区域边界安全：_____（如：防火墙、网络隔离、抗拒绝服务攻击等）

☐计算环境安全：_____（如：数据加密、WEB 应用防火墙、安全数据库等）

☐安全管理支持：_____（如：态势感知、安全管理平台、安全审计等）

☐人工智能安全：_____（如：人工智能应用安全、人工智能赋能安全、人工智能基础设施安全）

☐云计算与边缘计算安全：_____（如：云工作负载保护、云安全态势管理、云身份与访问管理、边缘计算安全）

☐大数据安全与隐私计算：_____（如：数据脱敏与隐私计算、数据流通安全）

☐物联网安全：_____（如：物联网设备安全、物联网通信安全）

☐工业互联网安全（工控安全）：_____（如：工控系统安全、工业安全管理平台）

☐车联网（智能网联汽车）安全：_____（如：车端安全、V2X 通信安全、车联网平台安全、自动驾驶数据安全）

☐区块链安全：_____（如：区块链平台安全）

☐卫星互联网（低轨星座）安全：_____（如：卫星互联网安全）

☐5G/6G 与新型通信网络安全：_____（如：5G/6G 网络切片、边缘计算与开放无线接入网安全。）

☐量子安全：_____（如：量子密钥分发系统与应用安全、抗量子密码算法评估与迁移。）

☐网络安全公共服务：_____（如：5G/6G 网络切片、边缘计算与开放无线接入网安全。）

☐其他：_____（如：量子安全、API 安全、供应链安全、信创安全、其他安全等）

五、应用案例

序号	案例名称	项目金额（万元）	用户单位	应用时间	效果反馈（简述）
1	案例 1		例：党政军领域		
2	案例 2		例：关键基础设施等重要行业		
3	案例 3		例：其他行业		

六、提交材料清单（按顺序编号）

序号	材料名称	是否提交	材料编号
1	企业法人营业执照副本复印件（加盖公章）		
2	分支机构证明（如适用）		
3	知识产权证明文件（专利、软著等）		
4	第三方测试报告		
5	其他测评证书		
6	著作权证书		
7	专利证书		
8	产品密码检测证书（如适用）		
9	经营场所及技术环境证明（房产证、设备清单等）		
10	项目案例证明（合同、验收报告等）		
11	无违法违规记录承诺书		
12	其他补充材料		

七、企业承诺

本企业郑重承诺：

1. 本申请书所填写内容及所附材料真实、准确、完整，无虚假记载、误导性陈述或重大遗漏；
2. 本企业严格遵守《网络安全法》《数据安全法》《个人信息保护法》等相关法律法规；
3. 本企业同意武汉市网络安全协会对认定所需的材料进行核查，并积极配合现场验证；
4. 如提供虚假材料，自愿接受认定撤销处理及 3 年内不得重新申请的限制。

申请单位（盖章）：

法定代表人（签字）：

日　　期：　　年　　月　　日

八、受理及审核意见

环　节	意　见	签字/盖章	日期
形式及材料审查	□通过　□补充材料（说明：_____）　□不通过（理由：_____）	审查组：_____	
现场评估	□无需现场评估　□现场评估通过　□现场评估需整改（说明：_____）	评估组：_____	
专家评审	□符合认定要求　□不符合认定要求（理由：_____）	评审委员会：_____	
最终认定	□同意认定为网络安全产品　□不同意（理由：_____）	武汉市网络安全协会	

附录 B

（规范性附录）

B.1 网络安全服务认定申请书（样式）

网络安全服务认定申请书

填 写 须 知

1. 本申请书填写应准确、完整，不得涂改。
2. 所有材料均需加盖申请单位公章。
3. 申请材料以 A4 纸打印并装订成册。
4. 申请书及相关材料不予退还，请自行留存底稿。
5. 标注"*"的项目为必填项。

一、企业基本信息

项　目	内　容
企业名称	
统一社会信用代码	
注册地址	
经营地址	
法定代表人	姓名：_____　职务：_____　办公电话：_____　手机：_____　邮箱：_____
申报联系人	姓名：_____　职务：_____　办公电话：_____　手机：_____　邮箱：_____
成立日期	_____年____月____日
企业类型	□国有企业　□民营企业　□外资企业　□合资企业　□其他（请注明_____）
是否上市	□是　□否
股票代码	
分支机构情况	□有　□无（如有，填写武汉分支机构的名称及经营地址：_____，_____）

二、服务基本信息

项　目	内　容
服务描述（简单概述安全服务内容）	□是　□否
网络安全技术人员共计	

其中取得初、中级专业认证人数	
其中取得高级专业认证人数	
网络安全专业技术人员占全体员工人数比重	
是否配备 7×24 小时应急响应团队，具备快速处置网络攻击、数据泄露等安全事件的能力	□是　□否

三、服务体系

项　目	内　容	编号/登记号/证书
具备相关资质的类别	□安全运维　□风险评估　□应急处置 □安全培训　□其他	xxxxx
测评资质（如有）	□等保　□密评	xxxxx
相关服务资质证书	证书名称	
	证书等级	
	证书编号	

四、服务案例

序号	案例名称	项目金额（万元）	用户单位	服务时间	概述
1	近 3 年承接网络安全服务项目或大数据/AI 相关安全项目				
2	....				
3	....				

五、申请认定类型

□安全运维与监测：_____（如：网络安全运维服务、网络安全监测服务）
□安全应急与恢复：_____（如：网络安全应急响应服务、灾难备份与恢复服务）
□安全评估与审计：_____（如：网络安全风险评估服务、信息安全测试服务、安全配置核查服务、安全审计服务）
□安全咨询与规划：_____（如：信息安全管理咨询、网络安全规划服务）
□安全培训：_____（如：网络安全意识培训、网络安全技能培训）
□网络安全产品批发：_____（如：安全软件批发、安全硬件批发）
□网络安全产品零售：_____（如：安全软件零售、安全硬件零售）
□网络安全系统集成总包：_____（如：安全集成总包服务）
□安全集成实施：_____（如：安全防护系统集成、物联网安全技术服务）
□其他网络安全服务_____（如：其他未列明网络安全服务）

六、提交材料清单

序号	材料名称	提交情况	备注
1	企业营业执照副本复印件（加盖公章）	□已提交　□未提交	
2	服务资质证书复印件	□已提交　□未提交	□不适用
3	服务流程文档	□已提交　□未提交	
4	服务团队人员名单及资质证书	□已提交　□未提交	

5	过往服务项目合同及交付报告	□已提交　□未提交	
6	服务工具清单及授权证明	□已提交　□未提交	
7	其他补充材料	□已提交　□未提交	

七、企业承诺

本企业郑重承诺：

1. 本申请书所填写内容及所附材料真实、准确、完整，无虚假记载、误导性陈述或重大遗漏；
2. 本企业严格遵守《网络安全法》《数据安全法》《个人信息保护法》等相关法律法规；
3. 本企业同意武汉市网络安全协会对认定所需的材料进行核查，并积极配合现场核查；
4. 如提供虚假材料，自愿接受认定撤销处理及 3 年内不得重新申请的限制。

申请单位（盖章）：

法定代表人（签字）：

日　　期：　　年　　月　　日

八、受理及审核意见

环　节	**意　见**	**签字/盖章**	**日期**
形式及材料审查	□通过　□补充材料（说明：_____）　□不通过（理由：_____）	审查组：_____	
现场评估	□无需现场评估　□现场评估通过　□现场评估需整改（说明：_____）	评估组：_____	
专家评审	□符合认定要求　□不符合认定要求（理由：_____）	评审委员会：_____	
最终认定	□同意认定为网络安全服务　□不同意（理由：_____）	武汉市网络安全协会	

附录 C

（规范性附录）

C.1 网络安全产品认定证书（样式）

网络安全产品认定证书（样式）

项目	内容
证书编号	武网安协产认〔_____〕第_____号
企业名称	
统一社会信用代码	
注册地址	
经营地址	
发证依据	根据《网络安全产品和服务认定规范》（T/WHCSA 009—2026）
产品名称	
产品型号	
产品类别	
证书有效期	自_____年_____月_____日至_____年_____月_____日

发证机构（盖章）：武汉市网络安全协会

发证日期：_____年_____月_____日

说明：

1. 本证书证明所载产品符合《网络安全产品和服务认定规范》（T/WHCSA 009—2026）中规定的产品认定条件。
2. 本证书有效期为 2 年，有效期满前 3 个月可申请复评换证。
3. 产品核心信息（如产品型号）变更的，需在变更后 30 日内申请证书变更。
4. 证书持有人在认定有效期内应遵守认定规范及协会相关管理规定，接受年度核查。

附录 C

（规范性附录）

C.2 网络安全服务认定证书（样式）

网络安全服务认定证书（样式）

项目	内容
证书编号	武网安协服认〔_____〕第_____号
企业名称	
统一社会信用代码	
注册地址	
经营地址	
发证依据	根据《网络安全产品和服务认定规范》（T/WHCSA 009—2026）
服务名称	
服务类型	
证书有效期	自_____年_____月_____日至_____年_____月_____日

发证机构（盖章）：武汉市网络安全协会

发证日期：_____年_____月_____日

说明：

1. 本证书证明所载服务符合《网络安全产品和服务认定规范》（T/WHCSA 009—2026）中规定的服务认定条件。
2. 本证书有效期为 2 年，有效期满前 3 个月可申请复评换证。
3. 服务核心信息（如服务范围）变更的，需在变更后 30 日内申请证书变更。
4. 证书持有人在认定有效期内应遵守认定规范及协会相关管理规定，接受年度核查。

参考文献

[1] 《团体标准管理规定》（国标委联〔2019〕1 号）

[2] 《中华人民共和国标准化法》（2017 年修订）

[3] 《中华人民共和国网络安全法》

[4] 《中华人民共和国数据安全法》

[5] 《中华人民共和国个人信息保护法》

[6] 《网络安全专用产品安全管理办法》（国家网信办、工信部、公安部、市场监管总局令第 4 号）

[7] 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

[8] GB/T 25067-2020 信息技术 安全技术 信息安全管理体系审核和认证机构要求

[9] GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

[10] GB/T 35273-2020 信息安全技术 个人信息安全规范

[11] CCRC《信息安全服务资质认证规范》（2024 版）

[12] 《工业互联网安全分类分级管理办法》（工信部网安〔2024〕68 号）