ICS 35.080
CCS L 77

团　　体　　标　　准

T/DGAG 037—2025

数字政府统一基础运维规范
第 4 部分：政务外网网络安全服务要求

Specification for digital government unified basic operation maintenance
—Part 4: Requirements for government external network security services

2025－12－12 发布　　2026－01－01 实施

广东省数字政务协会　　发 布

目　　次

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。

《数字政府统一基础运维规范》分为7个部分：

——第 1 部分：总则；（已以 DB4401/T 294.1—2024 发布）

——第 2 部分：信息基础设施服务要求；（已以 DB4401/T 294.2—2024 发布）

——第 3 部分：政务云服务要求；（已以 DB4401/T 294.3—2024 发布）

——第 4 部分：政务外网网络安全服务要求；

——第 5 部分：信息基础设施服务实施；

——第 6 部分：政务云服务实施；

——第 7 部分：政务外网网络安全服务实施。

本文件是《数字政府统一基础运维规范》的第4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。

本文件由广东省数字政务协会归口。

本文件起草单位：广州市数字政府运营中心、中国联合网络通信有限公司广州市分公司、广州市标准化研究院、联通（广东）产业互联网有限公司、联通数字科技有限公司、深信服科技股份有限公司、广州安恒智慧城市网络安全技术有限公司、广州方集信息科技有限公司、广东省数字政务协会、广州市信息安全测评中心、广州大学网络空间安全学院、赛讯数科（广东）技术有限公司、中网讯信息科技（广州）有限公司、广州尚古网络科技有限公司、云仓库（广东）信息科技有限公司。

本文件主要起草人：苏勇、廖盛辉、吴鹏、穆斌、陈刚、周绍午、罗世荣、何帅、汪旭、但莹、刘笛、钟志鸿、杨连成、季万松、曾剑锋、陈立龙、李鹭君、梁师瀚、李树栋、林兵、苏轶、方琼、刘洋、陈一强、廖奘龙、斯鹏、于代典、刘瑞婷、李昀辉、张清华、曾金杯、吴伟雄、董耀艺、叶将发、刘曦、杨小庆、陈文俊。

引　言

广州市为提升网络安全保障能力和基础设施运维管理能力，构建集约管理、安全可信、权责清晰、资源共享、高效有序的广州市数字政府统一基础运维管理体系，广州市政务服务和数据管理局通过开展数字政府统一基础运维，整合全市各部门现有基础运维资源，将原分散、各自负责的基础运维工作进行一体化服务。

目前，广州市数字政府统一基础运维主要针对信息基础设施、政务云和政务外网网络安全三个方面。为规范广州市数字政府统一基础运维服务，提高服务质量，2023年广州市政务服务和数据管理局提出建立一整套的服务标准。本标准依据广州市数字政府统一基础运维的实际实施情况，将标准分为7个部分。

其中，第1部分总则，主要说明统一基础运维的主要内容和范围，并为其余部分的编制提供依据；第2、3、4部分主要从管理方和使用方的角度，分别对信息基础设施、政务云和政务外网网络安全的服务内容与效果提出要求；第5、6、7部分则主要对服务方提供信息基础设施、政务云和政务外网网络安全服务的实施过程进行规范。

《数字政府统一基础运维规范》第1、2、3部分已以地方标准的形式发布，其第4、5、6、7部分以团体标准的形式发布。

本文件是《数字政府统一基础运维规范》的第4部分。该部分旨在指导相关方统一政务外网网络安全服务要求，确保服务方达到第1部分统一基础运维的总体工作要求。

数字政府统一基础运维规范
第 4 部分：政务外网网络安全服务要求

1 范围

本文件规定了数字政府统一基础运维中政务外网网络安全运维（含运营）服务的对象、内容、交付、评价与改进的要求。

本文件适用于广州市数字政府统一基础运维中政务外网网络安全的运维（含运营）工作，其它网络安全运维（含运营）可参考。

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 20986—2023 信息安全技术网络安全事件分类分级指南

GB/T 28827.2—2012 信息技术服务 运行维护 第2部分：交付规范

GB/T 30276—2020 信息安全技术 网络安全漏洞管理规范

GB/T 30279—2020 信息安全技术 网络安全漏洞分类分级指南

GB/T 38645—2020 信息安全技术 网络安全事件应急演练指南

GB/T 43557—2023 信息安全技术 网络安全信息报送指南

GB/T 45940—2025 网络安全技术 网络安全运维实施指南

DB4401/T 294.1—2024 数字政府统一基础运维规范 第1部分：总则

3 术语和定义

DB4401/T 294.1—2024界定的以及下列术语和定义适用于本文件。

3.1

网络安全运维 cybersecurity operation and maintenance

组织为抵御网络空间安全威胁，控制网络安全风险，确保业务持续、稳定运行，保证业务以及承载数据的保密性、完整性和可用性，统筹技术、流程、人员等要素，持续开展管理、识别、防护、监测分析、事件处置、协同等工作的一种网络安全服务方式。

[来源：GB/T 45940—2025，3.1]

4 服务对象

政务外网网络安全服务，包括网络和计算运行环境、应用系统及支持组件、业务数据、运行数据、安全服务设施及管理平台等。

a) 网络和计算运行环境：网络基础设施（路由器、交换机等）、服务器（物理服务器、虚拟机、容器）、操作系统等；不包括网络链接和计算运行环境的物理可用性、虚拟化平台（VMware、KVM、Hyper-V 等）和云平台基础资源（IaaS 层的计算、存储、网络资源）的自身安全。

b) 应用系统及支持组件：业务应用系统（WEB 应用系统、APP 等）、中间件、数据库管理系统、第三方插件和组件。

c) 业务数据：数据库表、文件系统中的文档静态存储数据，安全系统或平台的管理和配置文件，不包括业务系统的用户数据。

d) 运行数据：系统日志、审计日志、网络流量数据、性能监控数据、告警与事件数据等。

e） 安全服务设施：防火墙、入侵检测/防御系统、身份认证与访问控制系统、主机安全、终端安全系统、零信任系统、漏洞扫描系统、态势感知系统等。
f） 管理平台：安全运维平台、安全信息与事件管理平台、安全运营平台等。

5 服务内容

5.1 安全防护

5.1.1 边界安全

提供包括授权访问、病毒防护、入侵防范及远程访问服务等政务外网边界接入安全服务，防止未经授权的访问、攻击、病毒感染和数据泄露。

5.1.2 访问控制

5.1.2.1 提供包括身份认证、权限管理、访问控制审计等政务外网访问控制服务，保证政务外网访问的安全性和合规性。
5.1.2.2 通过终端安全接入，提供应用系统访问控制与授权、用户身份管理、登录认证、加密通信、网络隐身等服务，持续验证和动态授权，强化终端环境安全检测评估，防止通过脆弱或失陷终端攻击业务和数据。

5.1.3 WEB 安全

5.1.3.1 对政务外网 WEB 应用系统等业务应用的安全性与合法性进行检测和验证，主动发现恶意攻击，实时阻断非法请求，防止网页被篡改和非法利用。
5.1.3.2 根据 WEB 安全要求制定安全策略，对 WEB 应用漏洞进行防护。
5.1.3.3 对域名安全进行防护，防止域名被恶意篡改、劫持或滥用，保障用户安全准确地访问目标网站和服务。
5.1.3.4 对暴露在政务外网互联网的 WEB 应用系统，提供 7×24 小时实时安全监测服务，及时发现网页挂马、暗链等，保障应用系统可用性和完整性。
5.1.3.5 对暴露在政务外网互联网的 WEB 应用系统的访问流量进行深度检测，清洗过滤攻击流量，防止攻击、病毒感染和数据泄露。

5.1.4 主机安全

为接入政务外网的主机（包括虚拟机、物理服务器、容器）提供账号合规、资产清点、入侵检测、病毒查杀、恶意软件防护、基线检查、文件完整性监控、东西向流量监测等安全服务，保障主机的安全性、完整性和可用性。

5.1.5 终端安全

为接入政务外网的终端提供资产探测、防病毒管理、终端检测及响应、漏洞补丁管理、终端准入、终端外设管理及数据保护等安全服务，保证办公终端的安全性、完整性和可用性。

5.1.6 日志及审计

5.1.6.1 对政务外网接入的安全设备、安全系统、主机操作系统、数据库、中间件以及应用系统的日志、事件、告警等安全信息进行采集汇总。
5.1.6.2 对政务外网的系统及设备进行管控审计，对过程中的操作行为、权限使用及安全合规性进行记录、监控与审查，以确保系统稳定、数据安全和操作可追溯。
5.1.6.3 对汇总日志信息、服务安全进行审计，每季度提供日志审计报告，日志信息和审计记录保存时间不少于 1 年。

5.1.7 蜜罐

5.1.7.1 在政务外网通过构建攻击诱饵、伪装代理等方式部署蜜罐，检测和识别攻击行为。
5.1.7.2 基于对蜜罐的攻击行为进行分析、监控、管理和处理，记录并报告安全威胁。

5.1.8 高级威胁分析

5.1.8.1 对各种安全威胁进行自动化挖掘与云端关联分析，推送有针对性的威胁情报。
5.1.8.2 对受害目标及攻击源头精准定位，早期发现未知威胁的恶意行为。
5.1.8.3 对入侵途径及攻击者背景提供研判与溯源服务。

5.1.9 态势感知

5.1.9.1 实时监控政务外网网络安全态势，包括威胁、漏洞和攻击。提供系统接口，可实现与外部单位的安全态势信息、威胁情报的双向共享。
5.1.9.2 采集政务外网各类主机、服务、网站、域名等资产信息和资产的风险状态。
5.1.9.3 收集政务外网安全数据，识别安全趋势和潜在的风险。可采用流量监测、加密流量解密等方式进行安全态势感知分析。分析网络安全状态，预测网络安全发展趋势。

5.2 咨询评估

5.2.1 安全咨询

5.2.1.1 提供政务外网网络安全技术支持、报告内容等网络安全相关咨询服务。
5.2.1.2 提供咨询电话、网络等多种渠道的支持。

5.2.2 安全评估

采用包括分析、验证、核查、扫描检测、渗透测试等评估方法，对政务外网系统进行符合性验证与安全风险评估，可采用AI等智能化手段验证防御有效性，并提供安全评估报告。

5.2.3 应用检测

采用包括漏洞检测、基线检查、弱口令检查、渗透测试、代码审计等检测方法，对政务外网移动客户端和服务器端的应用开展安全检测。通过检测工具与人工排查的方式全面发现应用系统脆弱性，并提供应用检测报告及安全加固建议报告。

5.2.4 漏洞扫描

采用漏洞扫描工具检测与人工排查相结合的方式，至少每年1次对政务外网的系统主机及应用进行漏洞检测，提供漏洞检测报告及安全加固建议报告。

5.2.5 渗透测试

通过授权的模拟攻击，至少每年1次对政务外网（网络、主机、系统等）的弱点、技术缺陷和漏洞进行主动分析，并提供渗透测试报告及安全加固建议报告。

5.3 优化改善

5.3.1 资产管理

5.3.1.1 记录政务外网资产信息，建立政务外网资产信息台账。政务外网资产发生变更时，及时对变更信息进行确认与更新。政务外网资产类型清单见附录 A。
5.3.1.2 采用动态扫描检测、网络流量分析、资产测绘、人工排查等方式每季度检测，及时发现未知资产，并进行跟踪处理。
5.3.1.3 依据政务外网资产信息库，提供资产风险管理服务，包括资产攻击面分析、风险画像等。

5.3.2 漏洞管理

5.3.2.1 按照 GB/T 30279—2020 的规定，从漏洞危害程度、漏洞修补优先性、漏洞修补对业务影响程度等进行风险等级判断，对不同的风险等级提供相应的安全防护措施建议。
5.3.2.2 按照 GB/T 30276—2020 的规定，对漏洞识别、验证、修复、复测等环节进行全生命周期管理，实时掌握漏洞修复的具体情况，完成漏洞处理的监管。

5.3.3 策略管理

5.3.3.1　根据政务外网安全服务要求制定整体的安全策略。
5.3.3.2　针对不同使用方对政务外网稳定性、可用性及安全性等具体安全需求，统一为政务外网相关安全设备配置针对性的安全策略，并每季度对安全策略进行安全测试和验证，确保其有效性。

5.3.4　安全监测

5.3.4.1　使用多种技术方式，对防护互联网、各单位接入政务外网边界、办公终端、系统主机等安全设备进行周期性的状态检查并提交巡检报告及安全建议，及时发现长期运行的安全隐患，并进行及时修复，保障系统、设备的安全性和高可用性。相关监测项见附录 B。
5.3.4.2　结合安全巡检结果与态势感知，对异常设备进行安全监控和记录，包括筛选过滤告警日志，记录统计告警信息，及时发现内部失陷主机、外部攻击、违规外联等安全事件，经研判后，对安全事件进行上报并响应。
5.3.4.3　每月提供安全态势报告，内容包括对漏洞和威胁的发现、分析和统计，并提出修复建议，对受影响资产整改情况进行统计分析，对安全防护能力的建设和配置更改进行说明。

5.3.5　安全通告

5.3.5.1　实时提供网络安全通告，内容包括安全检测结果、威胁情报、行业重大安全事件以及高危漏洞预警等。
5.3.5.2　每月提供安全态势通告，内容包括高危漏洞、安全热点及威胁情报解读。
5.3.5.3　通告报送符合 GB/T 43557—2023 的规定。

5.3.6　安全培训

根据管理方和使用方需求，制定针对使用方工作人员的网络信息安全相关培训计划，组织开展培训和技术交流，评估培训效果，优化培训内容和方式，提高使用方工作人员的网络信息安全技术能力。

5.4　应急管理

5.4.1　应急响应

5.4.1.1　建立完善的应急响应组织及制度。
5.4.1.2　对风险进行评估，制定应急预案。
5.4.1.3　制定网络安全事件应急响应预案，预案内容包括：

a)　事件的分级及应急启动条件；
b)　组织架构及相关方职责、权利和义务；
c)　应急保障措施及应急响应过程中所需的软硬件、系统、网络与通信、环境场地、操作手册及资料等资源及相关人员；
d)　应急响应处理与恢复流程；
e)　响应时间与处置时限；
f)　事件通报等。

5.4.1.4　每年对应急响应预案进行评估、修订和更新。
5.4.1.5　按照 GB/T 20986—2023 中 6.2 的要求，将网络安全事件分为特别重大事件（一级）、重大事件（二级）、较大事件（三级）、一般事件（四级）4 个级别。
5.4.1.5.1　发生特别重大事件（一级）时，响应指标应满足以下要求：

a)　响应时间：不大于 10 分钟；
b)　服务时间：7×24 小时；
c)　到场时间：工作日不大于 30 分钟，非工作日不大于 1 小时；
d)　处置时间：1 小时内提交应急处置方案，4 小时内完成应急处置。

5.4.1.5.2　发生重大事件（二级）时，响应指标应满足以下要求：

a)　响应时间：不大于 20 分钟；
b)　服务时间：7×24 小时；
c)　到场时间：工作日不大于 1 小时，非工作日不大于 2 小时；
d)　处置时间：2 小时内提交应急处置方案，8 小时内完成应急处置。

5.4.1.5.3 发生较大事件（三级）时，响应指标应满足以下要求：

a) 响应时间：不大于 30 分钟；
b) 服务时间：7×24 小时；
c) 到场时间：工作日不大于 2 小时，非工作日不大于 4 小时；
d) 处置时间：4 小时内提交应急处置方案，16 小时内完成应急处置。

5.4.1.5.4 发生一般事件（四级）时，响应指标应满足以下要求：

a) 响应时间：不大于 40 分钟；
b) 服务时间：7×24 小时；
c) 到场时间：工作日不大于 4 小时，非工作日不大于 8 小时；
d) 处置时间：8 小时内提交应急处置方案，24 小时内完成应急处置。

5.4.1.6 发生网络安全事件，按照预案进行应急响应及事件处置。

5.4.1.7 网络安全事件处置结束后，协助相关使用方编制总结报告，协助管理方编制调查报告，报告内容包括事件概况、事件分类、处置过程、原因分析、加固建议及相关的过程证明材料。

5.4.2 应急演练

5.4.2.1 制定应急演练预案，包括应急演练方案，保障及评估等。

5.4.2.2 组织对应急预案涉及的相关人员进行培训，培训内容包括应急处理的流程和应急处理技能等。

5.4.2.3 每年应至少组织 1 次应急演练，对演练过程进行记录，对演练结果进行评估、总结及建议，出具应急演练报告。

5.4.2.4 应急演练符合 GB/T 38645—2020 的规定。

6 服务交付

6.1 交付管理

6.1.1 服务方应按照 DB4401/T 294.1—2024 中 9.1.3 的规定开展交付管理。

6.1.2 管理内容包括安全防护、咨询评估、优化改善、应急管理等。

6.2 交付方式

6.2.1 交付方式应按照 GB/T 28827.2—2012 中 7 的规定。

6.2.2 采用现场交付或远程交付的方式，确保政务外网网络安全服务的正常提供，以满足服务要求。

6.2.3 在不同使用方服务场景下，服务所采用的交付方式可能存在差异，供参考的方式见表 1。

表 1 服务内容交付方式表

序号	服务内容	服务项	交付方式	
			现场	远程
1	安全防护	边界安全	√	√
2		WEB安全		√
3		主机安全	√	√
4		终端安全	√	√
5		日志及审计	√	√
6		蜜罐		√
7		高级威胁分析		√
8		访问控制		√

表1　服务内容交付方式表（续）

序号	服务内容	服务项	交付方式	
			现场	远程
9	安全防护	态势感知		√
10	咨询评估	安全咨询	√	√
11		安全评估	√	√
12		应用检测	√	√
13		漏洞扫描	√	√
14		渗透测试	√	√
15	优化改善	资产管理	√	√
16		漏洞管理		√
17		策略管理		√
18		安全监测	√	√
19		安全通告		√
20		安全培训	√	√
21	应急管理	应急响应	√	√
22		应急演练	√	√

6.3　交付成果

6.3.1　无形成果包括政务外网的可靠性和稳定性的提升、统一服务和管理流程的优化、整体网络安全防护能力的提升、使用方满意度提高、服务效率的提升等。

6.3.2　有形成果包括检测报告、事件报告、安全加固建议等。交付文档清单见附录C。

7　评价与改进

7.1　管理方

管理方协调统筹各方对政务外网网络安全服务开展评价，根据评价结果，督促监理方、服务方改进服务质量。

7.2　使用方

使用方根据考核评价指标体系等开展服务效果评价，向管理方或服务方反馈本单位满意度、服务中发现的问题、服务效果。

7.3　监理方

7.3.1　采用定性、定量或定性定量相结合等方法进行评价，对全过程监督检查、考核评估，以保障评价结果的科学性。

7.3.2　制定政务外网网络安全服务考核评价指标，考核评价指标宜包括：

a)　服务效率：事件响应时效、事件处置时效等；

b)　服务质量：服务工单完成率，服务过程中可能遇到的安全风险及应对措施的有效性等；

c)　满意度：管理方满意度、使用方满意度、投诉率等；

d) 合规性：安全服务制度完善情况、执行情况、项目管理合规性等。
e) 根据管理方要求，对自身的服务进行评价改进。

7.4 服务方

7.4.1 通过网络、问卷、访谈等方法收集相关方反馈的问题。
7.4.2 通过开展自我评价，或专家评审、第三方评价等方式开展系统全面的服务评价。
7.4.3 采用定性、定量或定性定量相结合等方法进行评价，以保障评价结果的科学性。
7.4.4 评价内容包括服务内容、服务质量、服务效率、使用方满意度等；
7.4.5 根据使用方、监理方和管理方反馈的意见和要求、评价结果，制定并落实以下改进措施：
a) 防护能力优化：对安全防护设施的运行进行优化，提升其安全防护能力和稳定性；
b) 服务效率提升：通过自动化服务、流程优化等方式提高事件响应速度、服务工单处理效率，提升服务效率和效果；
c) 服务能力提升：每季度对服务团队进行技术和产品培训，提高其对新技术和新工具的掌握能力，建立知识共享平台促进团队成员互相学习和交流，提高服务人员的专业技能和服务态度；
d) 服务质量提升：每季度开展服务质量自评，审查管理制度执行情况及服务的规范性和一致性，分析服务过程中存在的质量问题，采取针对性改进措施，提升服务质量，提高使用方满意度。
7.4.6 根据改进结果，形成评价报告，包括改进成果和提升成效，并通报相关方。

附 录 A
（资料性）
政务外网资产类型清单

A.1 常用政务外网资产类型清单见表 A.1，在不同使用方、服务场景下，内容可能存在差异，服务方可根据实际情况进行调整。

表 A.1 政务外网资产类型清单

序号	类型分类	分类项
1	网络和计算运行环境	虚拟机、容器、物理服务器、路由器、三层交换机、二层交换机、无线路由器、TAP交换机、负载均衡、网闸/光闸、网络存储、互联网出口IP
2	访问控制	防火墙、虚拟防火墙、WEB应用防火墙（WAF）、网络接入控制（NAC）、VPN设备、4A身份认证、安全网关、零信任网关、零信任管理平台
3	威胁检测防御	DDoS防御、上网行为管理、入侵防御（IPS）、入侵检测（IDS）、APT攻击检测、态势感知、蜜罐/威胁狩猎、探针、流量分析、流量解密、网页防篡改、WEB业务系统云防护、防病毒、主机安全、终端防护/EDR
4	审计监控	漏洞扫描、日志审计、数据库审计、堡垒机、WEB日志安全分析系统
5	数据保护	数据防泄露（DLP）、API安全网关
6	终端及其它设备	台式微型计算机、便携式微型计算机、移动终端、打印机/扫描仪/一体机、其它办公设备、硬盘录像机、媒体分发器、摄像头、视频会议系统、视频会议终端
7	应用系统与组件	管理平台、WEB应用、小程序、APP、公众号、其它应用系统、操作系统、数据库、中间件、虚拟化平台

附 录 B
（资料性）
监测项

B.1 常用政务外网网络安全监测内容见表B.1，在不同使用方、服务场景下，内容可能存在差异，服务方可根据实际情况进行调整。

表B.1 政务外网网络安全监测项

序号	监测类别	监测项	监测内容
1	网络安全防护类	通用监测项	是否开启复杂密码策略 是否开放非必要的端口和服务 是否划分不同级别的用户，赋予其不同的权限，至少应包括系统管理员、审计管理员等用户角色 是否具备两个以上的用户身份，对系统策略和日志进行维护和管理 在网络拓扑图中是否有明显的标示 安全区域的划分是否明确合理 售后服务和技术支持手段是否完备 是否具有安全管理状况报告 是否具有运行监测报告 是否对CPU、内存和硬盘使用情况进行监测 是否记录所有的安全事件和日志信息
2		安全平台	是否配置管理终端 是否支持登录日志、操作日志的记录 是否关闭非必要的端口和服务 是否划分不同级别的用户，赋予其不同的权限，至少应包括客户角色、服务角色等用户角色 是否具备两个以上的用户身份，对系统策略和日志进行维护和管理 是否具有严格的口令保管措施 是否加密通信 是否具备防止暴力破解登录 是否支持用户长期未活跃锁定 是否支持双因子认证 是否支持监控告警（包括但不限于扫描探测、恶意通信、漏洞攻击、异常事件、账号异常、拒绝服务） 是否支持实时查看CPU、内存、网络流量等信息 是否支持数据库至少2点备份
3		态势感知	CPU、内存、硬盘使用情况是否正常 告警信息显示是否正常 日志检索全索引查询日志功能是否正常 探针是否正常在线 安全策略配置是否正常 告警信息是否正常 ES入库速率是否正常 EPS处理速度是否正常 集群状态是否正常 威胁情报更新频率

表B.1　政务外网网络安全监测项（续）

序号	监测类别	监测项	监测内容
4	网络安全防护类	防火墙	是否具有详细的访问控制列表 是否标注源地址和目的地址 是否标注允许和拒绝的动作 防火墙访问控制策略中是否出现重复或冲突 接口IP是否有明确的标注 是否具备双机热备功能 管理人员是否为双备份 是否具有防火墙应急恢复方案
5		WEB应用防火墙	是否针对加密数据包解析 是否开启攻击防护策略 是否开启WEB应用防护策略 是否开启僵尸网络攻击防护功能 是否开启针对色情，恶意脚本、URL等拦截能力
6		堡垒机	是否具有专门的配置管理终端 是否禁用堡垒机超级管理员 是否具有详细的访问控制（白名单访问） 通信是否支持国密通信 是否支持对多次登录封禁 是否支持用户长期未活跃锁定 是否支持双因子认证 是否支持告警外发，包含操作认证、系统资源告警等
7		审计类设备（日志审计、数据库审计等）	是否具有专门的配置管理终端 是否及时修改账号的密码 是否划分不同级别的用户，赋予其不同的权限，至少应包括系统管理员、审计管理员等用户角色 是否具备两个以上的用户身份，对系统策略和日志进行维护和管理 是否有IP地址访问限制 是否支持双因子认证 审计存储是否满足365天 配置是否有远程备份 设备是否已正确配置所有需要监控的日志源 是否能够正确解析各种格式的日志数据，确保日志信息的准确性和完整性 是否已设置合理的日志分析规则，能够准确识别并报告潜在的安全事件和异常行为 管理端是否具有观察客户端掉线 是否具有审计CPU、存储等信息内容 是否支持一键导出报告 数据库审计是否关闭非必要的端口

表B.1　政务外网网络安全监测项（续）

序号	监测类别	监测项	监测内容
8	办公终端防护类	办公终端防病毒	是否配备专职的终端管理员 管理员口令是否具有严格的保管措施 授权是否正常 是否开启实时扫描防护 是否开启预设全盘扫描任务 是否开启检测响应EDR功能 是否定时更新病毒码 是否开启客户端防退出、防卸载功能 是否有详细的终端资产信息 是否有详细的病毒日志 检测响应功能是否有告警记录
9		准入控制	准入是否正常运行 准入管控是否正常 是否开启设备入网审核 是否有实时告警
10		零信任接入	是否有详细账号、资源清单 是否有在线用户监控 是否有终端登录记录 是否有访问行为记录 运行是否正常 零信任账号是否开启密码策略 是否开启二次认证 是否限制资源权限 零信任网关运行是否正常
11	主机安全	主机安全防护	是否有防止暴力破解登录机制 是否及时修改管理平台超级管理员的默认口令 是否每季度清点防护客户端的资产信息 是否每季度对防护资产进行风险扫描 是否能够实时监测入侵行为 是否开启自动处置、防病毒功能 是否能够实时东西向流量可视化 是否有东西向访问管控
12		容器安全防护	是否每季度清点防护客户端的资产信息 是否每季度对防护资产进行风险扫描 是否能够实时监测入侵行为，是否具备基线检查 是否开启防病毒功能 是否具备镜像安全扫描、镜像阻断 是否具备应用漏洞检测 是否具备集群、节点风险扫描

附 录 C
（资料性）
交付文档清单

C.1 常用政务外网网络安全服务常用交付文档清单见表C.1，在不同使用方、服务场景下，内容可能存在差异，服务方可根据实际情况进行调整。

表C.1 交付文档清单

序号	文档类别	文档名称
1	安全评估类	安全评估报告
2		应用检测报告
3		渗透测试报告
4		漏洞检测报告
5		安全加固建议报告
6	安全监测类	日志审计报告
7		安全态势报告
8	设备巡检类	巡检报告
9	日常服务类	网络安全事件总结报告
10		网络安全事件调查报告
11		应急响应预案
12		应急演练预案
13		应急演练报告
14		资产信息台账
15		安全通告
16		培训报告

参 考 文 献

[1] GB/T 22239 信息安全技术 网络安全等级保护基本要求
[2] GB/T 28827.1 信息技术服务 运行维护 第1部分：通用要求
[3] GB/T 28827.3 信息技术服务 运行维护 第3部分：应急响应规范
[4] GB/T 32914 信息安全技术 网络安全服务能力要求
[5] GB/T 36074.2 信息技术服务 服务管理 第2部分：实施指南
[6] GB/T 37961 信息技术服务 服务基本要求
[7] SJ/T 11691 信息技术服务 服务级别协议指南
[8] ITSS.1 信息技术服务 运行维护服务能力成熟度模型
[9] ISO/IEC 20000-1 信息技术 服务管理 第1部分：服务管理体系要求
[10] ISO/IEC 20000-2 信息技术 服务管理 第2部分：服务管理体系应用指南