ICS 35.240.30
L 67

ZWFW

国家政务服务平台标准

C 0115-2018

国家政务服务平台
安全接入检测要求

（征求意见稿）

2018-XX-XX 发布　　2018-XX-XX 实施

国务院办公厅电子政务办公室 发布

目　次

前　言

本标准按照 GB/T 1.1-2009 给出的规则起草。

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这些专利的责任。

本标准由 提出并归口。

本标准起草单位：　。

本标准主要起草人：　。

国家政务服务平台安全接入检测要求

1 范围

本标准规定了国务院有关部门政务服务平台(业务办理系统)和各地区政务服务平台(以下简称“各地区各部门政务服务平台”)安全接入国家政务服务平台的检测要求，包括总体要求、检测流程和检测细则。

本标准适用于各地区各部门政务服务平台。

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，仅所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 22239 信息安全技术 网络安全等级保护基本要求（报批稿）

GM/T 0054-2018 信息系统密码应用基本要求

GW0202-2014 国家电子政务外网安全接入平台技术规范

GW0205-2014 国家电子政务外网跨网数据安全交换技术要求与实施指南

C 0116-2018 国家政务服务平台网络安全保障要求

3 国家政务服务平台安全接入检测总体要求

各地区各部门政务服务平台接入国家政务服务平台，应满足以下要求：

a) 应通过网络安全等级保护测评，具体要求见GB/T 22239，并提供相应的测评证书；

b) 应通过信息系统密码应用安全测评，具体要求见GM/T 0054-2018，并提供相应的测评证书；

c) 应依据附录A中安全接入检测细则的要求，由国务院办公厅电子政务办公室认可的第三方评估机构对各地区各部门政务服务平台进行安全接入检测，并将检测结果上报国家政务服务平台安全管理办公室复核；

d) 与国家政务服务平台进行数据交换和授权访问时，应对各类接入业务进行注册、监控与审计，并从链路、网络、主机、应用等方面采取必要的安全技术措施保障国家政务服务平台的网络安全，具体要求内容见GW0205-2014；

e) 应保证信息在接入过程中不被非法获取及篡改，具体要求内容见GW0202-2014；

f) 监控与审计系统应具有级联上报功能，国家政务服务平台应对其他接入平台的主要运行参数及安全状况等情况进行集中监控与审计，具体要求内容见C 0116-2018。

4 国家政务服务平台安全接入检测流程

各地区各部门政务服务平台应按要求开展安全接入检测工作，检测流程图见图1。

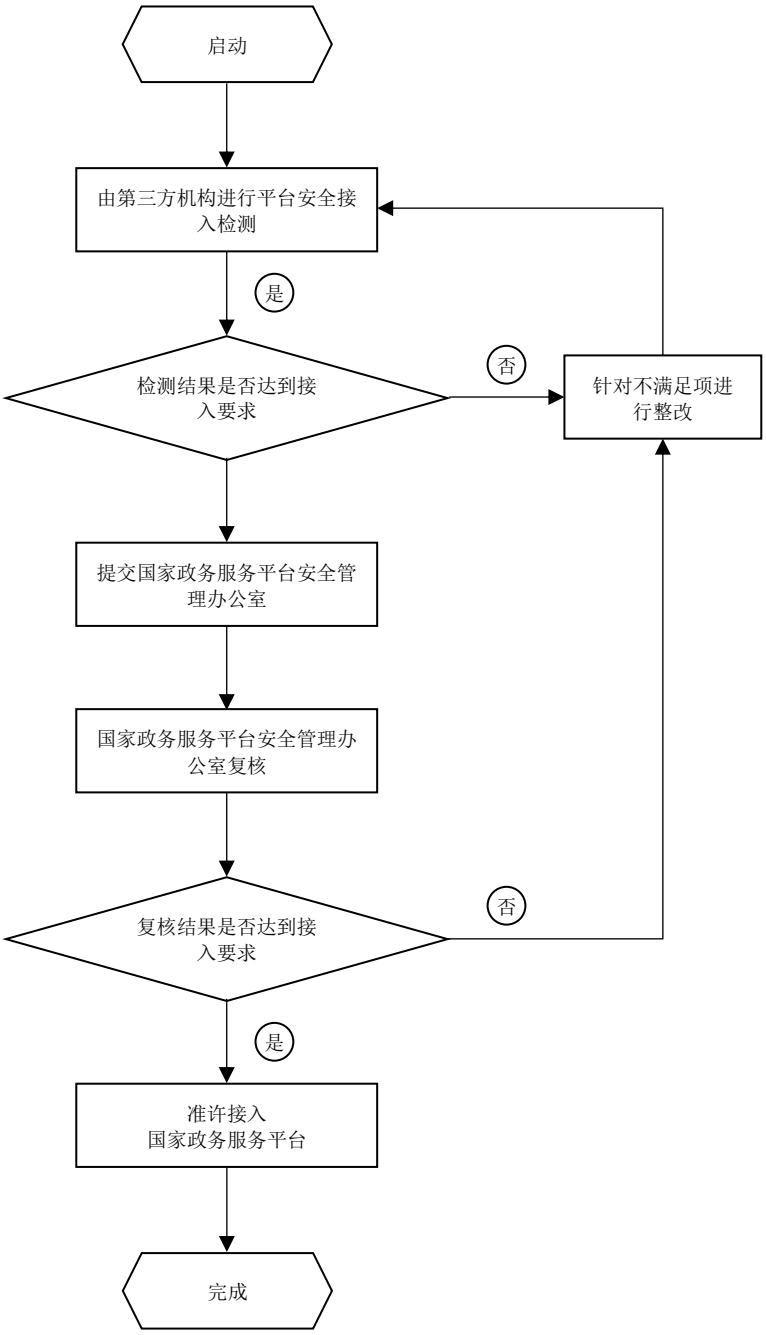

图1　安全接入检测流程图

5　国家政务服务平台安全接入检测细则

各地区各部门政务服务平台应按国家政务服务平台安全接入检测细则的要求开展安全接入检测工作，检测范围包括平台所有业务系统和运行环境。安全接入检测细则见附录A。检测结果判定依据如下：

a)　基本要求中包含的检测项为一票否决项，任一项不满足则检测终止；

b)　打分项满分为100分，得分低于90分则检测不通过；

c)　标“*”检测项要求必须满足，任一项不满足则检测不通过；

d)　最终检测结果由国家政务服务平台安全管理办公室予以判定。

附 录 A
（资料性附录）
安全接入检测细则

表 A.1 给出了国家政务服务平台安全接入的检测细则。

表 A1 安全接入检测细则表

序号	要求类别	要求项目	要求子项	要求小项	分值（单位：分）	是否满足	评分结果	备注
1	基本要求	网络安全等级保护基本要求	--	* 满足网络安全等级保护（三级）基本要求，并提供专业机构颁发的测评证书	一票否决项			
2		信息系统密码应用要求	--	* 满足信息系统密码应用要求，并提供专业机构颁发的测评证书	一票否决项			
3	技术要求（70 分）	通信网络安全（5 分）	网络架构安全（4 分）	* 关键设备应冗余部署，保证平台的高可用性	2			
4				应根据业务应用功能、资产价值、资产所面临的风险划分安全区域，明确定义区域边界	1			
5				采用云计算技术的平台应根据业务特点进行资源池划分并实现不同虚拟网络之间的隔离	1			
6			通信链路安全（1 分）	应采用冗余链路保证互联网区出口和公共区出口链路的高可用性	1			
7		区域边界安全（15）	政务外网边界安全（3 分）	* 各级政务服务平台公共区边界应部署防火墙系统、入侵检测系统和安全审计系统等与政务外网进行逻辑隔离并对公共区进行安全防护	3			
8			互联网边界安全（7 分）	* 应具备防范来自互联网的 DDoS 攻击、Web 攻击、木马病毒等各类恶意攻击的能力	3			
9				* 应在互联网边界部署访问控制设备，设置最小化访问控制规则，细粒度需要达到端口级	2			

序号	要求类别	要求项目	要求子项	要求小项	分值（单位：分）	是否满足	评分结果	备注
10				应具备基于恶意攻击（包括未知新型攻击）的实时监测能力和安全态势感知能力	1			
11				能对云主机主动散播和被操纵主机的被动有害信息散播行为进行检测、告警和清除	1			
12			跨网交互安全（3 分）	* 应部署跨网数据安全交换系统实现互联网区和公共区信息数据安全交换及传输，应采用数据库同步和文件交换模式，系统应具有内容检查、格式过滤及病毒查杀等功能	3			
13			域间安全（2 分）	应在公共区、互联网区内严格划分安全域并通过防火墙或虚拟防火墙实现逻辑隔离；存放重要业务应用及用户核心数据的网段不能直接与外部系统连接，需要单独划分区域	2			
14		计算环境安全（35）	身份鉴别与访问控制（4 分）	* 应对各业务系统及其所依托的基础运行环境（包括且不限于：网络设备、安全设备、主机操作系统、数据库操作系统、中间件等）的管理员账户进行身份验证	2			
15				身份标识应具有唯一性；应配置账户密码安全策略，启用密码复杂度要求，密码长度最小值推荐 8 位，密码至少使用大写字母、小写字母、数字和非字母数字字符中的 3 种；开启系统账户登录失败处理策略，锁定阀值 5 次，账户锁定时间 10 分钟	1			
16				应采取 SSH、Https 或远程桌面（加密）方式进行远程管理，防止鉴别信息在网络传输过程中被窃听	0.5			
17				应采用口令与动态令牌或数字证书等两种或两种以上组合的鉴别技术对用户进行身份鉴别	0.5			

序号	要求类别	要求项目	要求子项	要求小项	分值（单位：分）	是否满足	评分结果	备注
18			安全审计（3 分）	* 应配置各业务模块及其所依托的网络设备、安全设备、主机操作系统、数据库操作系统、中间件等基础设施的审计功能，审计范围覆盖每个用户及应用系统重要安全事件，审计内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等	2			
19				应部署统一的日志收集、存储系统，确保审计记录的留存时间符合法律法规要求,留存时间应至少为 6 个月；能够对审计记录数据进行统计、查询、分析及生成审计报表；审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的正确性	1			
20			恶意攻击防范（11 分）	* 应构建外围 Web 应用安全防护措施，对 SQL 注入、跨站攻击、非法上传等行为进行阻断，从而抵御和过滤外部安全威胁	2			
21				* 应针对服务界面和移动应用 APP 对外发布的 WEB 服务器，在服务器的操作系统内安装网页防篡改系统，防止服务页面内容被恶意篡改	2			
22				应部署主机安全加固系统，采用主动防御机制，通过过滤、隔离、认证等技术，从操作系统核心层实现对操作系统的安全增强	2			
23				应部署主机恶意代码防护系统，并保持恶意代码库实时更新	2			
24				应具备主机防入侵能力，包括 APT 攻击、间谍软件等攻击的防护	1			
25				应针对数据库攻击行为部署技术措施，进行有效检测和阻断，实现对数据库的安全防护	1			

序号	要求类别	要求项目	要求子项	要求小项	分值（单位：分）	是否满足	评分结果	备注
26				应采用数字签名技术校验移动 APP，防止数据被恶意篡改	1			
27			软件容错（2 分）	应按照已知的有效类型、模式和范围，限制用户输入的类型、长度、格式和范围，在服务器端对所有的输入进行安全验证，数据源包括且不限于：其他服务输出、共享文件、用户输入或是调用数据库	0.5			
28				应验证数据的格式、长度是否符合系统设计要求、是否包含带有攻击性的字符	0.5			
29				当应用系统发生故障时，应禁止反馈应用系统敏感信息（如：函数名、系统路径、堆栈跟踪信息）	0.5			
30				当系统发生故障时，应及时保存当前状态，保证系统能够进行恢复	0.5			
31			抗抵赖 (1 分)	应采用数字签名或严格审计记录的方式，实现抗抵赖功能；应对涉及业务数据的业务处理过程采用抗抵赖控制措施；在使用数字签名实现抗抵赖功能时，应采用签名、验签服务实行签名、验签处理，数字签名应采用国密算法	1			
32			数据分类分级 (1 分)	应对平台数据进行分类分级管理，不同类别级别的数据采取不同的安全保护措施(具体要求参见 C 0116-2018 附录 A 表 A.1)	1			
33			数据加密 (2 分)	应采用密码技术保证平台的鉴别数据、重要业务数据和重要个人信息等在传输过程中的保密性	1			
34				应对关键业务中的鉴别信息、重要业务数据进行加密存储	1			
35			数据脱敏与防泄漏（4 分）	* 应对关键业务中的鉴别信息、重要业务数据进行脱敏处理，防止数据泄露	2			

序号	要求类别	要求项目	要求子项	要求小项	分值（单位：分）	是否满足	评分结果	备注
36				应通过技术手段防止重要数据被恶意爬取	1			
37				应保证存有鉴别信息及敏感数据的存储空间被释放或重新分配前得到完全清除	1			
38			数据备份与恢复（2 分）	* 应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；对完整数据定期备份，并将备份介质存放在安全区域内，数据保存期限符合相关规定	2			
39			可信计算环境（2 分）	各级政务服务平台应建立可信计算环境，针对平台的核心业务部署可信计算节点、构建可信计算资源池，为核心业务提供可信计算应用环境	1			
40				应具备针对系统运行状态的度量防护能力，实时监视系统内所有关键进程、模块、执行代码、数据结构、重要跳转表等，对进程的资源访问行为进行实时度量和控制	1			
41			内网未知威胁检测与防御（3 分）	* 应具备内网未知威胁检测能力，可有效防止威胁通过被感染主机在内网范围内扩散，及时发现并隔离被感染主机	3			
42		安全管理中心（15）	综合审计（2 分）	* 应具备实时审计采集政务服务平台各类安全行为和日志的能力，审计对象应覆盖终端、数据库、服务器、云平台、安全设备、应用、互联网威胁情报等，具备针对异常网络行为的阻断、复原等应急处置的能力	2			
43			集中管控（3 分）	应具备对网络中的安全设备或安全组件进行集中管控的能力	2			
44				应具备联动控制安全设备进行威胁处置的能力	1			
45				应能对网络中各类安全数据进行数据采集，包括安全设备日志、审计数据和威胁情报数据等	1			

序号	要求类别	要求项目	要求子项	要求小项	分值（单位：分）	是否满足	评分结果	备注
46			态势感知及安全事件分析（7 分）	* 应具备安全分析和可视化能力，至少可以提供资产态势展示、威胁态势展示、操作行为态势展示、网络攻击展示和全网态势展示等	2			
47				* 应具备安全策略可视化能力，可有效验证安全策略配置的有效性及合理性	2			
48				对安全态势感知中可视化呈现出来的异常、违规、告警等网络行为，可以通过溯源分析技术，发现网络安全事件成因	1			
49				应具备对未知新型攻击等威胁源进行分析检测，识别国家政务服务平台受攻击情况	1			
50			责任认定分析（2 分）	应通过实时审计采集网络中的所需操作行为和日志，构建安全数据中心，对相关安全事件进行溯源分析，定位责任主体，从而达到网络行为可核查、网络责任事件可追究	2			
51			级联接口要求（1 分）	平台各级安全管理体系中的审计采集策略、接口通讯协议、数据指标类别、数据采集格式、数据报送格式等应符合接入要求，审计数据中心应能实现级联，以便安全审计策略能够上下贯通	1			
52	管理要求（18 分）	安全保障管理组织（12 分）	安全保障组织机构（7 分）	* 应成立安全及应急保障领导小组（以下简称领导小组），其组长应由各级政务服务平台主管单位的主要负责人担任，领导小组组长作为政务服务平台网络安全第一责任人，承担领导和管理责任	2			
53				* 应设立安全管理办公室，负责政务服务平台网络安全保障工作的规划与实施，安全管理办公室应在领导小组的领导下开展工作，办公室中应设立安全主管和各业务领域安全管理负责人岗位，并明确岗位职责	2			

序号	要求类别	要求项目	要求子项	要求小项	分值（单位：分）	是否满足	评分结果	备注
54				应设立应急响应办公室，负责政务服务平台安全事件应急响应工作，应急响应办公室下设应急响应处置小组和应急保障专家小组，负责应急响应工作的具体执行。应急响应办公室应在领导小组的领导下开展工作	1			
55				应设立系统管理员、网络管理员、安全管理员等岗位，并明确各个工作岗位的职责，安全管理员岗位要求配备专职人员，不可兼职	1			
56				应根据各个部门和岗位的职责明确汇报和授权审批流程，针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度	1			
57			人员安全管理（5 分）	* 应制定安全人员审查准则，并依据准则对安全管理负责人及关键岗位人员进行岗前或定期（要求至少每年一次）安全背景审查，审查通过才可从事相关岗位工作；负责维护政务服务平台的人员应经过严格筛选，并签订安全保密协议	2			
58				* 安全管理部门应定期（要求至少每季度一次）组织全员进行安全制度和责任培训；涉及网络和信息安全岗位的人员还应进行信息安全知识和岗位操作规程培训，并通过考核机制保证培训效果	2			
59				人员离岗前应办理严格的调离手续，并签署保密承诺，离岗人员应及时终止所有访问权限，收回各种身份证件、钥匙或门禁卡以及单位提供的软硬件设备、重要文件资料等	0.5			

序号	要求类别	要求项目	要求子项	要求小项	分值（单位：分）	是否满足	评分结果	备注
60				外部人员因工作原因访问办公场所时，应经过安全管理办公室批准，由专人接待并全程陪同，在指定区域内活动，外协人员因工作需要接入办公网络前，应向安全管理办公室提出书面申请，经批准后由安全管理员负责开设账号、分配权限，并登记备案，人员离开时应及时清除所有权限	0.5			
61		安全保障管理制度（6 分）	安全保密制度（3 分）	重要岗位人员应签署安全保密协议，防止重要信息外泄	1			
62				* 对于计算机、办公网络、存储设备等基础设施的使用，应由严格的管理制度，禁止违规或越权使用；针对重要数据和文件的使用、传递和保存应制定严格的管理制度，从各个环节做好防护工作，防止重要信息外泄	2			
63			安全考核制度（3 分）	应定期（要求至少每季度一次）对安全管理负责人及关键岗位责任人进行信息安全工作考核，对于不满足考核要求的人员或部门进行培训和整改	1			
64				应定期（要求至少每半年一次）对全员进行信息安全制度和知识的考核，对于不满足考核要求的人员进行培训和整改	1			
65				应制定奖惩机制，对安全保障工作中表现突出的人员予以奖励，对违反安全保障制度的人员给予惩罚，对于关键岗位存在安全违规行为的人员，应调离工作岗位	1			
66	运维要求（12 分）	安全监测与应急处置（6 分）	--	安全应急保障工作应在领导小组的指导下，由应急响应办公室具体负责	1			
67				* 应急响应办公室应依据《全国一体化在线政务服务平台应急保障要求》 C 0117-2018（工作组讨论稿）制定应急预案，作为安全应急响应工作的主要依据；制定安全事件应急处置流程，明确应急处置过程中各项工作的	2			

序号	要求类别	要求项目	要求子项	要求小项	分值（单位：分）	是否满足	评分结果	备注
				内容和责任主体，指导安全事件应急处置工作的具体开展				
68				* 应急响应办公室应建立安全监测机制，有效预防和应对安全事件的发生，安全监测工作应由应急响应处置小组负责执行，工作内容包括日常监测、事件判定、和事件上报	2			
69				应建立监测预警数据库和信息分析平台，为安全监测与应急处置工作提供技术辅助支持	1			
70		安全评估与审计（3 分）	--	* 安全评估与审计工作应由安全管理办公室负责组织开展，根据评估和审计结果开展安全防护措施和安全保障工作流程的整改工作，最终验证整改效果并报上级部门审核	2			
71				应依据政务服务平台评估办法对各级政务服务平台定期（要求每年至少一次）开展安全自评估工作，评估工作围绕资产识别、威胁识别、脆弱性识别三个方面进行，依据现有经过验证的安全防护措施完成风险分析，并输出评估文档，评估结果应存档记录并报上级管理部门审核	1			
72		安全自查与演练（3 分）	--	安全自查与演练工作应由应急响应办公室负责组织开展，自查结果计入政务服务平台运营者绩效考核	1			
73				* 应定期（要求每年至少一次）组织应急行动演练及安全防护措施有效性验证的攻防演练，以提高安全事件应急处置的能力，检验安全防护方案的合理性和时效性，并根据演练结果对应急预案及防护方案进行更新，对安全保障工作进行优化整改	2			
分数合计					100			

序号	要求类别	要求项目	要求子项	要求小项	分值 （单位：分）	是否 满足	评分结果	备注
注1：“是否满足”一列，填“是”、“否”或“不涉及” 注2：“评分结果”一列，“是”或“不涉及”得满分，“不满足”得0分								