国家电子政务外网标准

GW0101—2014

国家电子政务外网信息安全标准体系框架

Information Security Standards Framework of

National E-Government Network

2014－11－13 发布　　2015－1－1 实施

国家电子政务外网管理中心

目　次

前　言

本标准按照GB/T 1.1-2009的规则起草。

本标准由国家电子政务外网管理中心提出并归口。

本标准主要起草单位：国家电子政务外网管理中心、中国电子技术标准化研究院。

本标准的主要起草人：邵国安、罗海宁、杨瑛、周民、杨绍亮、王延鸣、周明霞、焦迪、陈星、吕品。

引　言

国家电子政务外网（以下简称“政务外网”）信息安全标准体系框架是指导规范政务外网建设运维单位组织开展信息安全标准研制的依据，也是政务外网信息安全建设、管理的基础。

本标准为政务外网信息安全标准的制定、修订与管理提供了依据。

国家电子政务外网信息安全标准体系框架

1 范围

本标准适用于指导各级政务外网建设运维单位开展信息安全标准的规划、制定、修订与管理，也可作为政务外网信息安全建设和管理的基础依据之一。

2 规范性引用文件

下列文件对于本标准的应用是必不可少的。凡是注明日期的引用文件，仅所注明日期的版本适用于本标准。凡是不注明日期的引用文件，其最新版本适用于本标准。

GB/T 13016-2009 标准体系表编制原则和要求

GB/T 20000.1-2002 标准化工作指南 第1部分：标准化和相关活动的通用词汇

GB/T 25069-2010 信息安全技术 术语

3 术语和定义

下列术语和定义适用于本标准。

3.1

标准体系 Standard System

一定范围内的标准按其内在的联系形成的科学有机整体。

[GB/T 13016-2009，定义3.3]

3.2

信息安全 Information Security

保护、维持信息的保密性、完整性和可用性，也可包括真实性、可核查性、抗抵赖性、可靠性等性质。

[GB/T 25069，定义2.1.52]

3.3

服务标准 Service Standard

规定服务应满足的要求以确保其适用性的标准。

[GB/T 20000.1，定义2.5.6]

4 标准体系框架建立原则

政务外网信息安全标准体系要坚持适用性、综合性、先进性与开放性等原则，建立适应政务外网建设、管理与应用需求的标准体系。

a) 遵循适用性原则。根据政务外网技术与管理的需求，协调标准与应用的关系，建立符合业务应用实际需要的标准体系；
b) 遵循综合性原则。建立框架结构清晰、层次分类明确的标准体系，形成总体与子类各层次标准之间、技术与管理各类别标准之间协调、配套的整体；
c) 遵循先进性原则。适应信息新技术发展，满足政务外网建设实践中先进技术应用的需求；
d) 遵循开放性原则。标准体系修订及标准化工作是开放的，可根据技术、应用等的发展需要进行更新、完善和扩充。

5 标准体系框架

政务外网信息安全标准体系框架见图1，标准体系分类列表见表1：
a) 标准体系框架是政务外网信息安全标准制定工作的范围和对象；
b) 标准体系框架分为总体和子类共二层；
c) 标准体系框架第一层分为基础标准、技术标准、管理标准、网络信任标准、测评标准、服务标准等总体六类；
d) 标准体系框架第二层按照第一层类别分别细分为不同子类，如基础标准分为总体、体系框架、等级保护、安全基线等子类四项。

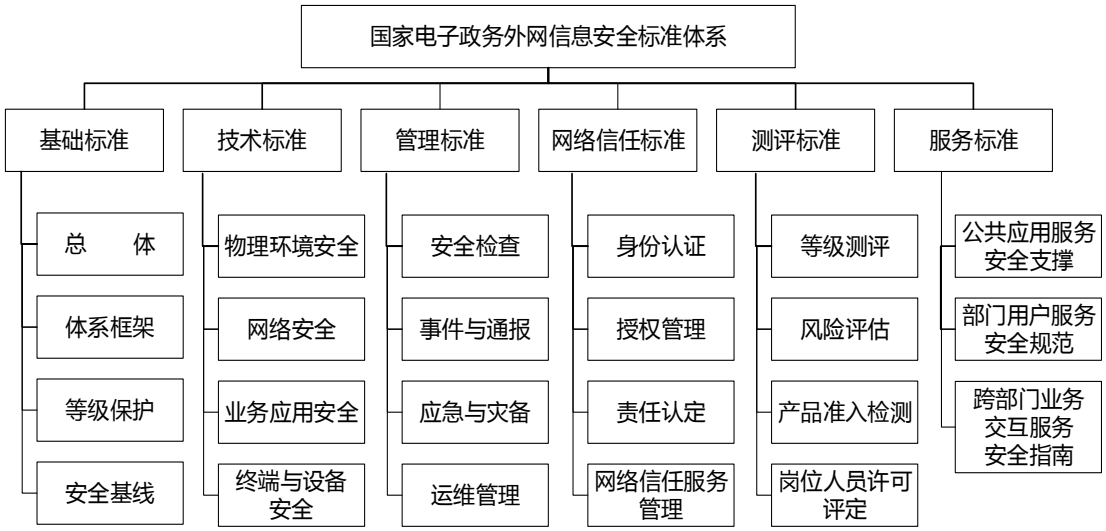

图1　国家电子政务外网安全标准体系框架

表1：国家电子政务外网信息安全标准体系分类列表

一级分类	二级分类
基础标准	总体
	体系框架
	等级保护
	安全基线
技术标准	物理环境安全
	网络安全
	业务应用安全
	终端与设备安全
管理标准	安全检查

一级分类	二级分类
	事件与通报
	应急与灾备
	运维管理
网络信任标准	身份认证
	授权管理
	责任认定
	网络信任服务管理
测评标准	等级测评
	风险评估
	产品准入检测
	岗位人员许可评定
服务标准	公共应用服务安全支撑
	部门用户服务安全规范
	跨部门业务服务安全指南

6 标准分类和内容

6.1 标准分类

a) 基础标准是保障政务外网安全运行的总体性、框架性标准，是保障政务外网安全需要遵循的技术与管理基本要求；
b) 技术标准是与政务外网建设、运行相关的安全产品、技术解决方案需要遵循的技术性规范，包括物理环境安全、网络安全、业务应用安全、终端与设备安全等；
c) 管理标准是政务外网网络与信息安全的技术管理规程，通过执行管理措施与流程，规范政务外网安全检查、事件通报、应急灾备、运维管理等管理工作；
d) 网络信任标准是对基于政务外网数字证书认证建立网络与应用身份信任源点的相关技术与管理规范，指导政务外网业务系统采用身份认证、授权管理、和责任认定的方法以及网络信任体系服务管理流程；
e) 测评标准是与政务外网建设和运行相关的安全测试与评估类标准，包括等级测评、风险评估、产品准入、岗位人员许可评定等；
f) 服务标准是政务外网面向公共服务、部门应用以及跨部门业务交互时所需遵循的具体业务流程、服务安全、服务质量等规范化服务要求。

6.2 标准内容

6.2.1 基础标准

a) 总体标准是总体性、通用性标准，包括政务外网特有的信息安全术语、模型和记法；
b) 体系框架标准反映政务外网信息安全标准的层次结构，包括政务外网技术、管理、业务、服务等体系结构、架构的标准；
c) 等级保护标准是按照国家信息安全等级保护相关制度和标准要求，结合政务外网实际需要制定的实施规范；
d) 安全基线标准是以政务外网达到基本安全防护水平为目标制定的安全策略和安全措施等基本要求。

6.2.2 技术标准

a) 物理环境安全标准是从物理环境角度对存储和传输的网络信息安全保护提出规范，使得政务外网物理环境免遭地震、水灾、火灾等事故以及人为行为导致的破坏，如对各级政务外网机房、计算机系统设备、通信与网络设备、存储媒体设备和人员所采取的区域防护、受灾防护等安全技术措施；
b) 网络安全标准是政务外网的广域网、城域网和各级接入网、局域网等网络承载和传输上所提出的边界安全、接入与互联安全等技术要求；
c) 业务应用安全标准是规范应用层安全防护策略、技术措施等以保护政务外网用户单位或用户的应用平台安全、访问程序安全、数据安全等，如数据、内容、交换等具体业务应用的安全；
d) 终端与设备安全标准是对接入政务外网的用户计算机终端、移动智能终端、网络设备、服务器设备等进行安全配置与加固的规范。

6.2.3 管理标准

a) 安全检查标准是针对各级政务外网主管单位或建设运维单位实施信息安全检查工作的流程、管理机制等提出的安全管理要求；
b) 事件与通报标准是针对政务外网识别信息安全事件的方法、发生信息安全事件时事件响应与处置流程以及所遵循的安全通报流程等提出的安全管理要求；
c) 应急与灾备标准是针对政务外网制定应急预案、组织应急演练、实施灾难恢复、部署容灾备份等所提出的安全管理要求；
d) 运维管理标准是面向各级政务外网网络的运行和维护工作在人员管理、网络维护管理、信息系统维护管理、运维外包管理以及运维角色管理等方面提出的安全管理要求。

6.2.4 网络信任标准

a) 身份认证标准是政务外网认证机构、数字证书注册认证系统、证书格式以及证书命名空间等所遵循的标准；
b) 授权管理标准是基于数字证书的信任源点对政务外网应用资源权限控制提供应用设施支撑的相关规范性要求；
c) 责任认定标准是基于数字证书的信任源点在对政务外网网络与应用访问行为责任进行认定过程中提供技术支撑的相关规范性要求；
d) 网络信任服务管理是对注册机构、多级注册点、电子认证支撑应用等提出的服务管理要求。

6.2.5 测评标准

a) 等级测评标准是按照政务外网等级保护标准要求，依据所确定的安全保护等级，对网络或业务系统安全保护状况进行检测与评估的规范性要求；
b) 风险评估标准是针对政务外网信息安全风险采取定期评估、量化识别等方法的规范；
c) 产品准入检测标准是针对政务外网拟入网的信息安全产品以技术标准为依据进行检测的方法和准入要求；
d) 岗位人员许可评定标准是针对政务外网信息安全岗位人员的选择提出的基本资质要求，人员须按标准评价流程获得通过后上岗。

6.2.6 服务标准

a) 公共应用服务安全支撑标准是指各级政务外网建设运维单位在建设公共应用服务设施、提供服务支撑过程中所遵循的流程规范；
b) 部门用户服务安全规范是指各级政务外网面向政务部门的业务应用提供托管或接入服务时所遵循的流程规范；

c） 跨部门业务服务安全指南是指政务外网面向跨部门业务系统提供技术与管理支撑时所遵循的服务安全指导。

附 录 A
（资料性附录）
政务外网信息安全标准计划清单

一级分类	二级分类	序号	标准名称
基础标准	总体		参照国家标准
		1	政务外网信息安全标准化工作规范
		2	政务外网安全监测体系技术规范与实施指南
	体系框架		参照国家标准
		3	政务外网信息安全标准体系框架
	等级保护	4	政务外网安全等级保护基本要求
		5	政务外网安全等级保护实施指南
		6	政务外网云计算安全等级保护设计基本要求
	安全基线	7	政务外网安全基线基本要求
		8	政务外网安全基线实施指南
技术标准	物理环境安全		参照国家标准
	网络安全	9	政务外网 IPSec VPN 安全接入技术要求与实施指南
		10	政务外网安全接入平台技术规范
		11	（专线）接入政务外网的局域网安全技术规范
		12	政务外网统一互联网出入口安全保障技术规范
		13	政务外网安全接入平台实施指南
		14	政务外网安全管理系统功能技术要求及接口规范
		15	政务外网安全审计技术要求（网络行为与运维管理）
		16	政务外网审计系统技术要求
	业务应用安全	17	政务外网业务应用安全基本要求
		18	政务外网业务应用安全实施指南
		19	政务外网数据安全基本要求
		20	政务外网数据安全测试规范
		21	政务外网门户网站安全管理技术要求
		22	政务外网跨网数据安全交换技术要求与实施指南
	终端与设备安全	23	政务外网终端安全实施规范
管理标准	安全检查	24	政务外网安全检查基本要求
		25	政务外网安全检查实施指南
	事件与通报	26	政务外网网络与信息安全事件分类及通报管理规范
	应急与灾备	27	政务外网总体应急预案规范

一级分类	二级分类	序号	标准名称
		28	政务外网机房、电力故障应急预案规范
		29	政务外网网络攻击、木马病毒等应急预案规范
		30	政务外网数据备份恢复管理规范
	运维安全管理	31	政务外网帐号权限口令等管理规范
		32	政务外网安全管理员职责及操作规程
		33	政务外网系统管理员职责及操作规程
		34	政务外网安全审计员职责及操作规程
		35	政务外网设备托管安全防护及管理规范
		36	政务外网运维故障处理安全规范
网络信任标准	身份认证	37	政务外网电子认证全国服务体系管理规范
		38	政务外网电子认证全国服务体系建设指南
		39	政务外网认证机构（CA)命名空间规范
		40	政务外网认证机构（CA)系统接口规范
		41	政务外网数字证书格式规范
	授权管理	42	政务外网授权管理系统技术要求
	责任认定	43	政务外网责任认定技术要求
	网络信任服务管理	44	政务外网 RA 管理规范
		45	政务外网注册机构建设审批管理办法
		46	政务外网注册服务点（RA）检测指南
		47	政务外网注册服务点（RA）建设指南
测评标准	等级测评		参照国家标准
		48	政务外网等级保护自评价工作规程
	风险评估标准	49	政务外网风险评估基本要求
		50	政务外网风险评估实施指南
	产品准入检测	51	政务外网产品准入检测规范
	岗位人员许可评定	52	政务外网岗位人员许可评定规范
服务标准	公共应用服务安全支撑	53	政务外网公共应用服务安全支撑
	部门用户服务安全规范	54	政务外网部门用户服务安全规范
	跨部门业务服务安全支撑	55	政务外网跨部门业务服务安全指南