信息系统安全等级测评

报告模板

项目名称：_____

委托单位：_____

测评单位：_____

年　　月　　日

报告摘要

一、测评工作概述

概要描述被测信息系统的基本情况（可参考信息系统安全等级保护备案表），包括但不限于：系统的运营使用单位、投入运行时间、承载的业务情况、系统服务情况以及定级情况。（见附件：信息系统安全等级保护备案表）

描述等级测评工作的委托单位、测评单位和等级测评工作的开展过程，包括投入测评人员与设备情况、完成的具体工作内容统计（涉及的测评分类与项目数量，检查的网络互联与安全设备、主机、应用系统、管理文档数量，访谈人员次数）。

二、等级测评结果

依据第 4、5 章的结果对等级测评结果进行汇总统计（测评项符合情况及比例、单元测评结果符合情况比例以及整体测评结果）；通过对信息系统基本安全保护状态的分析给出等级测评结论（结论为达标、基本达标、不达标）。

三、系统存在的主要问题

依据 6.3 章节的分析结果，列出被测信息系统中存在的主要问题以及可能造成的后果（如，未部署 DDos 防御措施，易遭受 DDos 攻击，导致系统无法提供正常服务）。

四、系统安全建设、整改建议

针对系统存在的主要问题提出安全建设、整改建议，是对第七章内容的提炼和简要描述。

报告基本信息

信息系统基本情况				
系统名称			安全保护等级	
机房位置	中心机房			
	灾备中心			
	其他机房			
委托单位				
单位名称				
单位地址				
邮政编码				
联系人	姓　　名		职务/职称	
	所属部门		办公电话	
	移动电话		电子邮件	
测评单位				
单位名称				
通信地址				
邮政编码				
联系人	姓　　名		职务/职称	
	所属部门		办公电话	
	移动电话		电子邮件	
报告	编制人		日期	

审核批准	审核人		日期	
	批准人		日期	

声明

声明是测评单位对于测评报告内容以及用途等有关事项做出的约定性陈述，包含但不限于以下内容：

本报告中给出的结论仅对目标系统的当时状况有效，当测评工作完成后系统出现任何变更，涉及到的模块（或子系统）都应重新进行测评，本报告不再适用。

本报告中给出的结论不能作为对系统内相关产品的测评结论。

本报告结论的有效性建立在用户提供材料的真实性基础上。

在任何情况下，若需引用本报告中的结果或数据都应保持其本来的意义，不得擅自进行增加、修改、伪造或掩盖事实。

测评单位机构名称

年　月

报告目录

附：信息系统安全等级保护备案表

测评项目概述

1 测评目的

描述信息系统的重要性：通过描述信息系统的基本情况，包括运营使用单位的性质，承载的主要业务和系统服务情况，进一步阐明其在国家安全、经济建设、社会生活中的重要程度，受到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等。

描述等级测评工作的基本情况，包括委托单位、测评单位、测评范围及预期（如，通过等级测评找出与国家标准要求之间的差距）。

描述测评报告的用途（如，作为后续安全整改的依据）。

2 测评依据

开展测评活动所依据的合同、标准和文件：

《信息安全等级保护管理办法》（公通字[2007]43号）

《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》（发改高技[2008]2071号）[1]

GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求

GB/T 20984-2007 信息安全技术 信息安全风险评估规范

《信息安全技术 信息系统安全等级保护测评要求》（国标报批稿）

被测信息系统安全等级保护定级报告

等级测评任务书/测评合同等

[1] 针对“国家电子政务工程建设项目”有效

1 测评过程

描述本次等级测评的工作流程（可参考《信息系统安全等级保护测评过程指南》），具体内容包括但不限于：

测评工作流程图

各阶段完成的关键任务

工作的时间节点

1 报告分发范围

依据项目需求，明确应交付等级测评报告的数量与分发范围（如本报告一式三份，一份提交测评委托单位、一份提交受理备案的公安机关、一份由测评单位留存）。

被测系统情况

1 基本信息

系统名称[2]		
主管机构		
系统承载业务情况	业务类型	1 生产作业　2 指挥调度　3 管理控制 4 内部办公　5 公众服务 9 其他_____
	业务描述	
系统服务情况	服务范围	10 全国　11 跨省（区、市）　跨_____个 20 全省（区、市）　21 跨地（市、区）　跨_____个 30 地（市、区）内 99 其它_____
	服务对象	1 单位内部人员　2 社会公众人员　3 两者均包括 9 其他_____
系统网络平台	覆盖范围	1 局域网　2 城域网　3 广域网 9 其他_____
	网络性质	1 业务专网　2 互联网 9 其它_____
系统互联情况	1 与其他行业系统连接　2 与本行业其他单位系统连接 3 与本单位其他系统连接 9 其它_____	
业务信息安全保护等级		
系统服务安全保护等级		
信息系统安全保护等级		

[2] 本报告模板针对作为单一定级对象的信息系统制定。

2 业务应用

描述信息系统承载的业务应用情况。

3 网络结构

给出被测信息系统的拓扑结构示意图，并基于示意图说明被测信息系统的网络结构基本情况，包括但不限于：

功能/安全区域划分、隔离与防护情况

关键网络和主机设备的部署情况和功能简介

与其他信息系统的互联情况和边界设备

本地备份和灾备中心的情况

1 系统构成

以列表的形式分类描述信息系统的软、硬件构成情况。

1.1 业务应用软件

以列表的形式给出被测信息系统中的业务应用软件（包括含中间件等应用平台软件），描述项目包括软件名称、主要功能简介和重要程度。

序号	软件名称	主要功能	重要程度
…	…	…	…

1.2 关键数据类别

序号	数据类型	所属业务应用	主机/存储设备	重要程度
…	…	…		…

1.3 主机/存储设备

以列表形式给出被测信息系统中的主机设备（包含操作系统和数据库管理系统软件），描述项目包括设备名称、操作系统、数据库管理系统以及承载的业务应用软件系统。

序号	设备名称	操作系统/数据库管理系统	业务应用软件
…	…		…

1.4 网络互联与安全设备

以列表形式给出被测信息系统中的网络互联及安全设备。

设备名称应确保在被测信息系统范围内的唯一性，建议采取类别-用途/功能/型号-编号（可选）的三段命名方式。

序号	设备名称	用　途	重要程度
1	路由器_内部_1	内部边界路由	重要
2	路由器_VPN_1	远程管理维护	重要
3	路由器_VPN_2	远程管理维护	重要
4	防火墙_WEB_1	Web　区之间访问控制	重要
…	…	…	…

1.5　安全相关人员

以列表形式给出与被测信息系统安全相关的人员，描述项目包括姓名、岗位/角色和联系方式。人员包括但不限于安全主管、系统建设负责人、系统运维负责人、网络（安全）管理员、主机（安全）管理员、数据库（安全）管理员、应用（安全）管理员、机房管理人员、资产管理员、业务操作员、安全审计人员等。

序号	姓名	岗位/角色	联系方式
…	…	…	…

1.6　安全管理文档

与信息系统安全相关的文档，包括：

管理类文档，如机构总体安全方针和政策方面的管理制度、、人员安全教育和培训方面的管理制度、第三方人员访问控制方面的管理制度、机房安全管理方面的管理制度等；

记录类文档，如设备运行维护记录、会议记录等；

其他类文档，如专家评审意见等。

序号	文档名称	主要内容
…	…	…

1 安全环境

描述被测信息系统的运行环境中与安全相关的部分：如数据中心位于运营服务商机房中、网络存在互联网连接、网络中部署无线接入点以及支持远程拨号访问用户等。

以列表形式给出被测信息系统的威胁列表，并基于历史统计或者行业判断进行威胁赋值，具体内容可参考《风险评估规范》。

序号	威胁分(子)类	描述	威胁赋值
1	网络攻击	利用工具和技术通过网络对信息系统进行攻击和入侵	高
…	…	…	

等级测评范围与方法

1 测评指标

测评指标包括基本指标和附加指标两部分，以列表的形式给出。

依据定级结果选择《基本要求》中对应级别的安全要求作为等级测评的基本指标；

1.1 基本指标

基本指标（物理和网络子类）的例子如下所示：

分类	子类	基本要求	测评项数[3]
物理安全	物理位置的选择	测评物理机房所在的外部环境安全性。	2
	物理访问控制	测评进出机房的审批控制手段以及机房出入口的安全控制情况。	4
	防盗窃和防破坏	测评机房内设备和通信线缆的安全性以及监控报警系统建设情况。	6
	防雷击	测评建筑防雷和防感应雷的建设情况。	3
	防火	测评自动监控防火系统设置情况以及机房材料防火情况。	3

[3] 测评项数量随信息系统的安全保护等级不同而变化

分类	子类	基本要求	测评项数[3]
	防水和防潮	测评机房内水管设置情况、防止结露所采取的措施以及监控报警系统建设情况。	4
	防静电	测评机房防静电所采取的措施。	3
	温湿度控制	测评机房温湿度控制措施	1
	电力供应	测评电力线路、备用电源以及发电机的配备情况。	4
	电磁防护	测评线缆电磁防护手段和设备电磁防护手段。	3
网络安全	结构安全	主要核查：主要网络设备的处理能力、业务高峰期需求带宽、路由控制、网络拓扑结构图是否一致、子网划分、技术隔离手段和带宽分配策略。	7
	访问控制	主要核查：访问控制功能、协议深层检测、网络连接超时、流量限制和并发连接数限制等等。	4
	安全审计	主要核查：网络设备日志收集、分析和统计以及保护等等。	6

分类	子类	基本要求	测评项数[3]
	边界完整性检查	主要核查：是否能够对非授权设备私自联到内部网络的行为进行检查并准确定位和阻断；是否能够对内部网络用户私自联到外部网络的行为进行检查并准确定位和阻断。	2
	入侵防范	主要核查：部署 IDS 系统以及使用情况。	2
	恶意代码防范	主要核查：是否有完整的防病毒体系以及代码库的升级情况。	2
	网络设备防护	主要核查：用户身份鉴别、管理员登录地址限制、用户标识唯一性、组合鉴别技术、口令策略、登录策略、远程管理和权限分离。	9

1.2 附加指标

参照基本指标的表述模式以列表形式给出附加指标。

附加指标包括但不限于：

行业标准/规范的具体指标

主管部门的规定的具体指标

信息系统的运营、使用单位基于特定安全环境或者业务应用提出的具体指标