

# 关于印发《信息系统安全等级测评 报告模版（试行）》的通知

公信安[2009]1487号

各省、自治区、直辖市公安厅（局）公共信息网络安全监察总队（处），新疆生产建设兵团公安局公共信息网络安全监察处：

为进一步贯彻落实《信息安全等级保护管理办法》（公通字[2007]43号）和《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）文件精神，规范等级测评活动并按照统一的格式编制测评报告，我局制定了《信息系统安全等级测评报告模版（试行）》，现印发给你们，请认真贯彻落实。

公安部十一局

二〇〇九年十一月六日

报告编号：(XXXXXXXXXXXX-XX-XXXX-XX)

# 信息系统安全等级测评报告

## 模版（试行）

系统名称：\_\_\_\_\_

被测单位：\_\_\_\_\_

测评单位：\_\_\_\_\_

报告时间：\_\_\_\_\_年 月 日

## 说明：

一、每个备案信息系统单独出具测评报告。

二、测评报告编号为四组数据。各组含义和编码规则如下：

第一组为信息系统备案表编号，由 11 位数字组成，可以从公安机关颁发的信息系统备案证明（或备案回执）上获得，即证书编号的前 11 位（前 6 位为受理备案公安机关代码，后 5 位为受理备案的公安机关给出的备案单位的顺序编号）。

第二组为年份，由 2 位数字组成。例如 09 代表 2009 年。

第三组为测评机构代码，由四位数字组成。前两位为省级行政区划数字代码的前两位或行业主管部门编号：00 为公安部，11 为北京，12 为天津，13 为河北，14 为山西，15 为内蒙古，21 为辽宁，22 为吉林，23 为黑龙江，31 为上海，32 为江苏，33 为浙江，34 为安徽，35 为福建，36 为江西，37 为山东，41 为河南，42 为湖北，43 为湖南，44 为广东，45 为广西，46 为海南，50 为重庆，51 为四川，52 为贵州，53 为云南，54 为西藏，61 为陕西，62 为甘肃，63 为青海，64 为宁夏，65 为新疆，66 为新疆兵团。90 为国防科工局，91 为电监会，92 为教育部。后两位为公安机关或行业主管部门推荐的测评机构顺序号。

第四组为本年度信息系统测评次数，由两位构成。例如 02 表示该信息系统本年度测评 2 次。

## 信息系统等级测评基本信息表

信息系统				
系统名称			安全保护等级	
备案证明编号			测评结论	
被测单位				
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			单位代码	
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	
审核批准	编 制 人	(签名)	编制日期	
	审 核 人	(签名)	审核日期	
	批 准 人	(签名)	批准日期	

注：单位代码由受理测评机构备案的公安机关给出。

## 声明

(声明是测评机构对测评报告的有效性前提、测评结论的适用范围以及使用方式等有关事项的陈述。针对特殊情况下的测评工作，测评机构可在以下建议内容的基础上增加特殊声明。)

**本报告是 XXX 信息系统的等级测评报告。**

**本报告测评结论的有效性建立在被测评单位提供相关证据的真实性基础之上。**

**本报告中给出的测评结论仅对被测信息系统当时的安全状态有效。当测评工作完成后，由于信息系统发生变更而涉及到的系统构成组件（或子系统）都应重新进行等级测评，本报告不再适用。**

**本报告中给出的测评结论不能作为对信息系统内部署的相关系统构成组件（或产品）的测评结论。**

**在任何情况下，若需引用本报告中的测评结果或结论都应保持其原有的意义，不得对相关内容擅自进行增加、修改和伪造或掩盖事实。**

# 目 录

报告摘要 .....	I
1 测评项目概述 .....	1
1.1 测评目的 .....	1
1.2 测评依据 .....	1
1.3 测评过程 .....	1
1.4 报告分发范围 .....	1
2 被测信息系统情况 .....	2
2.1 承载的业务情况 .....	2
2.2 网络结构 .....	2
2.3 系统构成 .....	2
2.3.1 业务应用软件 .....	2
2.3.2 关键数据类别 .....	2
2.3.3 主机/存储设备 .....	3
2.3.4 网络互联设备 .....	3
2.3.5 安全设备 .....	3
2.3.6 安全相关人员 .....	3
2.3.7 安全管理文档 .....	4
2.4 安全环境 .....	4
2.5 前次测评情况 .....	4
3 等级测评范围与方法 .....	4
3.1 测评指标 .....	4
3.1.1 基本指标 .....	5
3.1.2 特殊指标 .....	5
3.2 测评对象 .....	5
3.2.1 测评对象选择方法 .....	5
3.2.2 测评对象选择结果 .....	5
3.3 测评方法 .....	7
4 单元测评 .....	8
4.1 物理安全 .....	8
4.1.1 结果记录 .....	8
4.1.2 结果汇总 .....	8
4.1.3 问题分析 .....	8
4.2 网络安全 .....	9
4.2.1 结果记录 .....	9
4.2.2 结果汇总 .....	9
4.2.3 问题分析 .....	9
4.3 主机安全 .....	9
4.3.1 结果记录 .....	9

---

4.3.2	结果汇总 .....	9
4.3.3	问题分析 .....	9
4.4	应用安全 .....	9
4.4.1	结果记录 .....	9
4.4.2	结果汇总 .....	9
4.4.3	问题分析 .....	9
4.5	数据安全及备份恢复 .....	9
4.5.1	结果记录 .....	9
4.5.2	结果汇总 .....	9
4.5.3	问题分析 .....	9
4.6	安全管理制度 .....	9
4.6.1	结果记录 .....	9
4.6.2	结果汇总 .....	9
4.6.3	问题分析 .....	9
4.7	安全管理机构 .....	9
4.7.1	结果记录 .....	9
4.7.2	结果汇总 .....	9
4.7.3	问题分析 .....	9
4.8	人员安全管理 .....	10
4.8.1	结果记录 .....	10
4.8.2	结果汇总 .....	10
4.8.3	问题分析 .....	10
4.9	系统建设管理 .....	10
4.9.1	结果记录 .....	10
4.9.2	结果汇总 .....	10
4.9.3	问题分析 .....	10
4.10	系统运维管理 .....	10
4.10.1	结果记录 .....	10
4.10.2	结果汇总 .....	10
4.10.3	问题分析 .....	10
5	整体测评 .....	11
5.1	安全控制间安全测评 .....	11
5.2	层面间安全测评 .....	11
5.3	区域间安全测评 .....	11
5.4	系统结构安全测评 .....	11
6	测评结果汇总 .....	12
7	风险分析和评价 .....	13
8	等级测评结论 .....	14
9	安全建设整改建议 .....	15

## 报告摘要

( 建议不超过 800 字 )

简要描述被测信息系统的名称、安全等级、承载的业务等基本情况。

简要描述测评范围和主要内容。

简要描述测评指标的符合性情况，给出测评结论（包括符合、基本符合和不符合）。

简要描述测评中发现的主要问题和危害，并提出安全建设整改建议。

# 1 测评项目概述

## 1.1 测评目的

## 1.2 测评依据

列出开展测评活动所依据的文件、标准和合同等。

## 1.3 测评过程

描述等级测评工作流程，包括测评工作流程图、各阶段完成的关键任务和工作的时间节点等内容。

## 1.4 报告分发范围

说明等级测评报告正本的份数与分发范围。

## 2 被测信息系统情况

参照备案信息简要描述信息系统。

### 2.1 承载的业务情况

描述信息系统承载的业务、应用等情况。

### 2.2 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以及本地备份和灾备中心的情况。

### 2.3 系统构成

#### 2.3.1 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。

序号	软件名称	主要功能	重要程度 <sup>1</sup>
...	...	...	...

#### 2.3.2 关键数据类别

以列表形式描述具有相近业务属性和安全需求的数据集合。

序号	数据类别	所属业务应用	主机/存储设备	重要程度
...	...	...		...

<sup>1</sup> 依据《信息系统安全等级测评过程指南》判定

### 2.3.3 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，描述主机设备的项目包括设备名称、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
...	...		...

### 2.3.4 网络互联设备

以列表形式给出被测信息系统中的网络互联设备。

序号	设备名称	用途	重要程度
...	...	...	...

### 2.3.5 安全设备

以列表形式给出被测信息系统中的安全设备。

序号	设备名称	用途	重要程度
...	...	...	...

### 2.3.6 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情况。相关人员包括（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、业务操作员、安全审计人员等。

序号	姓名	岗位/角色	联系方式
...	...	...	...

序号	姓名	岗位/角色	联系方式

### 2.3.7 安全管理文档

以列表形式给出与信息系统安全相关的文档，包括管理类文档、记录类文档和其他文档。

序号	文档名称	主要内容
...	...	...

## 2.4 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，并以列表形式给出被测信息系统的威胁列表并赋值。威胁赋值是基于历史统计或者行业判断进行的，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
...	...	...	...

## 2.5 前次测评情况

简要描述前次等级测评发现的主要问题和测评结论。

# 3 等级测评范围与方法

## 3.1 测评指标

测评指标包括基本指标和特殊指标两部分。

### 3.1.1 基本指标

依据信息系统确定的业务信息安全保护等级和系统服务安全保护等级,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。

鉴于信息系统的复杂性和特殊性(如某些信息系统未部署数据库服务器),基本指标中可能存在部分不适用项,可以在单元测评时进行识别。

安全分类 <sup>1</sup>	安全子类 <sup>2</sup>	测评项数	备注
...	...	...	

### 3.1.2 特殊指标

结合行业和系统的实际,以列表形式给出《基本要求》未覆盖或者高于《基本要求》的安全要求。

安全分类	安全子类	特殊要求描述	测评项数
...	...		...

## 3.2 测评对象

### 3.2.1 测评对象选择方法

描述测评对象的选择规则和方法。

### 3.2.2 测评对象选择结果

#### 1) 机房

序号	机房名称	物理位置

<sup>1</sup> 安全分类对应基本要求中的物理安全、网络安全、主机安全、应用安全、数据安全与备份恢复、安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理等 10 个安全要求类别。

<sup>2</sup> 安全子类是对安全分类的进一步细化,在《基本要求》目录级别中对应安全分类的下一级目录。

## 2) 业务应用软件

序号	软件名称	主要功能
...	...	...

## 3) 主机（存储）操作系统

序号	设备名称	操作系统/数据库管理系统
...	...	...

## 4) 数据库管理系统

序号	设备名称	操作系统/数据库管理系统
...	...	...

## 5) 网络互联设备操作系统

序号	操作系统名称	设备名称
...	...	...

## 6) 安全设备操作系统

序号	操作系统名称	设备名称
...	...	...

### 7) 访谈人员

序号	姓名	岗位/职责
...	...	...

### 8) 安全管理文档

序号	文档名称	主要内容
...	...	...

## 3.3 测评方法

描述等级测评工作中采用的访谈、检查、测试和风险分析等方法。

## 4 单元测评

等级测评内容包括“3.1 测评指标”中涉及的物理安全、网络安全、主机安全等 10 个安全分类，具体内容结果记录、问题分析和结果汇总等三部分构成。

### 4.1 物理安全

#### 4.1.1 结果记录

以表格形式给出物理安全的现场测评结果。

安全子类	测评指标	结果记录	符合情况
物理位置的选择	...	...	...
	...	...	...
物理访问控制	...	...	...
...	...	...	...

#### 4.1.2 结果汇总

针对不同测评指标子类对物理安全的单项测评结果进行汇总和统计。

#### 4.1.3 问题分析

针对物理安全测评结果中存在的部分符合项或不符合项加以汇总和分析，形成安全问题描述。

## **4.2 网络安全**

### **4.2.1 结果记录**

### **4.2.2 结果汇总**

### **4.2.3 问题分析**

## **4.3 主机安全**

### **4.3.1 结果记录**

### **4.3.2 结果汇总**

### **4.3.3 问题分析**

## **4.4 应用安全**

### **4.4.1 结果记录**

### **4.4.2 结果汇总**

### **4.4.3 问题分析**

## **4.5 数据安全及备份恢复**

### **4.5.1 结果记录**

### **4.5.2 结果汇总**

### **4.5.3 问题分析**

## **4.6 安全管理制度**

### **4.6.1 结果记录**

### **4.6.2 结果汇总**

### **4.6.3 问题分析**

## **4.7 安全管理机构**

### **4.7.1 结果记录**

### **4.7.2 结果汇总**

### **4.7.3 问题分析**

## **4.8 人员安全管理**

### **4.8.1 结果记录**

### **4.8.2 结果汇总**

### **4.8.3 问题分析**

## **4.9 系统建设管理**

### **4.9.1 结果记录**

### **4.9.2 结果汇总**

### **4.9.3 问题分析**

## **4.10 系统运维管理**

### **4.10.1 结果记录**

### **4.10.2 结果汇总**

### **4.10.3 问题分析**

## 5 整体测评

从安全控制间、层面间、区域间和系统结构等方面对单元测评的结果进行验证、分析和整体评价。具体内容参见《信息安全技术 信息系统安全等级保护测评要求》。

### 5.1 安全控制间安全测评

### 5.2 层面间安全测评

### 5.3 区域间安全测评

### 5.4 系统结构安全测评

## 6 测评结果汇总

一是以表格形式汇总测评结果。表格以不同颜色对测评结果进行区分，部分符合的安全子类采用黄色标识，不符合的安全子类采用红色标识。

序号	安全分类	安全子类	符合情况		
			符合	部分符合	不符合
1	物理安全	物理位置的选择			<input type="checkbox"/>
2		物理访问控制	<input type="checkbox"/>		
3		防盗窃和防破坏		<input type="checkbox"/>	
4		防雷击	<input type="checkbox"/>		
5		防火	<input type="checkbox"/>		
6		防水和防潮	<input type="checkbox"/>		
7		防静电	<input type="checkbox"/>		
8		温湿度控制	<input type="checkbox"/>		
9		电力供应	<input type="checkbox"/>		
10		电磁防护		<input type="checkbox"/>	
...	...	...	...	...	...
统计			7	2	1

二是以柱状图形式统计不同设备和安全子类的测评结果。

三是以表格形式汇总信息系统中存在的安全问题。

## 7 风险分析和评价

依据等级保护的相关规范和标准，采用风险分析的方法分析信息系统等级测评结果中存在的安全问题（等级测评结果中部分符合项或不符合项的汇总结果）可能对信息系统安全造成的影响。

分析过程包括：

- 1) 判断安全问题被威胁利用的可能性，可能性的取值范围为高、中和低；
- 2) 判断安全问题被威胁利用后，对信息系统安全（业务信息安全和系统服务安全）造成的影响程度，影响程度取值范围为高、中和低；
- 3) 综合 1) 和 2) 的结果对信息系统面临的安全风险进行赋值，风险值的取值范围为高、中和低；
- 4) 结合信息系统的安全保护等级对风险分析结果进行评价，即对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益造成的风险。

以列表形式给出等级测评发现安全问题以及风险分析和评价情况。

### 系统安全问题风险分析和评价表

序号	问题描述	关联资产 <sup>1</sup>	关联威胁 <sup>2</sup>	风险值	风险评价
一					
二					
三					
...					

<sup>1</sup> 如风险值和评价相同，可填写多个关联资产。

<sup>2</sup> 对于多个关联的情况，应分别填写。

## 8 等级测评结论

综合第 5、6、7 章的测评与分析结果，对信息系统基本安全保护状态进行综合判断，并给出等级测评结论，应表述为“符合”、“基本符合”或者“不符合”。

测评结论的判别依据如下：

测评结论	判别依据
符合	等级测评结果中不存在部分符合项或不符合项
基本符合	等级测评结果中存在部分符合项或不符合项，但不会导致信息系统面临高等级安全风险
不符合	等级测评结果中存在部分符合项或不符合项，导致信息系统面临高等级安全风险

## 9 安全建设整改建议

针对系统存在的主要安全问题提出安全建设整改建议。