**湖南省未成年犯管教所**

**网络安全等级保护测评项目**

# 项目概述

## 项目背景

网络安全等级保护制度是我国网络安全保障工作的基本制度、基本策略和基本方法，是促进信息化健康发展，维护国家安全、社会秩序和公共利益的根本保障。国务院法规（国务院[1994]147号令）和中央文件（中办发[2003]27号文）明确规定，要实行信息安全等级保护，重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度。2017年6月1日正式施行的《中华人民共各国网络安全法》（主席令第五十三号）第二十一条明确规定国家实行网络安全等级保护制度。因此，开展网络安全等级保护工作不仅是保障重要信息系统安全的重大措施，也是一项事关国家安全、国家利益、社会稳定的重要任务，同时也是网络运营者应当履行的安全保护义务。

面对我国信息安全的严峻形势，国家采取了一系列重大举措加大网络安全和信息化发展的力度，将“网络安全”上升到国家战略。

近些年来，随着信息化的不断发展，信息系统的应用成为业务重要支撑平台，关键流程、重要数据的处理都依赖于信息系统，为切实减少未管所信息系统安全风险、保障信息系统安全运行，需开展信息系统安全等级保护测评工作，找出未管所系统与国家标准要求之间的差距，对存在的风险进行评估。

## 项目目标

依据《信息安全技术网络安全等级保护基本要求》（以下简称《基本要求》）二级和三级要求，对湖南省未成年犯管教所触发式报警系统、安防集成平台进行等级测评，找出系统与国家标准要求之间的差距，对存在的风险进行评估，并出具《信息安全等级测评报告》和《差距分析报告》。

# 项目内容

1、聘请第三方具有等保测评资质的公司，协助湖南省未成年犯管教所对信息系统进行定级，协助编写定级报告。

2、聘请第三方具有等保测评资质的公司，对未管所定级系统进行差距分析，如差距分析结果不能通过测试，则出具整改方案指导未管所进行安全整改，待安全整改后进行复测试。

3、第三方具有等保测评资质的公司测评后出具等级测评报告。

4、第三方具有等保测评资质的公司协助湖南省未成年犯管教所向所在地区的公安机关办理备案手续，获得备案证。



## **定级**

聘请第三方具有等保测评资质的公司协助我所，依据《网络安全等级保护定级指南》，确定信息系统的安全保护等级，编写定级报告。

系统定级阶段需完成以下工作：

1. 等级保护的培训：在进行测评服务之前，对我所信息技术人员进行等级保护的内容培训。
2. 系统业务安全域划分：进行信息收集和资产调研，明确业务系统的范围、边界、功能以及重要性等。
3. 协助我所召开专家评审会、获得备案证明：定级和备案是等级保护工作开展的前提，如果级别定错了，或者专家有不同的评审意见，则后续的测评将无法进行。

## **差距评估**

差距评估是以国际安全标准、行业最佳实践、国家安全法规及标准为依据，对客户网络与信息系统的资产价值、潜在的安全威胁、薄弱环节、现有安全防护措施等进行综合分析，以发现信息系统中存在的主要安全问题，并找到解决这些问题的方法。

聘请第三方具有等保测评资质的公司，依据差距分析表中的各项安全要求，通过人员访谈、现场检查和测试对比现状和安全要求之间的差距，确定不满足要求的安全项。通过等级差距评估，可以明确我所信息系统的现状，确定不符合安全项，找出目前信息系统与等级保护安全要求之间的差距，有针对性地提出整改建议。

## **安全整改方案设计**

参考国家标准《网络安全等级保护基本要求》、《网络安全等级保护安全设计技术要求》，依据差距分析的结论，结合我所实际情况，给出《安全整改方案》。

## **等级测评**

在我所根据第三方测评公司整改方案进行整改后，第三方公司再对我所定级备案的信息系统开展信息系统等级保护测评工作，并出具《等级测评报告》。

## **协助备案**

准备定级备案表和定级报告，协助湖南省未成年犯管教所向所在地区的公安机关办理备案手续，获得备案证（如系统已经取得备案证明，则协助取得公安部门出具的《信息系统安全等级保护测评报告回执单》）。

## **协助整改**

为协助我所通过等保测评及增强我所信息系统安全防护能力，第三方测评公司在开展等保测评时将同时为我所应用服务器部署防护工具“网防G01”，全称“网站综合防护系统”，是首款专门针对WEB应用服务器等关键信息基础资源进行综合防护的产品，由公安部第一研究所和计算机病毒防治技术国家工程实验室（北京）研发，该系统采用C/S与B/S的结合，通过PC端、客户端、浏览器即可实现对服务器端的安全管理与监控。系统跨平台支持Windows及Linux双操作系统，以操作系统内核加固技术、web访问控制技术作为核心防御体系，针对操作系统核心资源，如注册表、网络连接、系统文件、进程等进行有效防护，同时，采用web访问控制技术有效抵御网络层攻击。

# **项目实施流程**

 根据我所系统的等级与规模，测评时间进度为30天左右，具体工作流程见下表，第三方测评公司应派遣具有等保测评资质的人员负责本项目的实施工作，项目组人员不得少于5人，并能根据一些特殊的情况可以适当增加测评人员。

|  |  |
| --- | --- |
| **工作流程** | **时间** |
| 测评准备活动 | 1．项目启动 | 组建测评项目组 | 2天 |
| 编制项目计划书 |
| 确定湖南省未成年犯管教所应提供的资料 |
| 2．信息收集和分析 | 查阅定级报告、系统描述文件、系统安全设计方案、自查或上次等级测评报告(如果做过资产或等级测评)等资料 | 2天 |
| 根据查阅到的系统情况调整调查表内容 |
| 发放调查表给湖南省未成年犯管教所 |
| 协助湖南省未成年犯管教所填写调查表 |
| 收回调查结果 |
| 根据情况确定是否安排现场调查 |
| 分析调查结果 |
| 3．工具和表单准备 | 调试测评工具 | 1天 |
| 模拟被测系统搭建测评环境 |
| 模拟测评 |
| 准备和打印表单 |
| 方案编制活动 | 1．测评对象确定 | 识别被测系统等级 | 1天 |
| 识别被测系统的整体结构 |
| 识别被测系统的边界 |
| 识别被测系统的网络区域 |
| 识别被测系统的重要节点和业务应用 |
| 确定测评对象 |
| 2．测评指标确定 | 识别被测系统业务信息和系统服务安全保护等级 |
| 选择对应等级的ASG三类安全要求作为测评指标 |
| 就高原则调整多个定级对象共用的某些物理安全或管理安全测评指标 |
| 3．测试工具接入点确定 | 确定工具测试的测评对象 |
| 选择测试路径 |
| 确定测试工具的接入点 |
| 4．测评内容确定 | 识别每个测评对象对应的测评指标 | 1天 |
| 识别每个测评对象对应的每个测评指标的测评方法 |
| 5．测评指导书开发 | 从已有的测评指导书中选择与测评对象对应的手册 |
| 针对没有现成测评指导书的测评对象，开发新的测评指导书 |
| 6．测评方案编制 | 描述测评项目基本情况和工作依据 | 1天 |
| 描述被测系统的整体结构、边界和网络区域 |
| 描述被测系统的重要节点和业务应用 |
| 描述测评指标 |
| 描述测评对象 |
| 描述测评内容和方法 |
| 现场测评活动 | 1．现场测评准备 | 现场测评授权书签署 | 2天 |
| 召开现场测评启动会 |
| 双方确认测评方案 |
| 双方确认配合人员、环境等资源 |
| 确认信息系统已经备份 |
| 测评方案、结果记录表格等资料更新 |
| 2．现场测评和结果记录 | 依据测评指导书实施测评 | 7天 |
| 记录测评获取的证据、资料等信息 |
| 汇总测评记录，如果需要，实施补充测评 |
| 3．结果确认和资料归还 | 召开现场测评结束会 | 1天 |
| 湖南省未成年犯管教所确认测评过程中获取的证据和资料的正确性，并签字认可 |
| 测评人员归还借阅的各种资料 |
| 分析与报告编制活动 | 1．单项测评结果判定 | 分析测评项所对抗威胁的存在情况 | 1天 |
| 分析单个测评项是否有多方面的要求内容, 依据“优势证据”法选择优势证据，并将优势证据与预期测评结果相比较 |
| 综合判定单个测评项的测评结果 |
| 2．单元测评结果判定 | 汇总每个测评对象在每个测评单元的单项测评结果 | 1天 |
| 判定每个测评对象的单元测评结果 |
| 3．整体测评 | 分析不符合和部分符合的测评项与其他测评项（包括单元内、层面间、区域间）之间的关联关系及对结果的影响情况 | 2天 |
| 分析被测系统整体结构的安全性对结果的影响情况 |
| 4．风险分析 | 整体测评后的单项测评结果再次汇总 | 3天 |
| 分析部分符合项或不符合项所产生的安全问题被威胁利用的可能性 |
| 分析威胁利用安全问题后造成的影响程度 |
| 为被测系统面临的风险进行赋值 |
| 评价风险分析结果 |
| 5．等级测评结论形成 | 统计再次汇总后的单项测评结果为部分符合和不符合项的项数 | 1天 |
| 形成等级测评结论 |
| 6．测评报告编制 | 概述测评项目情况 | 3天 |
| 描述被测系统情况 |
| 描述测评范围和方法 |
| 描述单元测评情况 |
| 描述整体测评情况 |
| 汇总测评结果 |
| 描述风险情况 |
| 给出等级测评结论和整改建议 |
| 总结汇报阶段 | 1．编制汇报材料 | 从测评过程及测评结论、风险、整改建议等方面编写汇报材料 | 1天 |
| 2．进行汇报总结 | 针对测评过程及测评结论、风险、整改建议等向被测单位领导层汇报 |
| 3．项目验收 | 双方确认测评结果后进行测评项目验收工作，并对测评报告进行备案 |

# 四、项目预算清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **服务名称** | **服务内容** | **数量** | **备注** |
| 1 | 等级保护二级系统测评(触发式报警系统) | 定级备案 | 1次 | 按照等保2.0二级要求对触发式报警系统进行测评。出具《差距分析报告》、《信息系统安全等级保护测评报告》 |
| 专家评审 | 1次 |
| 差距分析 | 1次 |
| 协助整改 | 1次 |
| 等保测评 | 1次 |
| 2 | 等级保护三级系统测评(安防集成平台) | 定级备案 | 1次 | 按照等保2.0三级要求对安防集成平台进行测评。出具《差距分析报告》、《信息系统安全等级保护测评报告》 |
| 专家评审 | 1次 |
| 差距分析 | 1次 |
| 协助整改 | 1次 |
| 等保测评 | 1次 |
| 3 | 安全加固 | 服务器加固 | 1次 | 在应用服务器上部署“网防G01”安全加固软件，提升服务器网络安全防护能力。 |

**项目预算总价：125000元。**

**竞价要求**

1. **投标人须具有公安部第三研究所颁发的：网络安全等级测评与检测评估机构服务认证证书（提供扫描件并加盖公章上传），否则视为无效竞价。**
2. **投标人须具有中国网络安全审核技术与认证中心颁发的信息安全服务资质认证证书-信息安全风险评估资质、信息系统安全运维资质、信息安全应急处理服务资质（提供扫描件并加盖公章上传），否则视为无效竞价。**
3. **投标人须具备公安部指定的网防安全服务中心授牌（提供照片并加盖公章上传），否则视为无效竞价。**
4. **预成交商签订合同之前需提供涉密信息系统集成资质（运行维护）证明文件，否则视为无效竞价。**