附件一、宁夏巨灾防范工程等级保护测评服务项目内容

# 等级保护测评服务项目内容

## **项目概况**

宁夏回族自治区地震局根据《中华人民共和国网络安全法》、《中华人民共和国计算机信息系统安全保护条例》(国务院147号令)、《信息安全等级保护管理办法》(公通字[2007]43号)和《关于印发<宁夏回族自治区贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的实施意见>的通知》宁公（网安）通[2021]42号文等文件的要求，计划开展信息系统等级保护测评工作。测评机构应以国标委发布的《信息安全技术网络安全等级保护基本要求》(GB/T22239-2019)等标准为主要依据，制定系统安全等级保护评测具体内容，开展外部评测工作。通过等级保护测评，验证宁夏回族自治区地震局信息系统的安全性，并对信息系统的安全防护能力提出建议和意见，为进一步完善信息系统的安全防护措施提供依据。通过此次等保测评，有效控制安全风险，完善网络安全体系，修补安全漏洞，提升宁夏回族自治区地震局网络安全建设和风险抵御能力，确保运营的系统达到网络安全等级保护的要求。

自治区地震局需要测评的系统如下：

|  |  |  |
| --- | --- | --- |
| **序号** | **系统名称** | **定级情况** |
| 1 | 门户网站 | 二级 |
| 2 | OA（含档案系统） | 二级 |
| 3 | 地震灾害防御体系信息系统（宁夏震灾防御基础数据库系统、地市级地震灾害防御数据与业务应用服务终端系统） | 二级（拟定） |
| 4 | 综合业务系统（应急业务系统、地震数据处理系统与信息发布系统、地震信息服务可视化平台、地震模拟与触发系统、走时拾取及地震精定位平台、地震实时智能处理系统（AIRES）、地震智能数字人/机器人）） | 二级 |

另：本项目需提供3人的CISP培训服务。

注：系统名称和等保级别以公安机关出具的《备案证明》为主，系统发生变化时需要提供系统定级备案变更等服务。

## **服务需求说明**

### 项目需求

等级测评内容测评的内容包括但不限于以下内容：

一是安全技术测评：安全物理环境、安全计算环境、安全通信网络、安全区域边界、安全管理中心五个方面的安全测评。

二是安全管理测评：安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理五个方面的安全测评。

### 测评范围

测评机构需针对指定的系统，根据《基本要求》中规定的五个安全技术和五个安全管理方面的内容进行现场测评，包括但不限于：

■主机房（包括其环境、设备和设施等）、办公场地；

■存储被测系统重要数据的介质的存放环境；

■整个系统的网络拓扑结构；

■安全设备，包括防火墙、IPS等；

■对整个信息系统或其局部的安全性起作用的网络互联设备，如核心交换机、路由器等；

■承载业务处理系统主要业务或数据的服务器（包括其操作系统和数据库）；

■业务应用系统管理终端和主要文件传输系统终端；

■终端计算机；

■信息安全主管人员；

■涉及到信息系统安全的所有管理制度和记录。

### 保密要求

测评机构对项目实施过程中所获得数据及文档等保密信息，承担以下保密义务：

1.服务方应按要求与委托方签署保密协议。

2.服务方应主动采取加密措施对上述所列及之保密信息进行保护，防止不承担同等保密义务的任何第三者知悉及使用。

3.服务方不得刺探或者以其他不正当手段（包括利用计算机进行检索、浏览、复制等）获取与本职工作或本身业务无关的甲方关于该项目的商业秘密。

4.服务方不得向不承担同等保密义务的任何第三人披露甲方关于该项目的商业秘密。

5.服务方不得允许（包括出借、赠与、出租、转让等行为）或协助不承担同等保密义务的任何第三人使用甲方关于该项目的商业秘密。

6.不论何种原因终止参与委托方关于该项目的工作后，服务方都不得利用该项目之商业秘密为其他与委托方有竞争关系的企业（包括自办企业）服务。

7.该项目的商业秘密所有权始终全部归属委托方，服务方不得利用自身对项目不同程度的了解申请对于该项目的商业秘密所有权。

8.如发现委托方关于该项目的商业秘密被泄露或者自己过失泄露秘密，服务方应当采取有效措施防止泄密进一步扩大，并及时向委托方相关部门报告。

### 项目安排

1.测评机构的项目安排应该按照等级保护相关标准进行，项目测评周期为45个工作日。

2.等级测评过程分为四个基本测评活动：测评准备活动、方案编制活动、现场测评活动、分析及报告编制活动。

3.测评准备活动包括项目启动、信息收集和分析、工具和表单准备三项主要任务。

4.方案编制活动主要包括编制测评方案（包括编制配套的作业指导书）、评审和提交测评方案等。

5.现场测评活动是开展等级测评工作的核心活动，主要活动包括方案确认和资源协调、现场测评和结果记录、结果确认和资料归还。

6.分析及报告编制活动的主要任务是根据现场测评结果和等级测评的有关要求，通过单项测评结果判定、单元测评结果判定、整体测评和风险分析等方法，找出整个系统的安全，保护现状与相应等级的保护要求之间的差距，并分析这些差距导致被测系统面临的风险，从而给出等级测评结论，形成测评报告文本。

### **项目管理要求**

测评机构须委派一名代表作为项目经理，代表测评机构与委托方共同统筹及协调一切与本项目有关的事项，领导并监督项目组中人员的工作情况。双方委派的项目经理及其他人员组成本项目协调委员会，定时审查及监督项目实施过程，处理项目实施中的各项变更事宜。

### 服务方人员素质要求

测评机构具备《网络安全等级测评与检测评估机构服务认证证书》，测评机构测评人员必须具备等级测评师的相关证书及资质，熟悉检测流程，了解和掌握与被检单位有关的专业知识及相关的规范、规定，包括国家标准规范、行业规范、地方标准以及有关的安全程序、操作规程等。

检测人员进入检测现场，必须遵守委托方的有关安全规章制度，听从采购方安全监督管理人员的安排。

### 项目实施经验要求

供应商必须指派一名中级测评师作为现场项目经理，负责项目协调和测评工作。

### 成果文件要求

提交4个信息系统的测评报告，每个系统测评报告一式四份。供应商所提供的等级保护测评报告需具有等级保护测评专用章。