# 总体要求

**项目名称:**网络安全等级保护测评

**期限：**从合同签订之日30个工作日完成。

**预算：20**万元

**测评内容：三级系统2个，二级系统2个**；

**付款方式：**测评结果覆盖全面，符合等保相关标准，整体验收后支付100%

# 资格要求

1. 要求必须具备独立法人资格、无不良信用信息记录；

2. 具有独立承担民事责任的能力；

3. 投标单位组建的项目组成员必须提供《等级保护测评师证书》；

三、技术要求

**1、项目背景**

 等级保护是国家关于信息安全的基本政策，《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发【2003】27号），（以下简称27号文）明确要求我国信息安全保障工作实行等级保护制度，提出“抓紧建立信息安全等级保护制度制定信息安全等级保护的管理办法和技术指南”。

根据国家的相关要求进行信息安全等级保护测评。

**2、项目目的**

本项目是按照等级保护防护的要求对本项目内所包括的信息系统开展可控的安全等级保护符合性测评，通过测评发现系统中存在的安全漏洞和安全隐患，提出安全整改意见，从而有效降低系统遭受具有政治目的、经济目的的恶意攻击的可能性，以提高安全保障能力和防护水平；同时，测评报告将作为进一步完善系统安全防护措施的依据。

**3、项目依据**

《关于信息安全等级保护工作的实施意见》（公通字【2004】66号）

《信息安全等级保护备案实施细则》（公信安【2007】1360号）

《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 22240-2008 信息系统安全等级保护定级指南》

《GB/T 28448-2012 信息安全技术 信息系统安全等级保护测评要求》

《GB/T 28449-2012 信息安全技术 信息系统安全等级保护测评过程指南》

《GB/T 25058-2010 信息安全技术 信息系统安全等级保护实施指南》

《GB17859-1999 计算机信息系统安全保护等级划分准则》

《信息系统安全等级保护测评报告模版（2015年版）》（公信安【2014】2866号）

**4、项目内容**

（1）等级保护测评服务

等级保护测评内容包括但不限于以下内容（本项目中不同系统实际测评内容以具体测评要求为准）：

1. 安全技术测评：包括物理安全、网络安全、主机系统安全、应用安全和数据安全五个方面的安全测评；
2. 安全管理测评：安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理五个方面的安全测评。

1.1物理安全

根据系统机房和现场安全测评记录，针对这两个系统机房和现场在“物理位置选择”、“物理访问控制”、“防盗窃和防破坏”、“防雷击”、“防火”、“防水和防潮”、“防静电”、“温湿度控制”、“电力供应”和“电磁防护”等物理安全方面所采取的措施进行，判断出与其相对应的各项测评项的测评结果。

1.2网络安全

根据现场网络安全测评记录，针对这两个系统网络方面在“结构安全”、“访问控制”、“审计安全”、“边界完整性检查”、“入侵防范”、“恶意代码防范”、“网络设备防护”等网络安全方面所采取的措施进行检查，判断出与其相对应的各测评项的测评结果。

1.3主机安全

针对这两个系统主机安全现场测评内容包括“身份鉴别”、“访问控制”、“安全审计”、“剩余信息保护”、“入侵防护”、“恶意代码防护”、“资源控制”。

1.4应用安全

 针对这两个系统应用安全现场测评包括对系统“身份鉴别”、“访问控制”、“安全审计”、“剩余信息保护”、“通信完整性”、“通信保密性”、“抗抵赖”、“软件容错”、“资源控制”方面。

1.5数据安全及备份恢复

 针对这两个系统现场测评内容包括“数据完整性”、“数据保密性”、“备份和恢复”几个方面进行测评。

1.6安全管理制度

根据现场安全测评记录，在安全管理制度方面的“管理制度”、“制定和发布”以及“评审和修订”等测评指标，判断出与其相对应的各测评项的测评结果。

1.7安全管理机构

 根据现场安全测评记录，应在安全管理机构方面的“岗位设置”、“人员配备”、“授权和审批”、“沟通与合作”以及“审核和检查”等测评指标，判断出与其相对应的各测评项的测评结果。

1.8人员安全管理

根据现场安全测评记录，应在人员安全管理方面的“人员录用”、“人员离岗”、“人员考核”、“安全意识教育和培训”以及“外部人员访问管理”等测评指标，判断出与其相对应的各测评项的测评结果。

1.9系统建设管理

根据现场安全测评记录，对系统建设管理方面的“系统定级”、“安全方案设计”、“产品采购和使用”、“自行软件开发”、“外包软件开发”、“工程实施”、“测试验收”、“系统交付”、“系统备案”、“等级测评”以及“安全服务商选择”等测评指标，判断出与其相对应的各测评项的测评结果。

1.10系统运维管理

根据现场安全测评记录，在系统运维管理的“环境管理”、“资产管理”、“介质管理”、“设备管理”、“网络安全管理”、“备份与恢复管理”、“安全事件处置”以及“应急预案管理”等测评指标，判断出与其相对应的各测评项的测评结果。

（2）安全培训服务

根据采购人的具体工作情况，结合等级保护人员方面的相关要求，依托我国信息安全培训体系，要求服务方派遣具备国家注册信息安全培训讲师资质（CISI）的培训师进行不少于2次的信息安全培训，培训内容包括：信息安全意识、常见的WEB攻击与防护、信息安全事件处理，应急响应与灾难恢复等内容。

**5、服务实施要求**

在项目实施过程中，服务方应做好计划与安排，不影响委托单位正常业务办公的开展。服务方要给予承诺，并承担由此引起的损失。

（1）在等保测评过程中，每周五下午实施方需提交工作周报，内容应包括本周工作内容和下周工作安排等内容。

（2）等保测评工作应严格按照双方确认的工作方案开展，如遇任何变动，须在工作周报中及时提出，经采购人批准后方可变更。

（3）测评过程中实施方测评人员须记录在途经路径上涉及的可被利用存在漏洞的相关主机等设备的信息，以便于被测单位对相关漏洞进行全面修补。

（4）测评工作全部结束后实施方测评人员须卸载安置在目标机器或途径机器上的各类工具、脚本、文件等，还原各机器和系统的原始状态。

（5）测评结果中应包括测评过程中发现的所有漏洞，不能遗漏。

（6）在测评过程中若发现重大安全问题（如已被控制或存在严重安全隐患等），测评机构应在24小时之内以书面形式通知甲方，以便甲方第一时间做出处理。

（7）测评过程中，实施方测评人员在进入被测单位办公网络后若发现测评范围之外的未知信息系统，须列出系统名称、服务器IP地址、操作系统类型、数据库系统类型等信息，并与采购人协商是否继续进行测评。

（8）测评过程中不得获取测评范围以外的数据，获取的数据不得用于本次测评以外的其他用途。

（9）测评过程中应控制风险，防止测试对网络及系统运行造成影响，因测试造成系统运行问题应及时报告。

（10）测评过程中，测评机构应该针对被测系统发现的漏洞提交可行性的解决方案。

（11）需对被测系统进行全面、专业的渗透测试，发现应用系统存在的安全隐患，并出具渗透测试报告，测评机构有义务告知并协助开发厂商分析漏洞的成因及补救措施。

**6、保密要求**

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）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。

（2）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。

（3）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。

（4）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。

（5）不论何种原因终止参与委托方方关于该项目的工作后，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。

（6）该项目的商业秘密所有权始终全部归属委托方，被委托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，在本协议签订前被委托方已依法具有某些所有权者除外。

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，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。

**7、质量保证**

（1）为保证信息安全等级测评项目质量，要求在测评过程中就等级测评过程控制、等级测评过程监督、等级测评结果的验证等方面严格按照国家相关标准要求执行；测评方需对服务实时过程中可能发生的突发事件提供应急预案和应急响应服务方案。项目组成员应至少具有2名拥有“信息安全保障人员（应急服务（专业级））”证书；

（2）为确保测评过程中风险评估工作的服务质量与准确性，项目组成员应至少具有2名拥有“信息安全保障人员（风险管理（专业级））”证书

（3）参与等级测评的每个人都应具有等级保护测评师证书；

（4）为了保证投标单位更好的履行本项目中所包含的各项网络安全服务需求，具有《中国信息安全认证中心》颁发的《信息安全服务资质认证证书》（包含信息安全应急处理、信息系统安全运维、信息安全风险评估等服务资质）。