# 项目需求

## 1.概述

为做好网络安全保障工作，按照“全面排查风险、及时发现预警、快速有效处置、确保万无一失”的工作目标，确保关键时期不发生网络安全相关事件，保障重要信息系统平稳运行。拟对重要系统开展等级保护测评工作，投标人需要提供切实有效的整改方案、并提供整改咨询方案；对整改后的信息系统进行回归测评，最终达到国家等级保护相关要求。

## 2.维保服务内容

|  |  |  |
| --- | --- | --- |
| 序号 | 系统名称 | 级别 |
| 1 | 业财系统 | 二级 |

## 3.服务响应要求

3.1服务内容：

（1）协助开展系统和重要信息系统的自查自评估工作，对存在的风险隐患和安全问题及时提供有针对性的安全整改建议，保障整改措施的落实，指导完成重要信息系统的定级、备案等相关工作；

（2）依据《信息系统安全等级保护基本要求》，从安全技术和管理两个方面共十个层面对信息系统进行等级测评，出具等级测评报告。

（3）针对信息系统等保测评实施过程中发现的安全隐患和薄弱环节，提供安全建设整改和安全加固方面的咨询。

（4）提供国家和行业有关信息安全等级保护政策和标准方面的知识培训和安全管理咨询，增强信息安全意识。

|  |  |  |
| --- | --- | --- |
| **项目** | **服务内容** | **工作描述** |
| 等级测评 | 项目准备及现场调研 | 协助对信息系统物理环境、网络、终端、数据、安全管理等进行调研。**【具体要求详见3.1.1-3.1.10】** |
| 信息系统定级、备案 | 疏理信息系统定级工作，完成信息系统定级报告及定级材料的准备；整理、补充信息系统备案所有相关的文档，指导用户方完成相应信息系统等级保护备案工作。**【备注：原则上已取得信息系统备案证明的系统不需要重新备案】** |
| 信息系统差距分析 | 对定级的信息系统，依照《信息系统安全等级保护基本要求》进行逐个对照，由具备等级测评师、网络与息信安全管理员或同等技术能力资质的服务人员对信息系统安全情况与等级保护基本要求的差距进行评估，完成信息系统等级保护差距分析报告。 |
| 等级保护安全整改 | 协助落实相关的等级保护建设整改工作，等级保护整改实施具体内容包括安全管理制度修订、安全技术整改、形成安全配置基线、辅助进行安全增强配置和调试指导工作等工作内容，提升信息系统的安全防护能力，确保信息系统满足国家等级保护相应等级要求。 |
| 等级保护测评 | 参照《GBT22239-2019 网络安全等级保护基本要求》和《GB/T28448-2019 网络安全等级保护测评要求》等标准规范要求，对信息系统开展信息系统等级保护测评工作。  |
| 成果 | 服务目标为通过公安部门的等级保护检查，输出《信息系统等级保护测评报告》协助用户取得公安机关备案证明（已备案信息系统不需要再次出具备案证明）。 |

3.1.1安全物理环境

物理安全测评是对信息系统的机房和办公场所的物理位置选择、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、电磁防护等方面的安全状况。

3.1.2安全通信网络

网络安全测评是对信息系统的网络系统安全防护情况进行测评，包括网络结构安全、网络访问控制、网络安全审计、网络边界完整性测评、网络入侵防范、网络恶意代码防范、网络设备防护等方面的安全状况。

3.1.3安全区域边界

安全区域边界是对信息系统的边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证等方面的安全状况。

3.1.4安全计算环境

安全计算环境是对信息系统的身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护等方面的安全状况。

3.1.5安全管理中心

安全管理中心是对信息系统的系统管理、审计管理、安全管理、集中管控进行测评。

3.1.6安全管理制度

安全管理制度测评是对信息系统的安全策略、管理制度、制定和发布、评审和修订等情况进行测评。

3.1.7安全管理机构

安全管理机构测评是对信息系统的岗位设置、人员配备、授权与审批、沟通和合作、审核和检查等情况进行测评。

3.1.8安全管理人员

人员安全管理测评是对信息系统相关内部人员的人员录用、人员离岗安全意识教育和培训、外部人员访问管理等情况进行测评。

3.1.9安全建设管理

系统建设管理测评是对信息系统建设过程中的、测试验收、系统交付、等级测评服务投标人管理等情况进行测评。

3.1.10安全运维管理

系统运维管理测评是对信息系统运行维护过程中的环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理、外包运维管理等情况进行测评。

## 4.整体要求

4.1投标人具备公安部第三研究所认证发放的《网络安全服务认证证书等级保护测评服务认证》、具有中国网络安全审查技术与认证中心出具的专业信息安全服务资质）。

4.2投标人应详细描述本次信息系统安全等级保护测评的整体实施方案，包括项目概述、等级保护测评方案、测试过程中需使用测试设备清单、时间安排、阶段性文档提交等。

4.3投标人提供参与本项目的测评人员的组成、资质及各自职责的划分，参与现场人员的项目经理具备网络安全等级测评师证书（高级）资质或信息安全管理体系ISO27001主任审核员资质。参与本项目测评人员不少于5人，应配置有网络安全等级测评资质或网络与信息安全管理员等专业人员开展测评工作。

4.4本次信息系统安全等级保护测评实施过程中所使用到的各种工具软件由成交人推荐，经采购人确认后由成交人提供并在信息系统等级保护测评中使用。

4.5信息系统安全等级保护测评需要的运行环境（如场地、网络环境等）由采购人提供，投标人应详细描述需要的运行环境的具体要求。

4.6投标人必须具备项目所在省售后服务能力，出现安全事件能第一时间达到用户现场，要求售后服务团队成员不少于20人（需要提供近半年项目所在省的社保证明）。

4.7专用工具要求

本项目涉及工程实施和验收测试所需的工具，由投标人负责提供。用于测评的工具主要包括服务器安全测评工具、网络设备安全测评工具、终端计算机安全测评工具、网站等应用系统安全测评工具等。在使用前，应对工具进行测评，如果需要则对工具进行软件或代码升级。

4.8安全管理要求

为做好全过程的安全保密工作，在等级保护测评前、中、后三个阶段都要做好安全保密工作。

4.8.1等级保护测评前

（1）对等级保护测评人员要进行安全保密教育，制定安全保密措施。

（2）签订安全保密协议。

4.8.2等级保护测评中

（1）对被测单位的性质、机房物理位置、网络与系统、应用与服务、资料与数据、人员与管理等方面的信息进行严格的安全保密管理。

（2）等级保护测评工具应经过严格测试和检验，确保不对被测评系统造成损失，工作结束后不驻留任何程序。

（3）对被测单位信息系统的信息资产、发现的脆弱性和发生过的安全事件等威胁情况要控制知情范围。

（4）对测评设备、介质进行严格的保密管理。

（5）工作过程中对人员要实施封闭式集中管理.

（6）对进场人员遵守被测单位的相关管理规定。

4.8.3等级保护测评后

（1）认真清退各种文档、资料和数据并予以销毁，确保工作过程中敏感数据不被泄漏。

（2）现场工作结束后，按被测单位的要求及时还原系统，确保系统中不遗留任何代码或可执行程序。

（3）在其他风险测评任务或宣传材料中不涉及被测单位的秘密、敏感情况。

4.9文档要求

文档或报告的编写应完整清晰、用词规范、简明扼要，指出的问题应明确合理、符合逻辑、且有证据，出具的结论应公正客观、实事求是，提出的建议应符合国家标准规范、富有建设性和可操作性。

4.10售后服务

投标人应承诺能按要求实现本技术规范规定的所有条款及功能要求，配合完成相关政府部门的信息安全等级保护相关（登记、整改等）工作要求。

## 5.保密要求

投标人在服务过程中所接触到招标人商业秘密的相关内容，包括但不限于技术秘密、经营秘密、客户信息、市场策略等信息，应承担守商业秘密的保密责任，如有严重影招标人声誉或利益的行为，须承担相应的法律责任和赔偿责任，招标人保留追究其法律责任的权利。