附件1

采购需求一览表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 服务名称 | 服务描述 | 测评数量 | 售后服务 |
| 1 | 等级保护测评 | 依据GB/T 22239-2019 《网络安全等级保护基本要求》对金凤实验室官网、远程诊断系统、实验室大脑进行三级等保测评。 | 3套 | 1年 |
| 2 | 定级备案 | 协助完成远程诊断系统、门户网站、实验室大脑的定级备案工作。 |

一、技术需求

（一）质量要求及执行标准

依据GB/T 22240-2020 《网络安全保护等级定级指南》、GB/T 22239-2019 《网络安全等级保护基本要求》等法规要求对金凤实验室官网、远程诊断系统、实验室大脑进行网络安全等级保护测评。在服务实施过程中，对项目进行规范化管理，确保项目服务质量可控和过程文档完整。针对服务中发现的安全问题，成交人需通过专业的技术手段进行合理分析，正确评估风险，协助采购人完成整改工作。

（二）技术参数

测评范围主要包括：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等方面。

1.技术测评

（1）安全物理环境测评（物理位置的选择、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）；

（2）安全通信网络测评（网络架构、通信传输、可信验证）；

（3）安全区域边界测评（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）；

（4）安全计算环境测评（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）；

（5）安全管理中心测评（系统管理、审计管理、安全管理、集中管控）。

2.管理测评

（1）安全管理制度测评（安全策略、管理制度、制定和发布、评审和修订）；

（2）安全管理机构测评（岗位设置、人员配备、授权和审批、沟通和合作、审核和检查）；

（3）安全管理人员测评（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）；

（4）安全建设管理测评（定级和备案、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、系统支付、等级测评、服务供应商选择）；

（5）安全运维管理测评（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）。

二、商务需求

（一）实施要求

1.实施时间：成交人应在采购合同生效后，3个日历日内到采购人指定地点开展等级保护测评工作。

2.实施地点：重庆市高新区（采购人指定地点）。

3.实施方式：成交人按照合同约定和采购人要求开展等级保护测评工作。

（二）售后服务

在服务周期内，为采购人提供信息安全规划、方针、策略和管理制度体系咨询服务，配合对被检测系统安全加固提供技术指导。并且在重大信息安全检查或网络安全安保工作中，向采购人提供相关技术支撑服务。

（三）付款方式

出具测评报告后，15个工作日内支付合同金额的70%，取得定级备案证明材料后15个工作日内支付合同金额的30%，支付前供应商应开具等额服务发票。

（四）验收方式

具体组织程序、验收标准和方法，按采购人规定程序执行，成交人配合。

（五）知识产权

采购人在中华人民共和国境内使用报价人提供的产品及服务时免受第三方提出的侵犯其专利权及知识产权的起诉。如果第三方提出侵权指控，成交人应承担由此而引起的一切法律责任和费用。

（六）其他

1.依照渝网通〔2016〕11号文《重庆市网络与信息安全信息通报工作规范》要求，成交人需协助网络安全事件应急处置机制建设工作，落实本单位的网络安全应急处置通报工作。成交人需为重庆市网络与信息安全信息通报机制成员单位或重庆市网络与信息安全信息通报中心支撑单位（提供证明文件），按渝网通〔2016〕11号文开展相关通报工作。

2.成交人不得存在因违规经营网络安全等级测评业务受到行业主管部门、资质颁发机构、政府部门通报批评或者暂停测评资质使用、经济处罚、暂停测评业务、责令整改、吊销测评资质等处罚。