喀什地区数字化发展局政务云机房等级保护测评服务项目需求

一、项目概述

本项目主要对喀什地区数字化发展局政务云机房进行等级保护测评服务工作。为使得政务云机房达到相应等级的安全防护水平，指导用户完成政务云机房安全整改建设工作并提供网络安全等级保护测评服务，建立信息安全管理制度体系，协助用户完成政务云机房安全等级保护其他相关工作。

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 系统名称 | 保护等级 | 备注 |
| 1 | 政务云机房 | 三级 |  |

1. 项目概算

项目概算约10万元人民币。

## 三、企业资质要求

1.供应商须符合《中华人民共和国政府采购法》第二十二条规定的条件；

2.供应商须是中华人民共和国境内注册的，具有独立法人资格的企业（营业执照包含本次项目服务的经营范围）；

3.供应商须具有良好的商业信誉和健全的财务会计制度；

4.供应商须提供公安部门颁发的《网络安全等级测评与检测评估机构服务认证证书》具有ISO27001信息安全管理体系认证证书、ISO20000证书（以上资质均需提供复印件并加盖单位公章，且证书需在有效期限内）。

四、项目团队要求

1、对拟派项目经理须具备高级网络安全等级测评师证书和商用密码应用安全性评估测评能力证书、渗透测试高级工程师证书、数据安全工程师(高级)证书。

2、技术负责人：具有网络安全服务能力评价证书中级（CCSS-R）、软件测评工程师（STE）证书。

3、团队人员资质要求：具有中级测评师证书、网络安全能力认证-网络安全管理（CCSC）（Ⅱ级）、公安部信息安全等级保护评估中心颁发的CIIP-D证书。

（以上涉及人员资质，需提供证书扫描件并加盖公章，同时提供社保证明。）

## 五、项目技术服务要求：

### （一）等保测评依据标准和规范：

（1）《中华人民共和国网络安全法》；

（2）《信息安全等级保护管理办法》（公通字[2007]43号）；

（3）GB/T22239-2019《信息安全技术网络安全等级保护基本要求》；

（4）GB/T17859-1999计算机信息系统安全保护等级划分准则；

（5）GB/T25058-2020信息安全技术网络安全等级保护实施指南；

（6）GB/T25070-2019信息安全技术网络安全等级保护安全设计技术要求；

（7）GB/T22240-2020信息安全技术网络安全保护等级定级指南；

（8）ISO/IEC27001信息系统安全管理体系标准；

（9）GB/T28448-2019信息安全技术网络安全等级保护测评要求。

### （二）项目服务范围

本项目是针对喀什地区数字化发展局政务云机房进行等级保护测评服务，对不符合网络安全等级保护测评有关管理规范和技术标准的，提出可行性差距分析整改方案并配合整改，在整改完成后对整改项进行测评，在整改完成后需再次测评。

### （三）项目内容

1.工作阶段

（1）等级保护差距分析：

针对信息系统的安全保护现状，从物理安全、网络安全、主机安全、应用安全、数据安全、安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理十个方面进行分析，分析各层面安全现状与等级保护基本要求之间的差距，完成《信息系统安全差距分析报告》。

（2）安全整改方案设计：

安全管理设计：根据《信息系统安全差距分析报告》，对信息安全保障中各种制度、规章以及相关制度规章的落实，进行细致的规划设计；

安全技术设计：根据《信息系统安全差距分析报告》，从物理安全、网络安全、主机安全、应用安全、数据安全五个方面，对机房物理环境、网络结构、策略配置、工具评估结果等详细分析，根据分析结果设计安全技术方案，通过对现状的设计规划，完成《信息系统安全整改建设方案》。

（3）等级测评：由测评机构开展等级测评工作。包含现场正式测评工作、渗透测试、配置审计、远程扫描等，并出具《网络安全等级保护测评报告》。

（4）测评范围：物理环境、网络设备、安全设备、服务器、终端、数据库、业务系统、安全管理机构、人员安全管理、安全管理制度、系统建设、系统运维。

（5）工具测试：通过工具扫描测评范围内的系统及网络，进行渗透测试、安全配置审计、脆弱性扫描，发现安全风险、漏洞和威胁。

（6）人工检查：机房物理设施、网络设备、安全设备、服务器、终端、业务系统的安全策略及其日志分析。

（7）网络构架分析：网络安全规划、设备命名规范性、网络架构安全性。网络设备和链路冗余、设备选型及可扩展性。网络设备的ACL、防火墙SNMP、口令、设备版本、系统漏洞、服务、端口等。

（8）问卷调查：对管理人员、维护人员、业务人员进行问卷调查，问卷涉及威胁与管理脆弱性两个方面。

（9）应用系统调研：通过人工安全检查了解目前应用系统本身的安全性内容，了解前期信息安全建设中的安全思想是否能够准确的表达与使用。

（10）顾问访谈：了解各个层次的人员，了解目前网络中技术的缺陷、管理体系的缺陷。对制度的执行情况进行更为细致的了解和评定。

（11）安全培训：网络安全知识培训、信息安全等级保护技术培训、网络攻防技术培训。

2.具体内容

依据国家相关信息安全标准和规范，严格遵循GBT28448-2019《信息安全技术网络安全等级保护测评要求》和GBT22239-2019《信息安全技术网络安全等级保护基本要求》文件，根据信息系统安全保护等级，开展网络安全等级保护测评工作，测评工作包括技术测评和管理测评两部分，分别为：

（1）技术测评

安全物理环境：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。

安全通信网络：测评通过访谈、检查和测试的方式，具体的测评内容如下所示：网络架构、通信传输、可信验证。

安全区域边界：测评通过访谈、检查和测试的方式，具体测评内容包括：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。

安全计算环境：测评通过访谈、检查和测试的方式，具体测评内容包括：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。

安全管理中心：测评通过访谈和检查的方式，具体测评内容包括：系统管理、审计管理、安全管理、集中管控。

（2）管理测评

安全管理制度：安全管理制度测评通过访谈和检查的形式评估安全管理制度的制定、发布、评审和修订等情况。主要涉及的对象为安全主管人员、安全管理人员、其他人员、管理制度、操作规程文件等，具体测评内容包括：安全策略、管理制度、制定和发布、评审和修订。

安全管理机构：安全管理机构测评通过访谈和检查的形式评估安全管理机构的组成情况和机构工作组织情况。主要涉及的对象为安全主管人员、安全管理人员、相关的文件资料和工作记录等，具体测评内容包括：岗位设置、人员配备、授权和审批、沟通和合作、审核和检查。

安全管理人员：安全管理人员测评通过访谈和检查的形式评估机构人员安全控制方面的情况。主要涉及对象为安全主管人员、人事管理人员、相关管理制度、相关工作记录等，具体测评内容包括：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。

安全建设管理：安全建设管理测评通过访谈和检查的形式评估系统建设管理过程中的安全控制情况。主要涉及对象为安全主管人员、系统建设负责人、管理制度、操作规程文件、执行过程记录等，具体测评内容包括：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、系统交付、等级测评、安全服务商选择。

安全运维管理：通过访谈和检查的形式评测系统运维管理过程中的安全控制情况。主要涉及人员有安全主管人员、安全管理人员、运维人员，涉及内容有运维管理制度、运维服务团队的管理制度、操作规程文件、执行过程记录等。具体测评内容包括：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。

（3）等级保护测评培训

测评机构必须提供本项目所需的现场培训。

培训目的：使采购人人员熟悉国家对网络安全等级保护相应法律法规；使采购方人员熟悉网络安全等级保护测评的方法。

培训内容：信息安全等级保护法律法规；信息安全等级保护测评方法。

培训对象：采购人信息系统使用及安全管理人员。

培训教师：培训教师须具备相关专业认证资质与丰富经验。

培训人数：现场培训人数根据甲方需求确定。

培训天数：根据采购人需求确定。

（4）项目交付物

交付具有评估测评资质效力的报告:

《信息系统安全差距分析报告》

《网络安全等级保护测评报告》

### （四）项目建设要求

1.整体要求

（1）供应商应详细描述等级保护测评的整体实施方案，包括等保测评方案、项目实施方案、时间安排、阶段性文档提交和验收标准等。

（2）供应商应详细描述测评人员的组成、资质及各自职责的划分。

（3）供应商应配置经验丰富的测评人员进行等级保护测评工作。

（4）如需在等级保护测评实施过程中采用在线测评工具的，各种工具软件由供应商推荐，经采购人确认后由供应商提供并在测评中使用。

（5）应详细描述所使用的安全测评工具（软硬件型号、功能和性能描述）、使用的方式和时间、对环境和平台的要求以及使用可能对系统造成的风险等。

（6）等级保护测评应有详细的实施方案和严格的操作步骤，采取的措施应是经过测试、稳定可靠的。

（7）安全测评工具软件运行可能需要的硬件平台（如笔记本电脑、PC、工作站等）和操作系统软件等由供应商推荐，经确认后由供应商提供并在测评中使用。安全测评需要的运行环境（如场地、网络环境等）由采购人提供，供应商应详细描述需要的运行环境的具体要求。

2.实施原则

（1）保密原则：对测评的过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据进行任何侵害采购人的行为，否则采购人有权追究供应商的法律责任。

（2）标准性原则：测评方案的设计与实施应依据国家等级保护的相关标准进行。

（3）规范性原则：供应商工作中的过程和文档，具有很好的规范性，可便于项目的跟踪和控制。

（4）可控性原则：测评服务的进度要跟上进度表的安排，保证采购人对于测评工作的可控性。

（5）整体性原则：测评的范围和内容应当整体全面，包括国家等级保护相关要求涉及的各个层面。

（6）最小影响原则：测评工作应尽可能小的影响系统和网络，并在可控的范围内，不能对现有信息系统的正常运行、业务的正常开展产生任何影响。

3.信息系统安全等级保护测评流程分为四个阶段：测评准备阶段、方案编制阶段、现场测评阶段、分析与报告编制阶段。测评完成后，提供整改建议书，配合采购方根据测评范围进行整改实施，整改完成后由供应商针对整改问题进行复测。

## 五、商务要求：

### （一）服务期限：

2024年12月25日之前完成政务云机房测评工作，质保期一年。

### （二）服务地点：喀什地区或采购人指定地点。

### （三）服务要求：

1.验收：合格后质保期一年，终身维护，质保期内产品出现任何非人为问题免费上门服务，质保期后只收取成本费。

2.响应时间：服务期间提供7×24服务响应（7×24小时工程师2小时内作好服务应答和反馈），需要现场支撑时，供应商需安排不少于1名服务工程师到达现场处理。供应商应提供针对应急等事宜的保障方案。

3.保密要求：项目实施过程中所收集、产生的所有与本项目相关文档、资料，包括文字、图片、表格、数字等各种形式所属权均归属甲方，供应商有义务对所涉及到的内容保密，应按照要求签署保密协议。

4.供应商在新疆维吾尔自治区境内有运维机构，同时供应商为本项目提供本地化服务，投标人具备本地服务能力和快速响应能力同时提供本地化服务方案。

5.供应商应提供完整的等级保护测评培训服务，培训方案由供应商提出并经采购人认可后生效。