1. **企业**
2. 投标人具有ISP《第一类增值电信业务中的互联网接入服务业务》与IDC《第一类增值电信业务中的互联网数据中心业务》。
3. 投标人能提供增值税专用发票。
4. 项目具体需求
5. 定级备案

依据 GB/T 22240《网络安全等级保护定级指南》,指导相关人员编制未备案系统的定级报告，聘请专家进行专家评审，定级备案材料的准备等（一切费用由中标人包干）。

* 需审核系统初步确定的安全等级，提出审核意见
* 需要针对已确定安全等级但尚未备案的业务系统，指导编写系统定级报告。 针对发生安全等级变更的业务系统，进行重新定级。
* 聘请专家，提供定级意见（一切费用由中标人包干）。
* 其他定级备案材料准备（一切费用由中标人包干）。

1. 安全等保咨询

需要摸清被测系统所属企业信息资产等基础网络环境，了解企业网络安全工作情况和安全责任制落实情况，贯彻落实等级保护制度情况；

从网络安全结构、网络访问控制、网络安全设计、边界完整性检查、网络入侵防范、恶意代码防范、网络设备保护、制度建设等方面进行开展咨询。

1. 网络安全等级保护测评

调研和测评方案编制阶段，通过下发调研表获取被测系统的基本情况，掌握系统运行的环境，实际掌握网络设备、安全设备、服务器、数据库、应用系统、操作终端和管理制度等信息，并编制等保咨询测评计划；

差距分析阶段，根据测评方案从网络安全、主机安全、应用安全、数据安全、安全管理等方面对信息系统进行测评，完成差距分析：

技术层面的差距评估（三级）内容：

* 安全物理环境：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。
* 安全通信网络：网络架构、通信传输、可信验证。
* 安全区域边界：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：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：系统管理、审计管理、安全管理、集中管控。

管理层面的差距评估（三级）内容：

* 安全管理制度：安全策略、管理制度、制定与发布、评审与修订。
* 安全管理机构：岗位设置、人员配备、授权和审批、沟通与合作、审核和检查。
* 安全管理人员：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：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、服务供应商管理。
* 安全运维管理： 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。

安全整改阶段，依据相应等级要求对当前实际情况的差距分析结果对应策略设计整改加固措施，包含安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心以及管理要求内容，针对不符合项以及行业特性要求进行个性化的整改方案设计，包含岗位职责梳理、技术策略实施、风险评估、管理体系建设、安全产品集成、组织方案评审、提供安全产品等方面，设计信息安全等级保护建设详细方案，协助建设单位完成建设整改工作。

安全加固阶段，根据等级保护基本要求以及风险和差距分析结果，对服务范围内信息系统的关键资产编制安全加固实施方案。派遣专业工程师到现场根据安全加固实施方案实施边界防护安全策略优化辅导、服务器病毒检查与清理，提供主机安全加固建议、数据库安全加固建议以及应用安全加固建议。在安全加固实施前，应提交安全加固风险分析及风险规避说明书；安全加固实施后，应提交防火墙策略文件及配置清单、服务器安全加固建议报告、设备加固建议报告等文档。对于需要增加投资，部署新的信息安全产品和技术的整改措施，双方根据整改方案另行协商和实施。

组织等保测评，报告编制阶段，根据系统整改和加固情况，进行测评项单项符合性判定，综合分析剩余安全问题，在整改符合符合等保要求的前提下，获得公安主管单位认可的《等级测评报告》。