采购需求

本项目所属行业为：软件和信息技术服务业。（从业人员300人以下或营业收入10000万元以下的为中小微型企业。其中，从业人员100人及以上，且营业收入1000万元及以上的为中型企业；从业人员10人及以上，且营业收入50万元及以上的为小型企业；从业人员10人以下或营业收入50万元以下的为微型企业。）

一、服务内容：

1.项目概况：系统数量 21 个，等保级别 三 级。

2.系统调研：在系统相关人员的协助下，对信息系统进行调研和梳理，了解系统当前信息系统资产现状。

3.现场测评：根据国家等级测评的相关标准及已编制的相关等级保护测评指导书对信息系统中的相关资产进行测评项的检查、记录检查结果。

4.分析整改：根据前述工作内容，分析信息系统安全情况与等级保护基本要求的差距，提供差异化测评服务，并进行风险分析，可根据现场情况出具科学合理的整改建议及整改方案，配合采购人安全整改工作。

5.结论报告：根据前述工作内容，分析当前信息系统安全保护能力是否符合相应等级的安全要求，针对整改项进行再次测评,提供安全等级符合性测评服务，出具相关系统测评报告。

6.配合验收：整理项目过程中所有相关的过程文档，提交系统相关资料。

二、项目技术标准及要求

(一)总体要求

根据国家《信息安全等级保护管理办法》(公通字〔2007〕43号)与《信息安全技术 网络安全等级保护基本要求》GB/T22239-2019要求，等级测评工作须覆盖安全物理环境、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的内容，并根据现场实际情况完成风险分析工作,最终为完善等级保护安全防护体系提供指导依据。

(二)第一阶段：等级保护

信息安全等级保护工作共分为五步，分别是：“定级、备案、建设整改、等级测评、监督检查”。该项目主要完成系统的安全测评工作，依据安全技术和安全管理两个方面的测评要求，分别从安全物理环境、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、安全运维管理十个安全类别进行安全测评。

1.定级要求：

该项工作开展的主要依据是《网络安全等级保护定级指南》（GB/T 22240-2020）确定系统等级。

2.备案：

信息系统的安全保护等级确定后，二级以上（含二级）信息系统的运营使用单位或主管部门应到属地公安机关办理备案手续。按照国家政策要求，跨省或者全国统一联网运行的

信息系统在各地运行、应用的分支系统，向当地设区的市级以上公安机关备案。该项目系统应向归属地网络安全监察支队申请重要信息系统备案。

完成备案的信息系统，将获得公安机关颁发的《信息系统安全等级保护备案证明》。

3.等级保护测评要求：

供应商在测评过程中要求按照《计算机信息系统安全保护等级划分准则》（GB17859-1999）、《信息安全技术 网络安全等级保护实施指南》（GB/T25058-2019）、《信息安全技术 网络安全等级保护基本要求》（GB/T22239-2019）、《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019）、《信息安全技术 网络安全等级保护测评过程指南》（GB/T28449-2018）等相关的标准规范开展等级测评工作，对系统的安全物理环境、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、安全运维管理共10个层面进行安全等级保护测评。

(三)第二阶段：渗透测试（三级）

渗透测试是通过模拟恶意黑客的攻击方法，来对计算机网络的安全性进行检测评估的过程。对系统和网络进行非破坏性质的攻击性测试，尝试侵入系统，获取系统控制权并将入侵的过程和细节产生报告给采购人，由此证实采购人所存在的安全威胁和风险，及时提示开发人员修复安全漏洞，提醒安全管理员完善安全策略，提升系统安全防护能力。通过这种方法,可以发现系统面临和暴露的安全问题,同时渗透测试也是对安全措施有效性的重要验证。

(四)第三阶段：建设整改咨询及安全加固（不涉及硬件）

建设整改咨询工作以等级测评和渗透检测发现的安全问题为工作重点，编写《信息系统安全建设整改建议》;将信息系统的安全建设整改需求落实到可操作的安全技术和管理上，提出能够实现的技术参数或制度及其具体规范。

采购人依据相关《信息系统安全建设整改建议》开展建设整改工作时，供应商将提供建设整改过程中的与建设整改相关的咨询服务。

对信息系统安全整改建议进行确认，并依照建议，协助采购人进行漏洞修复，补丁升级等非硬件层面的安全加固，制定可执行的安全整改方案和计划，然后协助采购人分步实施安全整改工作。

(五)第四阶段：售后服务

为期一年的售后服务工作中，供应商将向采购人提供包括应急响应、安全监测、配合检查、电话支持、安全咨询等服务在内的安全维保服务。具体服务内容如下：

（1）应急响应服务

针对本次项目，服务方提供7×24的常规应急响应及灾难恢复专家服务。在接到用户故障报修电话10分钟内响应。对客户信息网络应用系统突发的信息安全事件进行响应、处理、恢复、取证、跟踪、事后分析的方法及过程。

（2）配合检查服务

供应商协助采购人响应公安机关、单位内部以及第三方机构针对信息系统安全等级保护工作的检查工作。服务内容包括协助采购人准备、完善各类资料文档，配合检查过程中的答疑及技术支持及其他现场检查的响应。

（3）电话支持服务

每周 7 天/每天 24 小时不间断的电话支持服务，解答采购人在使用过程中遇到的问题，及时提出解决问题的建议和操作方法。电话响应时间不超过 10 分钟，到达现场时间不超过 2 小时，解决问题不超过 24 小时。

（4）安全咨询服务

供应商为采购人提供一年技术咨询服务，包括信息系统整改建设咨询服务以及其他相关安全咨询服务，一旦接到用户的服务请求，技术服务工程师将立即开始提供服务，帮助客户解决信息安全相关技术问题，全面配合采购人做好业务系统全保障工作。

三、服务要求

1.供应商应按等级保护测评要求制定测评过程中产生的文档，做到科学、规范、详尽、统一。

2.供应商应严格遵守采购人有关保密的相关规定，不得泄漏被测单位的任何信息。

四、交付内容要求

1.《信息系统安全等级保护定级备案证明》（每个系统各一份）；

2.《信息系统测评方案》（每个系统各一份）；

3.《信息系统整改建议书》（每个系统各一份）；

4.《信息系统渗透测试报告》（每个系统各一份）；

5.《信息系统安全等级测评报告》（每个系统各一份）。

五、服务期限要求

服务期：一年

维护期：一年

六、人员配置要求

1.测评人员要求：项目经理、技术负责人必须具备丰富的安全服务经验及相关资质认证，并提供人员管理及配备方案，并确保人员稳定。如需更换测评人员，须由采购人同意。测评人员需具有 1 年以上网络安全等级保护测评工作经验。本项目由项目经理统一负责，项目经理具有一定的技术及管理知识和经验，能容易地与客户沟通，能很好的执行与完成测评工作，并根据适当情况增加测评人员。 ★2.测评项目组人员配备要求：供应商参与此项目不少于 10 人，其中包括管理人员（项目经理和技术负责人）及现场测评人员。项目组至少包含 2 名高级测评师，2 名中级测评师及 5 名初级及以上测评师，并提供相应证书。

七、设施设备要求

供应商根据项目采购项目特性及要求，自行配置投入履行合同所必需的各类设施设备，保证项目顺利实施。

八、其他要求

1.等级保护测评实施方案，供应商根据网络安全等级保护基本要求（GB/T 22239-2019）制定等级保护测评工作的实施方案，内容包括但不限于：①测评对象分析；②测评方法；③测评过程；④测评内容；⑤安全服务计划等。 2.需求分析，供应商对本项目采购需求有充分理解与认识，对项目重点、难点分析透彻并提出解决方案，内容至少包含：①项目需求理解；②重点分析；③难点分析；④解决办法及应对措施。 3.进度控制计划方案，供应商根据服务需求制定测评进度控制计划方案，内容包括但不限于：①进度分解；②影响因素分析；

③影响因素应对措施；④进度监测措施。 4.售后服务方案，供应商为保障在测评项目结束后的信息安全，须提供完善的售后服务方案，内容包括但不限于：①应急响应服务；②电话支持服务；③配合检查服务；④安全咨询服务；⑤安全培训服务。 5.培训方案，供应商制定针对受测系统所属部门的培训方案，内容包括但不限于：①培训需求分析；②培训对象；③培训人数；④培训方式；⑤培训时间等安排。