2023年度张家港市智慧生态平台
网络安全等级保护测评项目谈判采购公告

资格条件：

1 具有独立承担民事责任的能力；

2 具有良好的商业信誉和健全的财务会计制度；

3 具有履行合同所必须的设备和专业技术能力；

4 有依法缴纳税收和社会保障资金的良好记录；

5 参加政府采购活动前三年内，在经营活动中没有重大违法记录；

6 具有公安部第三研究所（国家认证认可委员会批准的认证机构）认证发放的《网络安全等级测评与检测评估机构服务认证证书》

7 法律、行政法规规定的其他条件。

招标需求：

一、 项目背景

为更好的贯彻落实中央领导同志关于网络安全的重要指示精神，有效应对当前网络安全面临的严峻威胁与挑战，全力做好重要信息系统网络安全保卫工作，亟需对重要信息系统展开等保评测工作，通过该评测工作及时发现系统安全隐患并迅速进行整改，从而全面提升重要信息系统的网络安全防护水平，保障系统的安全、高效、稳定运行。

二、 项目内容及要求

序号	系统名称	等保测评级别
1	张家港市智慧生态平台	二级

（一）项目依据

《中华人民共和国网络安全法》

《关于加强党政机关计算机信息系统安全和保密管理的若干规定》

《计算机信息系统安全保护等级划分准则》（GB 17859-1999）

《关于信息安全等级保护工作的实施意见》(公通字[2004]66号)

《信息安全等级保护管理办法》(公通字[2007]43号)

《信息系统安全保护等级定级指南》（GB/T 22240-2008）

《信息安全技术 网络安全等级保护实施指南》（GB/T 25058）

《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）

《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）

《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018）

《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T 25070-2019）

《信息系统安全管理测评》（GA/T 713-2007）

《信息安全等级保护等级测评实施细则》

《信息安全风险评估规范》（GB/T 20984-2007）

《信息安全风险管理指南》（GB/Z 24364-2009）

《信息安全管理体系要求》（GB/T 22080-2008）

《信息安全管理实用规则》（GB/T 22081-2008）

《信息系统安全管理要求》（GB/T 20269-2006）

《信息安全事件分类分级指南》（GB/Z 20986-2007）

《信息安全事件管理指南》（GB/Z 20985-2007）

《信息系统灾难恢复规范》（GB/T 20988-2007）

《信息安全应急响应计划规范》（GB/T 24363-2009）

（二）项目工作内容

1、等级保护测评

按照用户现状参照所定等级对应的技术要求进行测评分析，对评估对象的现状作记录，包括物理安全、网络安全、主机安全、应用安全、数据安全及备份和恢复；按照用户系统现状对应的管理要求进行测评分析，对评估对象的现状作记录，包括安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理。

1）识别信息安全风险。通过对信息系统在安全技术和安全管理方面的分析，发现信息系统在安全技术和安全管理方面与相应安全等级保护要求之间的差距，并进行风险分析，出具差距分析报告，明确信息系统面临的风险。

2）增强安全防护能力。依据差距分析报告的结果，并结合实际情况，区分轻重缓急，制定针对性的安全整改计划，通过安全整改不断提高信息系统的整体安全保护水平。

3）测评结果分析

（1）单项测评结果判定

（2）单元测评结果判定

（3）整体测评分析

（4）形成测评分析报告

（5）针对测评分析报告的整改建议

2、渗透测试

选取可能发起攻击的测试点，使用渗透测试的方式查找可能存在的渗透点,发现信息系统防护体系的薄弱环节，找出可能发生的恶意攻击事件和违规行为。

1）渗透测试的内容

- 工作内容包括渗透测试及提供漏洞修复方案。
- 本次渗透测试工作为黑盒测试。

2）需要包含如下阶段

- 前期交互阶段：与用户组织进行讨论，确定渗透测试范围和目标。
- 信息搜集阶段：采用各种方法搜集用户方的所有相关信息。
- 威胁建模阶段：使用在信息搜集阶段所获取到的信息，标识出目标系统上可能存在的安全漏洞与弱点。
- 漏洞分析阶段：综合前面几个环节获取到的信息，从中分析和理解，找出攻击途径和攻击方法。
- 渗透攻击阶段：针对确定好的攻击途径和攻击方法实施渗透攻击，获取系统相关权限。
- 后渗透攻击阶段：以特定的业务系统作为目标，识别出关键的基础设施，找出用户组织最具价值和尝试进行安全保护的信息和资产，找出能够对用户组织造成重要业务影响的攻击途径。
- 报告阶段：将渗透测试结果编制成文档提交给用户，提供安全解决方案。并将在渗透测试阶段产生的垃圾数据进行清理。

3）渗透测试工作要求

本次渗透攻击测试工作应当以不破坏用户应用系统为前提条件，不做危害用户应用系统的工作行为，遵守职业道德，遵守行业规则，严格遵守保密制度，保密要求，不得擅自修改、拷贝用户数据，不得泄露、传播用户的敏感信息，如有违反将负法律责任。

（三）服务成果

本次安全服务应提交以下成果：

1）《信息系统等级测评报告》，包括单元测评分析结果、整改测评分析结果、测评结论和安全整改建议等。

2）《信息系统渗透测试报告》，包含但不限于如下方面的内容：渗透测试的方法、目标、范围。测试的人员、时间、策略。测试的工具、风险规避措施。测试的过程、漏洞利用截图，

测试的结果等。

（四）服务人员要求

1、项目实施过程中实行专人专职原则，保证各安全层面的测评全面有效，能够发现实际存在安全风险，现场实施人员均需持有等级保护测评师证书。

2、项目组人员必须熟练掌握信息安全相关标准与规范，具备丰富的信息安全测评工作经验，具有成熟的信息安全技术和项目管理能力，能够应对可能的突发性安全事件应急工作。

（五）工具配备要求

1、投标人必须单独配备安全测评工具，包含但不限于以下种类工具：网络漏洞扫描系统、web 漏洞扫描系统。

2、投标人必须在技术方案内明确专项检查所需要的所有技术检测工具，至少包含以下内容：名称、型号、主要功能、数量等。