# 宁波市区域数字档案管理服务一体化平台项目第三方测评

# 采购需求

**一、采购范围**

本次采购范围：对宁波市档案馆指定的区域数字档案管理服务一体化平台开展等保测评、软件测评、代码审计并出具相应测评报告。

1. **服务内容**

1、根据《中华人民共和国计算机信息系统安全保护条例》（国务院147号令）、《信息安全等级保护管理办法》（公通字[2007]43号）、《浙江省信息安全等级保护管理办法》（省政府223号令）、《浙江省信息安全等级保护测评机构管理规定》（浙等保〔2008〕4号）、《关于开展信息安全等级测评工作的通知》（浙等保〔2008〕5号）等文件中要求，明确对重要信息系统实施信息安全等级保护工作。《中华人民共和国网络安全法》第二十一条：国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。依据《中华人民共和国计算机信息系统安全保护条例》（国务院147号令）、《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发〔2003〕27号）、《关于信息安全等级保护工作的实施意见》（公通字〔2004〕66号）和《信息安全等级保护管理办法》（公通字〔2007〕43号）等相关文件及标准要求，对区域数字档案管理服务一体化平台进行二级等保测评及备案。

2、区域数字档案管理服务一体化平台所涉及软件系统开发完成后，对本项目所涉及的软件系统按照《软件需求规格说明书》、《用户手册》或项目承建单位的合同条款，以及相关的国家和行业的质量标准，对系统功能、性能等方面进行软件验收测试，并提供具备CMA或CNAS认证的《软件测试报告》。

3、依据GB/T 39412-2020《信息安全技术代码安全审计规范》，对“区域数字档案管理服务一体化平台软件系统开展软件代码审计，采用代码安全审计工具和人工排查的方式对代码中存在的编码漏洞和缺陷等进行检查分析，发现当前应用程序存在的漏洞，如跨站脚本漏洞、SQL注入漏洞、命令执行漏洞、日志伪造漏洞、参数篡改等，完成初测并提供初测报告供符合要求的测评报告《代码审计安全评估报告》，协助采购方制定整改方案、完成问题整改并对系统进行复测，确保信息系统的各项技术措施及管理手段能够满足标准要求，并提供源代码审计报告。

1. **服务要求**

1.供应商应满足采购人提出的标准性、规范性、可控性、整体性、最小影响性及保密性原则，做到守时、保质。

2.保密性要求：供应商必须和采购人签订保密协议，供应商必须要与参加此次测评项目的所有项目组成员签订保密协议，在合同签订时一并提供给采购人。

3.供应商应协助安全测评报告和软件代码审计报告的编写，对于测评中的重要资料和结果，在测评期间和测评结束后，供应商不得带离。

4.供应商对本规范书中的内容及在应标过程中接触的设备信息、数据资料等负有保密责任，不得泄露给任何第三方。无论供应商成交与否，其对上述内容的保密责任将长期存在。测试过程中其相关人员应注意测试记录和证据的接收、处理、存储和销毁，保护其在测试期间免遭改变/遗失，并保守秘密。

5.各项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。安全调查和测评的过程中，供应商如需采购人配合，供应商需要详细描述需要配合的内容。

6.信息安全等级保护是国家信息安全保障的基本制度、基本策略、基本方法，开展信息安全等级保护工作是保护信息化发展、维护国家信息安全的根本保障。实施信息安全等级保护制度，信息系统运营使用单位和主管部门能按照标准进行安全建设、整改，信息系统安全也有了一个衡量尺度。

根据《中华人民共和国计算机信息系统安全保护条例》（国务院147号令）、《信息安全等级保护管理办法》（公通字[2007]43号）、《浙江省信息安全等级保护管理办法》（省政府223号令）、《浙江省信息安全等级保护测评机构管理规定》（浙等保〔2008〕4号）、《关于开展信息安全等级测评工作的通知》（浙等保〔2008〕5号）等文件中要求，明确对重要信息系统实施信息安全等级保护工作。

《中华人民共和国网络安全法》第二十一条：国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。依据《中华人民共和国计算机信息系统安全保护条例》（国务院147号令）、《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发〔2003〕27号）、《关于信息安全等级保护工作的实施意见》（公通字〔2004〕66号）和《信息安全等级保护管理办法》（公通字〔2007〕43号）等相关文件及标准要求，对信息系统进行二级等保测评及备案、软件测评、代码审计。

1. **测评依据**

供应商应依据国家等级保护相关标准开展工作，依据标准包括但不限于如下国家标准：

* GB/T 22239-2019《信息安全技术网络安全等级保护基本要求》GB/T
* GB/T 22240-2020《信息安全技术网络安全等级保护定级指南》
* GB/T 25058-2019《信息安全技术网络安全等级保护实施指南》
* GB/T 28448-2019《信息安全技术网络安全等级保护测评要求》
* GB/T 28449-2018《信息安全技术网络安全等级保护测评过程指南》
* GB/T 20984-2007《信息安全技术 信息安全风险评估规范》
* GB/T39412-2020《信息安全技术代码安全审计规范》
* GB/T25000.51-2016《系统与软件工程 系统与软件质量要求和评价（SQuaRE） 第51部分：就绪可用软件产品（RUSP）的质量要求和测试细则》
1. **测评应满足的原则**
2. 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集成服务商的行为，否则集成服务商有权追究供应商的责任；
3. 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；
4. 规范性原则：测评工作过程中的文档，具有良好的规范性，便于项目的跟踪和控制；
5. 可控性原则：测评服务的进度要严格进度表的安排；
6. 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；
7. 最小影响原则：测评工作对系统和网络的影响必须在可控范围内，测评工作不能对现有信息系统的的正常运行、业务的正常开展产生任何影响。
8. **项目实施要求**
9. 供应商应保证本项目在采购人条件成熟时应立即开展实施；
10. 供应商在项目实施过程中应服从采购人的统一领导和协调，采购人有权裁决供应商的责任范围，供应商必须执行，在采购人限定的时间内解决问题。如果供应商不能按时完成评估内容，采购人有权中止项目、索赔或拒付款项；
11. 供应商应在项目现场实施周期内，供应商必须为本项目成立等级保护测评小组，安排包括项目经理和核心技术人员的现场驻场服务；
12. 供应商需根据自己的实施经验结合采购人的实际需求进一步细化和完善工作任务书，作为工程实施的指导性文件；
13. 供应商应根据采购人工作需求、进度要求、实际情况制定详细的项目实施管理规范和项目实施计划，对工程目标、工作任务、阶段性工作、项目组织机构、职责分工、项目进度、质量控制等内容进行详细的说明，以确保工程实施按时保质的完成；
14. 供应商应负责配合采购人制定相关验收标准，并完成工程实施等验收工作；
15. 在整改过程中，集成服务商整改加固过程需本项目供应商全程驻场配合并进行符合性复测；
16. 项目验收完成后，要求提供为期一年的技术咨询服务，以保证项目正常运行。
17. **其他要求**
18. 供应商需在响应截止前到现场实地查看并听取业主方现场介绍，未踏勘供应商不具备成交条件；
19. 投标供应商须提供书面承诺函（承诺函格式自拟），若项目成交后，供应商遵守保密义务，与服务人员签订保密协议，按照采购文件要求做好信息保密工作。
20. 服务成交供应商应在项目成交后2个工作日内准备完整的资质证明文件递交至采购人处，如发现递交的资质证明文件不符合本次采购所需要提供的资质文件或存在弄虚作假的情况，将上报采购监管部门要求废除成交供应商的成交资格，并追究相关法律责任。

**评分标准**

|  |  |
| --- | --- |
| 评分标准 | 分值 |
| 商务技术分85分 | 企业资质1. 投标人具备中国合格评定国家认可委员会颁发的检验机构认可证书，认可范围包含等级保护测评4级及以上检测能力且证书范围含信息安全风险评估的得6分；不满足不得分；
2. 投标人同时具备ISO 9001质量管理体系证书；ISO/IEC 27001信息安全管理体系证书得4分；没有不得分；
3. 投标人同时具有中国网络安全审查技术与认证中心颁发的信息系统安全运维服务资质二级及以上认证证书、信息安全风险评估服务资质认证证书、信息安全应急处理服务资质认证证书的得2分，有任意缺项不得分；
4. 投标人具有网络安全等级测评与检测评估机构服务认证证书的得2分；

**注：须提供证书复印件加盖公章，未提供不得分。注：磋商响应文件中提供有效期内的证书复印件加盖单位公章。** | 14分 |
| 项目理解根据供应商对宁波市区域数字档案管理服务一体化平台测评项目建设背景、建设目标、测评内容方向分析的理解程度进行综合评议（14分）理解程度高的得7.1-14分；理解程度一般的得0-7分；未提供不得分。 | 14分 |
| 项目测评技术服务方案根据供应商制定的测评技术服务方案进行综合评议，包括测评内容、测评计划、测评步骤、测评工具、阶段性文档及验收标准等进行综合评议（12分） 测评技术服务方案内容完整详尽、针对性强、设计内容科学合理、具有可行性的，与本项目的贴合程度高的得8.1-12分；测评技术服务方案完整、具有一定针对性、设计内容较为合理、具备可行性，基本贴合本项目的得4.1-8分；测评技术服务方案一般、设计内容欠周全、与项目贴合程度一般的得0-4分。 | 12分 |
| 项目实施方案评委根据供应商对项目进度计划安排的详细程度、与项目实际要求的符合性和项目组织实施方案（包括等保测评、软件测评、代码审计等内容，以及组织机构、实施场所、管理和协调方法）的完整性、合理性、可操作性进行综合评议（24分）方案合理针对性强的得16.1-24分；方案较合理针对性较强为的得8.1-16分；方案一般针对性一般的得0-8分。 | 24分 |
| 质量管理方案评委根据供应商对项目管理组织、实施规范和管理制度等项目质量管理方面提供的方案进行综合评议（10分）方案较合理针对性较强为的得6-10分；方案一般针对性一般的得1.1-4分；方案一般针对不合理的得得0-1分。 | 10分 |
| 项目实施团队1）供应商拟派项目负责人必须同时具备注册网络安全渗透评估专业人员（高级）证书、信息安全工程师（中级）证书，网络安全服务能力安全管理能力认证中级及以上证书，注册网络安全专业防御人员最高得4分，不满足不得分。2）项目组成员同时具有注册网络安全源代码审计专业人员、软件测试工程师证书的，最高得2分，不满足不得分。3）项目组成员具有注册信息安全专业人员得1分，最高2分。4）项目组成员具有注册网络安全专业防御人员得1分，最高1分。**注：项目负责人和其他项目组成员须提供近3个月内任意一个月在本单位的社保缴纳证明材料和有效证书复印件并加盖单位公章，未提供或资料提供不全的不得分。** | 9分 |
| 供应商业绩供应商自2022年1月1日以来（以合同签订时间为准）独立承担过类似项目（等保测评、软件测评、代码审计、安全测评等）案例，每提供1个项目案例得0.5分，最高得2分。**注：提供合同复印件并加盖公章，未提供不得分。** | 2分 |
| 价格分15分 | 基准价格=有效响应单位中参与评审的价格的最低报价，基准价格得满分。磋商报价得分=基准价格÷参与评审的价格×价格满分分值。（磋商报价得分以四舍五入方法整合到小数点后两位） | 15分 |
| 综合评分得分（满分100分） |

计算公式：响应单位的最终得分= 技术商务得分+最终报价价格得分（所有分值四舍五入保留到小数点后两位）。