廊坊市发展和改革委员会关于

廊坊市人民政府网站关键信息基础设施

风险评估服务采购的公告

一、资质要求：符合《政府采购法》第二十二条规定：

（一）具有独立承担民事责任的能力；

（二）具有良好的商业信誉和健全的财务会计制度；

（三）具有履行合同所必需的设备和专业技术能力；

（四）有依法缴纳税收和社会保障资金的良好记录；

（五）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；

**以上需提供承诺函**。

（六）符合政府采购信用相关规定；

（七）须具备CCRC信息安全服务资质认证证书复印件并加盖公章（须同时具备以下三项：风险评估、信息安全应急处理、信息系统安全运维）；

二、项目实施地点：廊坊市发改委

三、服务期限：合同签订后10个工作日内完成评估，并出具评估报告。

四、服务内容及标准：

1、服务说明

依据《网络安全法》、《关键信息基础设施安全保护条例》对廊坊市人民政府网站关键信息基础设施进行安全风险评估；合同签订后3个工作日内出具风险评估实施方案，我方同意后5个工作日内完成风险评估。风险评估完毕，出具风险评估报告。报告中应包含对存在的所有风险点进行整改、加固建议。协助我方对现有软硬件存在的所有风险点进行整改、加固。

五、付款方式：服务完成后一次清付清全款。

2、具体服务要求

1）通过对系统进行信息安全风险评估服务，确保信息安全整体保障水平的提高，需要实现以下目标：

a.梳理系统安全等级保护现状，为信息安全等级保护工作奠定基础；

梳理信息系统现状，从信息安全等级保护基本要求出发，形成现有信息系统与安全等级保护基本要求的差距。从信息安全等级保护完善的角度，确保信息系统的安全策略和管理规范符合国家信息安全等级保护基本要求。

b.掌握信息系统的风险管理现状，为信息安全规划提供依据；

开展一次信息系统的风险评估工作，提供专业的人工检测分析和工具测试服务。全面识别出信息系统中目前存在的技术和管理脆弱性，基于已发现的技术和管理脆弱性，提出相关的安全建议。

c.持续优化信息安全管理机制，提升信息安全管理水平；

梳理和完善信息安全管理制度，持续提升信息安全管理水平。在日常工作中针对发现的安全问题定期及不定期进行总结分析和汇报，针对各种问题给出安全改进建议，并协助采购人从安全管理机制上持续完善信息安全规范和流程。

2)项目范围

评估对象如下：

机房物理环境评估；

相关业务信息系统服务器人工检查；

应用服务器的操作系统、数据库人工检查；

网络设备、网络安全设备人工检查；

内控制度脆弱性检查；

具体评估资产对象清单（评估可采取抽样选取的方法）：

核心网络设备：全部选取评估；

接入网络设备：抽样选取评估；

安全设备：抽样选取评估；

主机设备：抽样选取评估；

数据库设备：抽样选取评估；

3)评估依据

本项目遵循/引据如下内容：

**政策法规：**

* 中华人民共和国计算机信息系统安全保护条例（1994国务院147号令）
* 计算机信息系统安全保护等级划分准则（GB17859－1999）
* 《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）
* 《信息安全等级保护管理办法》公通字[2007]43号
* 关于开展全国重要信息系统安全等级保护定级工作的通知（公信安[2007]861号）
* 《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）
* 其他相关标准

**标准规范：**

* 《计算机信息系统安全保护等级划分准则》GB/T 17859-1999
* 《信息安全技术 信息系统安全等级保护基本要求》GB/T 22239-2019
* 《信息安全技术 信息系统安全等级保护定级指南》GB/T 20440-2020
* 《信息安全技术 信息系统等级保护安全设计技术要求》GB/T 25070-2019
* 《信息安全技术 信息系统安全等级保护实施指南》GB/T 25058-2019
* 《信息安全技术 信息安全风险评估规范》GB/T 20984-2007
* 《信息安全技术 信息安全风险评估实施指南》GB/T 31509-2015
* 《信息安全技术 信息安全控制实践指南》GB/T 22081-2016
* 《信息安全技术 信息技术安全评估准则 第1部分：简介和一般模型》GB/T 18336.1-2015
* 《信息安全技术 信息技术安全评估准则 第2部分：安全功能组件》GB/T 18336.2-2015
* 《信息安全技术 信息技术安全性评估方法》GB/T 30270-2013
* 《信息安全技术 信息安全治理》GB/T 32923-2016 ISO\_IEC 27014 2013
* 《信息安全技术 安全管理指南第1部分：信息技术安全概念和模型》GB/T 19715.1-2005
* 《信息安全技术 安全管理指南第2部分：管理和规划信息技术安全》GB/T 19715.2-2005

**4）评估内容**

风险评估工作共分为6个阶段：即准备阶段、识别阶段、分析阶段、风险控制规划阶段、总结汇报阶段以及验收阶段。

准备阶段：主要完成项目组织、项目实施方案确定、组织培训、项目启动的工作。

识别阶段：主要完成大量的现场识别工作，主要有资产识别、威胁识别、脆弱性识别、安全措施识别。

分析阶段：在识别的基础上进行大量整理并分析，得出风险评估各要素的风险状况，具体有资产影响分析、威胁分析、脆弱性分析、安全措施有效性分析、综合风险分析。

总结汇报阶段：总结以上所有结论形成最终报告，并向领导小组汇报并提交。

验收阶段：进行离场交接（包含借阅文档交接等），对项目依据验收方案进行项目最终验收。

a资产评估

通过安全访谈、现场调研、安全检测等方式，全面梳理网络内所有资产状况，形成资产清单，并对资产根据其在保密性、完整性、可用性的等级分析结果，经过综合评定进行赋值。

b威胁评估

识别所评估信息资产存在的潜在威胁，识别威胁利用脆弱性的可能性，并分析威胁利用脆弱性对采购方可能造成的影响。

依据相关国家标准或国际标准，对存在脆弱性的资产进行威胁的全面识别，及时发现潜在威胁的原因，避免或降低威胁发生的几率。

威胁来源应至少包括但不限于以下四类：

人员威胁：包括内部人员、第三方人员，有意、无意威胁；

环境威胁：自然灾害、设施故障等；

社会威胁：社会动乱、恐怖袭击、战争、自然威胁（洪水、地震、台风、滑坡、雷电等）。

c脆弱性评估

在评估中，将从基础环境、网络环境、技术、安全管理四个方面进行脆弱性评估。基础环境评估按照国家等级保护三级系统的机房物理环境基本要求对现有的机房物理环境进行检查，发现物理环境中的缺陷和不足。

技术方面主要是通过远程和本地两种方式进行手工检查、工具扫描（漏洞扫描、渗透测试、基线检查等）、数据分析等方式进行评估，以保证脆弱性评估的全面性和有效性；

管理脆弱性评估按照国家等级保护三级系统的基本要求对现有的安全管理制度的制定和执行情况进行检查，发现其中的管理漏洞和不足。

d安全措施有效性分析

识别信息系统中已有的安全措施，分析安全措施的效力，确定威胁利用弱点的实际可能性，一方面可以指出当前安全措施的不足，另一方面也可以避免重复投资。安全措施识别工作完成之后，对安全措施所采取后的有效性进行分析，分析其安全措施对防范威胁、降低脆弱性的有效性。

e风险识别

完成资产、威胁和脆弱性的评估赋值后，计算信息资产的风险值，确定风险值对应的风险等级。

f综合风险分析

综合现场专家的访谈、问卷调查、现场制度核查、手工技术核查和安全工具检测结果，并进行综合风险的分析，得出采购方信息系统主机、数据库、应用中间件、网络架构、网络设备和安全设备、机房物理环境、内控制度管理等方面脆弱性风险的结果，并提出可落地的建议、方案。

5）风险评估交付成果

项目验收前应提交真实可靠、客观公正的评估文档，文档应包括但不限于以下内容：

《信息系统风险评估报告》

六、报价文件递交截止时间： 2022年11月16日17：30，超出此时间发出的报价文件为无效文件。

七、请按以下格式制作报价文件。报价文件须加盖公章后转换成PDF格式发送电子邮件到：qdl@lf.gov.cn。

联系人：齐工 电话：2317032

八、评分标准

|  |  |  |
| --- | --- | --- |
| **评审项目** | **标准分** | **评分标准** |
| 投标报价 | 10分 | 综合评分法中的价格分统一采用低价优先法计算，即满足招标文件要求且最后报价最低的供应商的价格为投标基准价，其价格分为满分。其他供应商的价格分统一按照下列公式计算：  投标报价得分=（投标基准价/投标报价）×10 |
| 投标人综合实力 | 14分 | 1.通过ISO9001质量管理体系、ISO14001环境管理体系、ISO45001职业健康安全管理体系、ISO27001信息安全管理体系、ISO20000信息技术服务管理体系证书，每具有一个证书得1分，最高得5分；  2.具有中国合格评定国家认可委员会检验机构认可证书和实验室认可证书的，得5分；  3.具备基于大数据的网络安全风险评估系统、网络安全风险评估态势感知系统、网络安全风险测评分析系统、网络安全检测评估分析服务平台软件著作权证书的每具有一个得1分，最高得4分。  注：投标文件中附以上证明材料复印件。以证书复印件加盖供应商公章为准。 |
| 类似业绩 | 5分 | 供应商按要求提供2019年10月1日起至今类似项目业绩，每提供一个得1分，最高得5分。  注：业绩以合同或协议为准，投标文件中附以上证明材料复印件。以合同复印件加盖供应商公章为准。 |
| 项目组人员配置 | 14分 | 供应商项目组须至少配备2名高级测评师及2名中级测评师。其中中级测评师同时具备信息安全保障人员认证证书、注册信息安全专业人员（CISP）证书、重要信息系统保护人员（CIIP-A）证书、IT服务工程师（ITSS）证书、国家网络安全应用检测专业测评人员（NSATP-A)证书的，每有一名得5分，最高得10分。项目组测评师每具备一名保密局颁发的涉密岗位资格证书的得1分，最高得4分。  注：投标文件中附以上证明材料复印件。以上人员须提供由人社部门开具的近三月在投标单位的社保缴纳证明复印件并加盖供应商公章，其他证明无效。 |
| 服务方案 | 15分 | 熟悉项目所有工作内容，提供的服务方案规范性及标准化程度很高得10-15分 |
| 基本能够完成项目所有工作内容，提供的服务方案规范性及标准化程度较高得5-9分 |
| 提供的服务方案规范性及标准化程度一般得1-4分 |
| 总体服务方案的针对性、可行性、完整性 | 15分 | 服务方案完整，充分考虑用户需求，服务方案针对性及可行性很高得10-15分 |
| 服务方案比较完整，服务方案具有一定的针对性及可行性较高得5-9分 |
| 服务方案不够完整，针对性不强得1-4分 |
| 服务质量控制及保证措施 | 15分 | 服务质量控制及保证措施科学合理且保障措施科学有效得10-15分 |
| 服务质量控制及保证措施切实可行且满足项目需要得5-9分 |
| 服务质量控制及保证措施基本满足项目需要得1-4分 |
| 安全和风险管理方案 | 12分 | 应急预方案完整详细、科学合理，可行性强8-12分 |
| 方案较完整详细、较科学合理，可行性较强4-7分 |
| 方案完整详细程度一般、不够科学合理，可行性一般1-3分 |

2022年11月11日

投标文件模板（\*标项为必有项目，不得缺少）

廊坊市人民政府网站关键信息基础设施

风险评估的服务采购报价文件

报价公司名称（公章）：

法定代表人或授权委托人（签字或盖章）：

报价时间： 年 月 日

**\*一、投 标 函**

致：廊坊市发展和改革委员会：

(供应商全称)授权 (供应商代表姓名)

(职务、职称)为我方代表，参加贵方组织的(写明项目名称、； )的招标活动，并对以上项目进行投标。为此：

1、我方同意在本项目招标文件中规定的开标日起的有效期内（见前附表）遵守

本投标文件中的承诺且在此期限期满之前均具有约束力。

2、我方承诺已经具备《中华人民共和国政府采购法》中规定的参加政府采购活动的供应商应当具备的全部条件。

3、提供投标须知规定的全部投标文件，包括：加密的电子公开文件一份（\*.PDF 格式）；

4、按招标文件要求提供和交付的货物和服务的投标报价详见开标一览表。

5、我方承诺：完全理解投标报价超过开标时公布的预算金额时，投标将被拒绝。

6、保证忠实地执行双方所签订的合同，并承担合同规定的责任和义务。

7、承诺完全满足和响应招标文件中的各项商务和技术要求，若有偏差，已在投标文件商务条款偏离表中予以明确特别说明。

8、保证遵守招标文件的所有规定。

9、我方完全理解贵方不一定接受最低价的投标或收到的任何投标。

10、我方愿意向贵方提供任何与本项投标有关的数据、情况和技术资料。若贵方需要，我方愿意提供我方作出的一切承诺的证明材料。

11、我方已详细审核全部投标文件，包括投标文件修改书（如有的话）、参考资料及有关附件，确认无误。

12、我方承诺：采购人若需追加采购本项目招标文件所列货物及相关服务的，在不改变合同其他实质性条款的前提下，按相同或更优惠的折扣率保证供货。

13、 我方承诺提供的所有材料均为真实的、有效的，愿承担所有责任。

所有有关本投标的一切往来联系方式为：

地址： 邮编： 电话： 传真：

供应商代表姓名： 供应商代表联系电话： E-mail：

供应商(公章)：

日 期：

说明：除可填报项目外，对本投标函的任何修改将被视为非实质性响应投标，从而导致该投标被拒绝。

**\*二、报价一览表**

廊坊市人民政府网站关键信息基础设施

风险评估的询价报价一览表

报价公司（公章）：

联系人： 联系电话： 报价时间：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 服务内容 | | 价格 | 备注 |
| 1 | 对廊坊市人民政府网站关键信息基础设施进行安全风险评估；合同签订后3个工作日内出具风险评估实施方案，我方同意后5个工作日内进行风险评估。风险评估完毕，出具风险评估报告。报告中应包含对存在的所有风险点进行整改、加固建议。协助我方对现有软硬件存在的所有风险点进行整改、加固。 | |  |  |
| 4 | 总价 |  | |  |

**报价说明：本表所报单价应包含购买本服务项目所需的各类费用（包含但不限于税费、人员工资、差旅费等）**

**\*三、资质证明文件：**

1、授权委托书；

廊坊市发展和改革委员会：

本授权委托书声明：注册于（供应商住址）的（供应商名称） 。法定代表人（法定代表人姓名、职务、身份证号）代表本公司在下面授权的 （供应商代表姓名、职务、身份证号）为本公司的合法代理人，就贵方组织的项目（项目名称 ）， 以本公司名义处理一切与之有关的事务。

单位名称（公章）

年 月 日

委托代理人身份证复印件（正反面） 法定代表人身份证复印件（正反面）

（粘贴此处） （粘贴此处）

2、营业执照复印件（加盖公章）；

3、符合《政府采购法》第二十二条规定承诺函（格式自拟，加盖公章）；

4、CCRC信息安全服务资质认证证书复印件（加盖公章）；

四、评审相关资料。