**参选人须知**

**一、说 明**

**（一） 适用范围**

1.本比选文件仅适用于本次比选邀请函中所叙述的项目。

2.本比选文件的解释权在比选人。

**（二） 定义**

1.比选人：本项目建设单位

2.参选人：系响应比选人要求，向比选人申请参与本项目方案比选的供应商。

**二、比选文件**

本比选文件阐明了申请人所需提供项目范围和参加比选的程序，是本次比选活动具有法律效应的文件。

参选人应认真阅读比选文件中所有的事项、格式条款和规范等要求。参选人没有按照比选文件要求提交全部资料，或者提交的应答文件没有对比选文件做出实质性响应而导致发生影响得分、比选被拒绝或按照无效比选处理的不利后果，由参选人自行承担相关风险。

（**一） 比选文件的组成**

1、封面（封面必须标明项目名称，投标人名称和“比选文件”字样）

2、目录（每项目录内容均须标注页码）

3、比选函(附件1)

4、参选人资格要求证明文件

(1) 关于资格要求的声明函(附件2)

(2) 统一社会信用代码证正副本复印件盖公章

(3) 法定代表人授权委托书原件(附件3，法定代表人亲自参加投标的除外)

(4) 法定代表人身份证正反面复印件

(5) 授权代理人身份证原件及正反面复印件(法定代表人亲自参加投标的除外)

(6) 最近3个月授权代理人（法定代表人亲自参加投标的除外）依法缴纳社会保障资金的缴款凭证复印件

(7) 承诺书(附件4)

5、明细报价表(附件5)

6、项目人员配置清单(附件6)

7、参选人具有从事与本项目类似服务经验的合同证明文件

8、本项目比选评分细则中对应的相关证明文件

9、项目技术方案

10、参选人认为需要加以说明的其他内容

上述材料中1-6项参选人必须全部提供，否则投标文件无效。

**（二）比选文件的编写与密封**

1.申请人应按本比选文件所规定的格式、内容等编制比选文件，比选文件一式贰份，正本一份，副本壹份。

2.密封件上应注明“于XXXX年XX月XX 日之前（指“比选邀请函”中规定的应答文件递交截止时间）不准启封”字样。

3.比选人将拒绝比选截止时间后递交的比选文件。

**三、比选评定**

**（一）比选**

1.比选人按比选文件规定的时间、地点组织比选。评标小组由比选人代表及评标专家组成，并邀请有关监督部门到现场进行监督。

2.比选人及监督人检查比选文件密封情况，并当场宣布检查情况。

**（二）评定**

1.评标小组成员由单数组成。

2. 评标小组将遵循“公平、公正、科学、择优”的原则，对所有申请人的比选文件评估，都采用相同的程序和标准。评议过程将严格按照比选文件的要求和条件进行。

3. 本项目评标采用综合评分法，由评标小组根据评分细则(附件8)分别对每位申请人进行打分，总分最高者为中选者。

**四、签订合同**

比选文件、参选人的比选应答文件均为签订合同的依据。合同签订后不允许将合同转与其他单位。

中选人因不可抗力或者自身原因不能履行合同的，比选人可以与总分次高的中选候选人签订合同。

**五、参选人需要注意的其它事项**

（一）参选人应遵守有关法律、法规，不得采取不正当的竞争手段，否则后果由参选人自负。

（二）在比选开始直至宣布结果之前，参选人不得向评标小组成员询问评选情况，不得进行旨在影响评选结果的活动，否则其比选资格无效并追究法律责任。

（三）参选人的比选资料一律不予退还。

（四）本比选文件的未尽事项，按现行的有关法律、法规及规章执行。

（五）经查实，参选人若有提供虚假证明文件的行为，比选人将首先停止其比选资格；同时视情节轻重追究其相关责任。

（六）参选人认为比选文件、中选结果使自己的合法权益受到损害的，应当在五个工作日内，以书面形式向比选人提出质疑，但参选人行使质疑权时，必须坚持“谁主张谁举证”，遵守“实事求是”和“谨慎性”原则，承担使用虚假材料或恶意方式质疑的法律责任。

**六、项目技术要求和有关说明**

**（一）项目背景和建设目标**

**项目背景**

为贯彻落实《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《无锡市使用财政性资金信息化项目网络安全管理规定》（锡网委[2021]4号）《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）等文件要求，结合部、省、市各级网信办、公安的网安部门、行业主管部门的护网、攻防、检测通报等工作，依据国家及行业等级保护标准，通过信息安全相关的网络安全等级保护测评、漏洞扫描、渗透测试、网络安全自查、网络安全建设咨询服务等工作，查找无锡市住房和城乡建设局及下属单位信息系统各安全层面与相应安全保护标准的差距，明确存在的安全问题及现有安全措施的有效性，并针对安全问题关联的资产、威胁、脆弱性，综合分析信息系统面临的安全风险，寻求风险降低或规避的方法、提出建设整改建议、编制建设整改方案、提供整改实施技术支持，为无锡市住房和城乡建设局以后的安全决策、安全管理、安全运维、持续整改提供依据。

**建设目标**

通过采购第三方信息安全技术服务，主要包括以下内容：

1.信息系统等保测评服务。包含无锡市房屋安全管理信息系统二级等保测评、无锡市城市基础设施配套费征收系统二级等保测评、无锡市建筑业实名制和分账制平台三级等保测评、智慧住建三级等保测评。

2.渗透测试服务。渗透测试是一种黑盒安全测试方法，安全专家通过模拟真实黑客的技术手段对目标进行漏洞检测，突破系统的安全防护手段，全面检测系统目前存在的安全隐患，深入评估漏洞可能造成的实际影响。以攻击者思维，模拟黑客对业务系统网络层、系统层、应用层乃至业务逻辑层进行全面深入的安全测试，帮助企业挖掘出正常业务流程中的隐藏的安全缺陷和漏洞，并提出修复建议、协助系统运维单位进行加固。

3.漏洞扫描服务。是利用漏洞扫描工具，通过对信息系统的扫描、探测等操作，使其产生特定的响应等活动，查看、分析响应结果，获取证据以证明信息系统安全保护措施是否得以有效实施的一种方法。

4.网络安全自查服务。根据省、市网络安全主管部门要求，并结合我局信息安全管理实际需要，协助建设单位在重要时点对全局网络和信息系统开展信息安全专项自查工作。通过定期网络安全检查及时发现局机关及局属事业单位、住建行业在信息安全方面与国家标准要求之间的差距，为全局信息系统安全建设和管理提供系统性、针对性、可行性的指导和服务，有效监控住建条线信息安全建设成本，提高全局信息系统安全防护的整体水平，确保全局信息安全建设与信息化发展相协调。

5.提供SDL(安全开发生命周期)相关服务。SDL即Security Development Lifecycle，是[微软](https://baike.baidu.com/item/%E5%BE%AE%E8%BD%AF/124767)提出的从安全角度指导软件开发过程的管理模式。SDL的核心理念就是将[软件安全](https://baike.baidu.com/item/%E8%BD%AF%E4%BB%B6%E5%AE%89%E5%85%A8)的考虑集成在[软件开发](https://baike.baidu.com/item/%E8%BD%AF%E4%BB%B6%E5%BC%80%E5%8F%91)的每一个阶段[需求分析](https://baike.baidu.com/item/%E9%9C%80%E6%B1%82%E5%88%86%E6%9E%90)、设计、编码、测试和维护。通过SDL的实施，有望从源头加强系统安全防御能力，保证安全技术措施同步规划、同步建设。包含但不限于：协助建设单位编制和审查信息系统安全设计方案，协助建设单位开展代码审计等服务。

6.应急保障、宣传培训等其他服务。协助建设单位开展应急演练，网络安全法律法规宣传、培训。

服务模式：远程服务与现场服务相结合。

1. **项目内容及要求**

**项目内容概况及总体要求**

采购的安全技术服务清单及考核要求如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **服务内容** | **频次** | **考核要求** |
| 1 | 网络安全等级保护测评 | 相关系统每年1次 | 提交无锡市房屋安全管理信息系统、无锡市城市基础设施配套费征收系统、无锡市建筑业实名制和分账制平台、智慧住建平台等保测评报告，并协助整改。 |
| 2 | 渗透测试 | 三级系统每年4次，  二级系统每年2次 | 《渗透测试用例清单》、《渗透测试记录》、《漏洞汇总表》、《渗透测试报告》及对应复测报告，并协助整改。 |
| 3 | 漏洞扫描 | 三级系统每年4次，  二级系统每年2次 | 提交漏洞扫描报告及对应复测报告，并协助整改。 |
| 4 | 网络安全自查（局机关含事业单位） | 每年2次 | 协助建设单位开展网络安全检查及编制网络安全自查报告。 |
| 5 | 协助建设单位编制和审查信息系统安全设计方案 | 审查项目不低于5个  协助编制项目安全方案不低于3个 | 出具信息化项目安全设计方案审核意见，协助编制安全设计方案。 |
| 6 | 协助建设单位开展代码审计 | 三级系统每年2次，  二级系统每年1次 | 提交代码审计报告，并协助整改。  主要针对新建或扩建系统，服务对象包括局机关系统全覆盖，下属单位所有系统抽查覆盖。 |
| 7 | 应急演练 | 三级系统每年2次  二级系统每年1次 | 提交应急演练总结报告，并协助建设单位完善相关管理制度。 |
| 8 | 宣传培训 | 提供网络安全法律法规等相关培训  每年不少于2次 | 根据建设单位要求不定期组织。 |

本项目服务内容主要包括：

1.等保测评服务。包含无锡市房屋安全管理信息系统二级等保测评、无锡市城市基础设施配套费征收系统二级等保测评、无锡市建筑业实名制和分账制平台三级等保测评、智慧住建三级等保测评。

2.渗透测试服务。以攻击者思维，模拟黑客对业务系统网络层、系统层、应用层乃至业务逻辑层进行全面深入的安全测试，帮助建设单位挖掘出正常业务流程中的隐藏的安全缺陷和漏洞，并提出修复建议、协助系统运维单位进行加固。

主要针对以下信息系统开展渗透测试服务（包含但不限于）：

**表一：信息系统清单**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 系统名称 | 安全等级 | 渗透测试频率 |
| 1 | 智慧住建 | 三级 | 每季度一次 |
| 2 | 无锡市建筑业实名制和分账制平台 | 三级 | 每季度一次 |
| 3 | 无锡市建筑市场信用管理系统  （含无锡市造价企业信用管理系统、无锡市监理企业信用管理系统） | 三级 | 每季度一次 |
| 4 | 建筑工地智慧监管平台 | 二级 | 每半年一次 |
| 5 | 城市基础设施配套费征收管理系统 | 二级 | 每半年一次 |
| 6 | 无锡市房地产开发企业信用系统 | 二级 | 每半年一次 |
| 7 | 无锡市勘察设计信用管理系统 | 二级 | 每半年一次 |
| 8 | 无锡市房屋安全管理信息系统 | 二级 | 每半年一次 |
| 总计 |  |  | 每年22次 |

**渗透测试方法。**针对各应用系统的渗透测试方法原则上应包括以下方法但不局限于以下方法，根据以下方法编制不少于20个渗透测试用例：

表二：渗透测试方法

|  |  |
| --- | --- |
| 测试  类型 | 测试描述 |
| 信息收集 | 信息收集是渗透攻击的前提，通过信息收集可以有针对性地制定模拟攻击测试计划，提高模拟攻击的成功率，同时可以有效的降低攻击测试对系统正常运行造成的不利影响。 信息收集的方法包括端口扫描、操作系统指纹判别、应用判别、账号扫描、配置判别等。 |
| 端口扫描 | 通过对目标地址的TCP/UDP端口扫描，确定其所开放的服务的数量和类型，这是所有渗透测试的基础。通过端口扫描，可以基本确定一个系统的基本信息，结合安全工程师的经验可以确定其可能存在以及被利用的安全弱点，为进行深层次的渗透提供依据。 |
| 口令猜测 | 本阶段将对暴露在公网的所有登陆口进行口令猜解的测试，找出各个系统可能存在的弱口令或易被猜解的口令。猜解成功后将继续对系统进行渗透测试，挖掘嵌套在登录口背后的漏洞、寻找新的突破口以及可能泄漏的敏感信息，并评估相应的危害性。  猜解的对象包括：WEB登录口、FTP端口、数据库端口、远程管理端口等。 |
| 远程溢出 | 这是当前出现的频率最高、威胁最严重，同时又是最容易实现的一种渗透方法，一个具有一般网络知识的入侵者就可以在很短的时间内利用现成的工具实现远程溢出攻击。 对于防火墙内的系统存在同样的风险，只要对跨接防火墙内外的一台主机攻击成功，那么通过这台主机对防火墙内的主机进行攻击就易如反掌。 |
| 本地溢出 | 本地溢出是指在拥有了一个普通用户的账号之后，通过一段特殊的指令代码获得管理员权限的方法。使用本地溢出的前提是首先要获得一个普通用户的密码。也就是说由于导致本地溢出的一个关键条件是设置不当的密码策略。 多年的实践证明，在经过前期的口令猜测阶段获取的普通账号登录系统之后，对系统实施本地溢出攻击，就能获取不进行主动安全防御的系统的控制管理权限。 |
| 脚本测试 | 脚本测试专门针对Web服务器进行。根据最新的技术统计，脚本安全弱点为当前Web系统尤其存在动态内容的Web系统存在的主要比较严重的安全弱点之一。利用脚本相关弱点轻则可以获取系统其他目录的访问权限，重则将有可能取得系统的控制权限。因此对于含有动态页面的Web系统，脚本测试将是必不可少的一个环节。 |
| 权限获取 | 通过初步信息收集分析，存在两种可能性，一种是目标系统存在重大的安全弱点，测试可以直接控制目标系统；另一种是目标系统没有远程重大的安全弱点，但是可以获得普通用户权限，这时可以通过该普通用户权限进一步收集目标系统信息。接下来尽最大努力取得超级用户权限、收集目标主机资料信息，寻求本地权限提升的机会。这样不停的进行信息收集分析、权限提升的结果形成了整个的渗透测试过程。 |

**渗透测试内容**。渗透测试将参考OWASP 2021最新发布的Top10 Web应用漏洞排名，并使用测试框架中相应的技术方法：

表三：OWASP 2021 Top 10（包含但不限于本表格内容）

|  |  |  |
| --- | --- | --- |
| **序号** | **漏洞名称** | **漏洞描述** |
| **A01** | 访问控制失效 | 它也被称为授权，它定义了 Web 应用程序如何向某些用户而不是其他用户授予对内容和功能的访问权限。  访问控制强制执行策略，使用户不能在其预期权限之外采取行动。故障通常会导致未经授权的信息泄露、修改或破坏所有数据或执行超出用户限制的业务功能。常见的访问控制漏洞包括：   1) 通过修改 URL、内部应用程序状态或 HTML 页面，或仅使用自定义 API 攻击工具来绕过访问控制检查。   2) 允许将主键更改为其他用户的记录，允许查看或编辑其他人的帐户。   3) 特权提升。在未登录的情况下充当用户或以用户身份登录时充当管理员。   4) 元数据操作，例如重放或篡改 JSON Web 令牌 (JWT) 访问控制令牌，或用于提升权限或滥用 JWT 失效的 cookie 或隐藏字段。   5) CORS 错误配置允许未经授权的 API 访问。   6) 强制以未经身份验证的用户身份浏览经过身份验证的页面或以标准用户身份浏览特权页面。访问 API 时缺少对 POST、PUT 和 DELETE 的访问控制。 |
| **A02** | 加密失败  （此前名为“敏感数据泄露”） | 缺乏加密通常会导致敏感数据泄露或系统受损。   首先是确定传输中和静止数据的保护需求。例如，密码、信用卡号、健康记录、个人信息和商业秘密需要额外保护，主要是考虑个人信息保护法相关要求。对于所有此类数据：   1) 是否有任何数据以明文形式传输？这涉及 HTTP、SMTP 和 FTP 等协议。外部互联网流量是危险的。验证所有内部流量，例如，负载平衡器、Web 服务器或后端系统之间的流量。   2) 默认情况下或在较旧的代码中是否使用任何旧的或弱的加密算法？   3) 是否正在使用默认加密密钥、生成或重复使用弱加密密钥，或者是否缺少适当的密钥管理或轮换？   4) 是否未强制执行加密，例如，是否缺少任何用户代理（浏览器）安全指令或标头？   5) 用户代理（例如，应用程序、邮件客户端）是否不验证收到的服务器证书是否有效？ |
| **A03** | **注入** | 它是一种攻击者利用未经验证的输入漏洞并通过在后端数据库中执行的 Web 应用程序注入 SQL 命令的技术。  跨站脚本攻击现在是此版本中此类别的一部分。  应用程序在以下情况下容易受到攻击：   1) 应用程序不会验证、过滤或清理用户提供的数据。   2) 没有上下文感知转义的动态查询或非参数化调用直接在解释器中使用。   3) 在对象关系映射 (ORM) 搜索参数中使用恶意数据来提取额外的敏感记录。   4) 直接使用或连接恶意数据。SQL 或命令包含动态查询、命令或存储过程中的结构和恶意数据。  源代码审查是检测应用程序是否容易受到注入攻击的最佳方法。强烈建议对所有参数、标头、URL、cookie、JSON、SOAP 和 XML 数据输入进行自动化测试。 |
| **A04** | **不安全的设计** | 它关注与设计和架构缺陷相关的风险。  安全设计是一种文化和方法，它不断评估威胁并确保代码经过稳健设计和测试，以防止已知的攻击方法。安全设计需要安全的开发生命周期、某种形式的安全设计模式或铺砌道路组件库或工具，以及威胁建模。 |
| **A05** | **安全配置错误** | 它侧重于跨应用程序堆栈的安全加固或对云服务的权限配置不当。XML 外部实体 (XXE) （XML External Entities，XXE）现在属于此类别。如果应用程序是：   1) 在应用程序堆栈的任何部分缺少适当的安全强化或对云服务的权限配置不正确。   2) 启用或安装了不必要的功能（例如，不必要的端口、服务、页面、帐户或权限）。   3) 默认帐户及其密码仍处于启用状态且未更改。   4) 向用户显示堆栈跟踪或其他信息过多的错误消息。   5) 对于升级的系统，最新的安全功能被禁用或未安全配置。   6) 应用程序服务器、应用程序框架（例如，Struts、Spring、ASP.NET）、库、数据库等中的安全设置未设置为安全值。   7) 服务器不发送安全标头或指令，或者未设置为安全值。   8) 软件已过时或易受攻击 |
| **A06** | **易受攻击和过时的组件** | 此类别重点关注客户端和服务器端使用的所有易受攻击的组件版本。你的系统可能很脆弱：   1) 如果您不知道您使用的所有组件的版本（客户端和服务器端）。这包括您直接使用的组件以及嵌套的依赖项。   2) 如果软件易受攻击、不受支持或已过期。这包括操作系统、Web/应用程序服务器、数据库管理系统 (DBMS)、应用程序、API 和所有组件、运行时环境和库。   3) 如果您不定期扫描漏洞并订阅与您使用的组件相关的安全公告。   4) 如果您没有以基于风险的方式及时修复或升级底层平台、框架和依赖项。这通常发生在修补是变更控制下的每月或每季度任务的环境中，使组织面临数天或数月不必要地暴露于固定漏洞的风险。   5) 如果开发人员不测试升级或修补的库的兼容性。   6) 如果您不保护组件的配置（请参阅 A05:2021-安全配置错误）。 |
| **A07** | **认证和授权失败** | 此类别侧重于身份验证失败。  确认用户的身份、身份验证和会话管理对于防止与身份验证相关的攻击至关重要。  如果应用程序存在以下情况，则可能存在身份验证漏洞：   1) 允许自动攻击，例如撞库，其中攻击者拥有有效用户名和密码的列表。   2) 允许蛮力或其他自动攻击。   3) 允许使用默认密码、弱密码或众所周知的密码，例如“Password1”或“admin/admin”。   4) 使用弱或无效的凭据恢复和忘记密码流程，例如无法确保安全的“基于知识的答案”。   5) 使用纯文本、加密或弱散列密码（请参阅 A3:2017-敏感数据泄露）。   6) 缺少或无效的多因素身份验证。   7) 在 URL 中公开会话 ID（例如，URL 重写）。   8) 成功登录后不要轮换会话 ID。   9) 不会正确地使会话 ID 无效。用户会话或身份验证令牌（主要是单点登录 (SSO) 令牌）在注销或一段时间不活动期间未正确失效。 |
| **A08** | **软件和数据完整性故障** | 它侧重于与无法防止完整性违规的代码和基础设施相关的软件和数据完整性故障。  软件和数据完整性故障与不能防止完整性违规的代码和基础设施有关。例如，在对象或数据被编码或序列化为攻击者可以看到和修改的结构的情况下，很容易受到不安全的反序列化的影响。另一种形式是应用程序依赖来自不受信任的来源、存储库和内容交付网络 (CDN) 的插件、库或模块。不安全的 CI/CD 管道可能会导致未经授权的访问、恶意代码或系统受损。最后，许多应用程序现在包括自动更新功能，其中更新在没有充分完整性验证的情况下被下载并应用于以前受信任的应用程序。攻击者可能会上传自己的更新以分发并在所有安装上运行。  2017 年的不安全反序列化（Insecure Deserialization）现在是这一大类别的一部分。 |
| **A09** | **安全日志记录和监控失败** | 如果没有日志记录和监控，就无法检测到漏洞：   1) 不记录可审计的事件，例如登录、失败登录等。   2) 警告和错误不会生成、不充分或不清楚的日志消息。   3) 不监控应用程序和 API 的日志是否存在可疑活动。   4) 日志仅存储在本地。   5) 适当的警报阈值和响应升级流程没有到位或有效。   6) DAST 工具（例如 OWASP ZAP）的渗透测试和扫描不会触发警报。   7) 应用程序无法实时或接近实时地检测、升级或警告主动攻击。 |
| **A10** | **服务器端请求伪造** | 侧重于保护 Web 应用程序在不验证用户提供的 URL 的情况下获取远程资源的连接。  每当 Web 应用程序在未验证用户提供的 URL 的情况下获取远程资源时，就会出现 SSRF 缺陷。它允许攻击者强制应用程序将精心设计的请求发送到意外目的地，即使受到防火墙、VPN 或其他类型的网络 ACL 的保护也是如此。 |

**编制渗透测试报告。**渗透测试过程中，需提交《渗透测试用例清单》、《渗透测试记录》、《漏洞汇总表》等过程文件以及最终版《渗透测试报告》。渗透测试报告应包含渗透测试的整个流程描述，同时还会对发现安全问题的思路与技术手法进行必要的说明，并结合测试目标所处的业务环境，对安全问题进行风险分析（如：可能产生的后果等方面）。除此以外，测试人员还将针对发现的问题提出解决方案，以便用户在修复过程中参考使用。

**渗透测试验证。**协助系统运维单位针对渗透测试过程中发现的漏洞进行层次性的安全加固，特别对于通过渗透测试发现的漏洞进行适应性的补救和加固措施，在保证不影响正常业务的情况下，配合客户实施加固方案。对于加固后的系统进行重复性的渗透测试验证，以保障漏洞不可利用性，同时验证安全加固措施的有效性。确保客户对外提供安全稳定的服务。

3.漏洞扫描服务。利用漏洞扫描工具，通过对信息系统的扫描、探测等操作，使其产生特定的响应等活动，查看、分析响应结果，获取证据以证明信息系统安全保护措施是否得以有效实施的一种方法。测试系统清单见表一：信息系统清单。

4.网络安全自查服务。根据省、市网络安全主管部门要求，并结合我局信息安全管理实际需要，协助建设单位在重要时点对全局网络和信息系统开展信息安全专项自查工作。通过定期网络安全检查及时发现局机关及局属事业单位、住建行业在信息安全方面与国家标准要求之间的差距，为全局信息系统安全建设和管理提供系统性、针对性、可行性的指导和服务，有效监控住建条线信息安全建设成本，提高全局信息系统安全防护的整体水平，确保全局信息安全建设与信息化发展相协调。

5.提供SDL(安全开发生命周期)相关服务。

SDL即Security Development Lifecycle，是[微软](https://baike.baidu.com/item/%E5%BE%AE%E8%BD%AF/124767)提出的从安全角度指导软件开发过程的管理模式，核心理念是将[软件安全](https://baike.baidu.com/item/%E8%BD%AF%E4%BB%B6%E5%AE%89%E5%85%A8)的考虑集成在[软件开发](https://baike.baidu.com/item/%E8%BD%AF%E4%BB%B6%E5%BC%80%E5%8F%91)的每一个阶段[需求分析](https://baike.baidu.com/item/%E9%9C%80%E6%B1%82%E5%88%86%E6%9E%90)、设计、编码、测试和维护。通过SDL的实施，有望从源头加强系统安全防御能力，保证安全技术措施同步规划、同步建设。包含但不限于：协助建设单位编制和审查信息系统安全设计方案，协助建设单位开展代码审计等服务。

**协助建设单位编制和审查信息系统安全设计方案。**根据采购人要求，对住建局（含局属事业单位）的信息化项目进行进行安全专项审查（包含但不限于），并出具意见。协助建设单位编制局机关及局属事业单位信息系统建设方案、可行性研究报告或初步设计的《安全系统建设》章节，包括分析安全风险隐患、明确系统安全域划分、安全等级设定、制定安全策略、提出安全解决方案、安全设备或服务选型等。

**协助建设单位开展代码审计。**代码审计是对信息系统源代码的全面分析，旨在发现错误、安全漏洞或违反编程约定。代码审计对象包括并不限于对Windows和Linux系统环境下的以下语言进行审核：Java(J2EE)、JavaScript、C#（.Net）、Python、Node、Go、C++等。

代码审计的目标系统包括但不限于表1信息系统清单，原则上应覆盖全局（含局属事业单位）新建或扩建类系统，结合软件工程师人工审计和自动化工具审计，审计内容包括但不限于：

（1）弱口令（重点针对强制性密码规则、默认密码、密码加密存储、限制登录失败尝试次数等）。

（2）中间件的配置规范（重点针对数据库连接串加密配置、使用超级账户作为开发账号、应用服务器安全配置等）

（3）SQL语句的编写规范（重点针对SQL注入等)

（4）WEB服务（页面、接口）的权限配置（明确各类角色对不同资源的访问控制权限、强制除公开信息外所有HTTP请求均应通过访问控制检查）

（5）对抗爬虫引擎的处理措施（验证码）

（6）使用含有已知漏洞的组件（移除代码中不必要的依赖、不需要的功能、组件、文件和文档，使用DependencyCheck等工具来持续监控代码依赖库的版本信息和漏洞信息，及时升级存在已知漏洞的组件）

（7）日志记录（确保登录、访问控制失败、输入验证失败信息、时间戳、标识信息(IP和用户ID)被保存到日志，但不能记录敏感信息，日志保存应不低于6个月）。

（8）数据库验证。通过相关系统供应商的支持，可直接进入系统数据库对相关安全设计进行验证，比如弱口令、敏感信息加密保存等。

6.应急保障、宣传培训等其他服务。协助建设单位开展应急演练，网络安全法律法规宣传、培训。

7.商务要求及服务周期。

等保测评服务：根据采购人要求及时开展相关系统等保测评服务并协助整改到位后及时出具测评报告。

其他渗透测试、漏洞扫描等各项服务：合同起始日期不早于2023年5月22日，服务期限1年。

**附件1 比选函**

无锡市住房和城乡建设局：

我公司(单位)已收到贵单位的比选邀请文件，经认真研究，我公司(单位)决定参与“**信息系统安全技术服务项目**”的方案比选。

1.我公司(单位)提供该项目报价总金额为：人民币\_\_\_\_万元（大写： 元整 ）。

2.如果中选，我公司(单位)将履行比选文件中规定的每一项要求，按期、按质、按量完成本项目。

参选人(盖章)：

法定代表人或授权代理人（签字或盖章）：

日 期：

附件2 关于资格要求的声明函

无锡市住房和城乡建设局：

我公司（单位）参加本项目政府采购活动前三年内，在经营活动中没有重大违法记录，我公司（单位）投标文件中所有关于参选人资格要求的文件、证明、陈述均是真实的、准确的。若有违背，我公司（单位）愿意承担由此而产生的一切后果。

参选人（盖章）：

法定代表人或授权代理人（签字或盖章）：

日期：

附件3 法定代表人授权委托书

无锡市住房和城乡建设局：

特授权代表我公司（单位）全权办理针对**“信息系统安全技术服务项目”**的投标、参与开标、评标、签约等具体工作，并签署全部有关的文件、协议及合同。

我公司（单位）对被授权代表的签名负全部责任。

在撤销授权的书面通知送达你处以前，本授权书一直有效，被授权代表签署的所有文件（在授权书有效期内签署的）不因授权的撤销而失效。

被授权代表情况：

姓名：电话：

身份证：

参选人（盖章）：

法定代表人（签字或盖章）：

附件4 承诺书

（参选人名称）在此承诺：

1．本公司（单位）对本项目所提供的产品和服务满足比选文件要求；

2．本公司（单位）具备履行合同所必需的设备和专业技术能力；

3. 本公司未被“信用中国”网站（[www.creditchina.gov.cn](http://www.creditchina.gov.cn)）列入失信执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单。

如违背上述承诺，本公司（单位）将承担一切法律责任。

参选人（盖章）：

日期：

附件5 明细报价表

参选人名称（盖章）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **信息系统安全技术服务** | | | | |
| **项目名称** | | **数量** | **单价** | **分项总报价** |
|  | |  |  |  |
|  | |  |  |  |
|  | |  |  |  |
|  | |  |  |  |
| **合计** | |  | **总价** |  |
| **完工期** | |  | | |
| **项目整体免费质保期** | |  | | |
| **投标人是否属于小、微型企业** | |  | | |
| 服  务  承  诺 | 1.质量 2.安装3."三包"(包修、包退、包换)4.其他承诺  （以上是主要承诺，供投标人参考，投标人应在满足招标文件要求的基础上，根据自己单位的情况作出具体承诺） | | | |
|  | | | |

**法定代表人或法定代表人授权代表签字或盖章：**

**备注：工作量清单需包含软件开发、测试、部署、培训、税费都所有费用。**

附件6 项目人员配置清单

参选人名称（盖章）

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **姓名** | **性别** | **本项目职责** | **工作经验(年)** | **职称/证书** | **是否驻场** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| …… |  |  |  |  |  |  |

**法定代表人或法定代表人授权代表签字或盖章：**

附件7 中小企业声明函

本公司郑重声明，根据《政府采购促进中小企业发展暂行办法》（财库[2011]181号）的规定，本公司为\_\_\_\_\_\_（请填写：中型、小型、微型）企业。即，本公司同时满足以下条件：

1、根据《工业和信息化部、国家统计局、国家发展和改革委员会、财政部关于印发中小企业划型标准规定的通知》（工信部联企业[2011]300号）规定的划分标准，本公司为\_\_\_\_\_\_（请填写：中型、小型、微型）企业。

2、本公司参加\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_单位的\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_项目采购活动，由本企业提供服务，本企业承诺不再委托第三方企业间接提供服务。

本公司对上述声明的真实性负责。如有虚假，将依法承担相应责任。

参选人（盖章）：

日 期：

附件8 无锡市住建局方案比选评分细则

项目名称：**信息系统安全技术服务项目**

比选时间：年月日

|  |  |  |  |
| --- | --- | --- | --- |
| 参选企业 |  | | |
| 报价(万) |  | | |
| 报价得分  (40分) | 备注：满足比选文件要求且投标价格最低的报价为评标基准价，其报价得分为满分。其他参选人报价得分=(评标基准价/投标报价)×报价得分上限 | | |
| 投标人综合情况  (10分) | 投标人近三年来承担过类似项目的成功案例，每提供1个有效合同复印件得1分，最高5分 | |  |
| 项目经理具有高级等级测评师或CISP证书或CISSP证书或中国信息安全认证中心CISAW证书或CIIPT证书或CISA证书的得2分。（相关证书复印件加盖公章） | |  |
| 除项目经理外，其他项目组成员具有中级等级测评师证书或CIIPT证书，每个得1分，累计不超过3分。同一项目组成员具备多个证书的，不重复计分（相关证书复印件加盖公章）。 | |  |
| 技术分  (50分) | 服务方案  (40分) | 等保测评（5分）（优秀4-5分，良好3-4分，一般2-3分，无方案不得分） |  |
| 渗透测试（5分）（优秀4-5分，良好3-4分，一般2-3分，无方案不得分） |  |
| 漏洞扫描（5分）（优秀4-5分，良好3-4分，一般2-3分，无方案不得分） |  |
| 网络安全自查（5分）（优秀4-5分，良好3-4分，一般2-3分，无方案不得分） |  |
| 协助安全设计方案审查和编制（5分）（优秀4-5分，良好3-4分，一般2-3分，无方案不得分） |  |
| 代码审计（5分）（优秀4-5分，良好3-4分，一般2-3分，无方案不得分） |  |
| 应急演练（5分）（优秀4-5分，良好3-4分，一般2-3分，无方案不得分） |  |
| 宣传培训（5分）（优秀4-5分，良好3-4分，一般2-3分，无方案不得分） |  |
| 项目实施  （10分） | 进度安排（5分）：有完善的项目实施方案，提出较合理的项目管理建议，制定详细的进度计划（优秀4-5分，良好3-4分，一般2-3分，无方案不得分） |  |
| 质量控制（5分）：对等保测评以及其他服务提出合理的质量控制措施（优秀4-5分，良好3-4分，一般2-3分，无方案不得分） |  |
| 评审人员 |  | |  |

备注：

1、本项目实行综合评分法，满分100分。参选人最终得分取所有评委打分的算术平均值，得分最高的候选人为中选人。

2、报价得分计算方式：满足比选文件要求且投标价格最低的报价为评标基准价，其报价得分为满分。其他参选人报价得分=(评标基准价/投标报价)×报价权值×100分。

3、价格扣除。①对小型和微型企业产品的价格给予10%的扣除，用扣除后的价格参与评审。参加比价的中小企业，应当按照《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）的规定提供《中小企业声明函》（货物/服务）（中小企业划型标准详见《关于印发中小企业划型标准规定的通知》工信部联企业〔2011〕300号）。②监狱企业视同小型、微型企业，对其产品价格给予10%的扣除，用扣除后的价格参与评审。参加比价的监狱企业，应当按照《关于政府采购支持监狱企业发展有关问题的通知》（财库〔2014〕68号）的规定提供由省级以上监狱管理局、戒毒管理局(含新疆生产建设兵团)出具的属于监狱企业的证明文件复印件。③残疾人福利性单位视同小型、微型企业，对其产品价格给予10%的扣除，用扣除后的价格参与评审。参加比价的残疾人福利性单位，应当按照《财政部、民政部、中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）的规定提供《残疾人福利性单位声明函》。

同一供应商，上述三项价格扣除优惠不得重复享受。

无锡市住建局方案比选打分汇总表

项目名称：**信息系统安全技术服务项目**

日期：年月日

各参选企业得分如下：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 参选企业 | 报价  (万元) | 专家打分 | 专家打分 | 专家打分 | 专家打分 | 专家打分 | 得分  (平均分) |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

评审小组成员签字：