## 第二章 招标项目需求

### 一、对通用条款的补充内容

|  |  |  |
| --- | --- | --- |
| **序号** | **内 容** | **规 定** |
| 1 | 联合体投标 | 见《招标公告》中“投标人资格要求”部分的相关内容 |
| 2 | 投标有效期 | 120日历天（从投标截止之日算起） |
| 3 | 投标人的替代方案 | 不允许 |
| 4 | 投标文件的投递 | 本项目实行网下投标，按照招标文件的要求提交纸质文件正本1份，副本4份，电子文件1份（WORD和PDF格式电子文档各1份）电子文档要求U盘，PDF格式有签字盖章，不留密码，无病毒，不压缩，密封提交，所有应答文件应于递交截止时间之前送达招标文件规定的地址。 |
| 5 | 履约保证金 | \_\_\_\_\_万元或合同金额的\_\_\_\_\_%，缴纳方式：/ |
| 6 | 中标服务费 | 根据“深圳市财政委员会关于规范深圳市社会采购代理机构管理有关事项的补充通知(深财购[2018]27号)”的规定执行。招标代理服务收费以中标/成交通知书公布的中标金额为计算基准,按差额定率累进法计算,作为招标代理服务费。低于人民币陆仟元的，按陆仟元计取。 |

备注：本表为通用条款相关内容的补充和明确，如与通用条款相冲突的以本表为准。

### 二、实质性条款

|  |  |
| --- | --- |
| 序号 | 具体内容 |
| 1 | 完全满足本项目服务期限的要求。 |
| 2 | 为保证项目数据保密性，相关人员需签署保密协议 |
| …… |  |

注：上表所列内容为不可负偏离条款

### 三、项目概况

（一）预算金额: 人民币柒拾肆万肆仟玖佰元（744,900.00），最高投标限价: 人民币柒拾肆万肆仟玖佰元（744,900.00）

（二）项目概况:

根据国务院应对新型冠状病毒肺炎疫情联防联控机制综合组《关于进一步做好疫情防控管理平台使用工作的通知》、省疫情防控信息系统管理联席会商机制《关于进一步加强疫情防控相关信息系统网络安全保障的通知》以及深圳市疫情防控指挥办、市委网信办关于加强疫情防控相关信息系统平台网络安全保障的工作要求，我局需重点加强全市各涉疫系统网络安全、数据安全和运行安全保障，强化涉疫系统平台数据资源融合安全。根据疫情防控需要，全市紧急上线了一批涉疫系统平台，我局在摸底调研全市涉疫系统中发现，全市大部分涉疫系统未进行网络安全等级保护测评，提升涉疫系统平台安全防控水平迫在眉睫。我局将组织专业技术力量加大对全市涉疫系统平台的网络安全漏洞扫描、渗透测试强度，常态化开展全市涉疫系统平台网络安全和数据安全检查，督促指导相关单位整改修复，筑牢全市常态化疫情防控防线。

（三）项目服务内容及清单

|  |  |  |
| --- | --- | --- |
| 序号 | 服务项 | 服务内容 |
| 1 | 网络安全漏洞扫描服务 | 通过人机结合的方式，使用自动化漏洞扫描工具发现各涉疫应用系统及其他相关系统存在的漏洞，评估各涉疫系统存在的各种安全隐患，并输出相关的漏洞检测报告和相应的修复或整改建议。 |
| 2 | 深度渗透测试与安全加固协助工作 | 对涉疫系统及其他相关系统统一进行一次全面深度渗透测试工作，充分挖掘系统存在的安全漏洞并协助整改，确保安全漏洞及时清零。 |
| 3 | 安全自查与检查工作 | 推动各单位开展涉疫系统及其他相关系统的专项检查工作，并依据自查结果抽取部分单位进行针对性自查，确保系统安全保障工作得到有效落实 |
| 4 | 安全监测与安全加固协助工作 |  对涉疫系统及其他相关系统实行7\*24小时的重点监测，及时发现安全隐患，协助责任单位完成整改加固。 |
| 5 | 基础渗透测试与安全加固协助工作  | 对涉疫系统及其他相关系进行每月一次的基础渗透测试工作，定期进行安全状况体检，及时发现系统的安全隐患，进行整改。 |
| 6 | 系统基线制定工作 | 针对已经发现的安全漏洞进行分析总结，形成具体的管理要求和操作指引，并下发给各单位进行落实，让同类漏洞不再重复出现。 |
| 7 | 预案完善工作 | 完善深圳市网络安全事件应急预案，同时督导相关责任单位制定专项应急预案，确保出现安全事件时可以及时处置。 |
| 8 | 应急响应工作要求  | 提供应急专家协助责任单位进行应急处置工作，确保安全事件得到有效解决 |

### 四、项目技术要求

**1.网络安全漏洞扫描服务**

 对服务范围内的业务系统及服务器等开展漏洞扫描工作，并对发现的所有漏洞进行验证，验证漏洞在已有的网络安全体系发生的风险及分析发生后可造成的危害，并进行优先级排序，按照计划高质量提供网络安全风险加固建议并指导相关责任人进行修复。

输出交付：《漏洞扫描报告》。

服务质量要求：首次扫描发现的所有中高危漏洞原则上必须在3个月内完成加固；新扫描发现的中高危漏洞原则上在24小时内给出解决方案，尽快完成修复。

**2.深度渗透测试与安全加固协助工作要求**

对指定的涉疫系统和其它系统统一进行一次全面深度渗透测试工作，充分挖掘系统存在的安全漏洞并协助整改，确保安全漏洞及时清零。专业渗透测试根据招标人所指定信息资产情况，制定渗透测试方案，在征得招标人同意后，通过现场+远程方式模拟入侵者，使用主流攻击技术对目标网络环境、信息系统、数据库等进行模拟非破坏性攻击测试，旨在发现潜在的各类风险、威胁及漏洞。针对性给出整改防护措施，并全程协同招标方人员进行风险排除和漏洞加固。每次服务需至少包括渗透测试一次、复检一次，复检如仍发现风险，需继续加固，直至风险消除。

**系统测试至少应包含但不限于以下内容：**

| **测试大类** | **测试项** | **测试目的** |
| --- | --- | --- |
| 身份验证类 | 用户注册 | 检查用户注册功能可能涉及的网络安全问题 |
| 用户登录 | 检查用户登录功能可能涉及的网络安全问题 |
| 修改密码 | 检查用户修改密码功能可能涉及的网络安全问题 |
| 密码重置 | 检查忘记密码、找回密码、密码重置功能可能涉及的网络安全问题 |
| 验证码绕过 | 检测验证码机制是否合理，是否可以被绕过 |
| 用户锁定功能 | 测试用户锁定功能相关的网络安全问题 |
| 会话管理类 | Cookie重放攻击 | 检测目标系统是否仅依靠cookie来确认会话身份，从而易受到cookie回放攻击 |
| 会话令牌分析 | Cookie具有明显含义，或可被预测、可逆向，可被攻击者分析出cookie结构 |
| 会话令牌泄露 | 测试会话令牌是否存在泄露的可能 |
| 会话固定攻击 | 测试目标系统是否存在固定会话的缺陷 |
| 跨站请求伪造 | 检测目标系统是否存在CSRF漏洞 |
| 访问控制类 | 功能滥用 | 测试目标系统是否由于设计不当，导致合法功能非法利用 |
| 垂直权限提升 | 测试可能出现垂直权限提升的情况 |
| 水平权限提升 | 测试可能出现水平权限提升的情况 |
| 输入处理类 | SQL注入 | 检测目标系统是否存在SQL注入漏洞 |
| 文件上传 | 检测目标系统的文件上传功能是否存在缺陷 ，导致可以上传非预期类型和内容的文件 |
| 任意文件下载 | 检测目标系统加载/下载文件功能是否可以造成任意文件下载问题 |
| XML注入 | 测试目标系统-是否存在XML注入漏洞 |
| 目录穿越 | 测试目标系统是否存在目录穿越漏洞 |
| SSRF | 检测目标系统是否存在服务端跨站请求伪造漏洞 |
| 本地文件包含 | 测试目标站点是否存在LFI漏洞 |
| 远程文件包含 | 测试目标站点是否存在RFI漏洞 |
| 远程命令/代码执行 | 测试目标系统是否存在命令/代码注入漏洞 |
| 反射型跨站脚本 | 检测目标系统是否存在反射型跨站脚本漏洞 |
| 存储型跨站脚本 | 检测目标系统是否存在存储型跨站脚本漏洞 |
| DOM-based跨站脚本 | 检测目标系统是否存在DOM-based跨站脚本漏洞 |
| 服务端URL重定向 | 检查目标系统是否存在服务端URL重定向漏洞 |
| 信息泄露类 | error code | 测试目标系统的错误处理能力，是否会输出详尽的错误信息 |
| Stack Traces | 测试目标系统是否开启了Stack Traces 调试信息 |
| 敏感信息 | 尽量收集目标系统的敏感信息 |
| 第三方应用类 | 中间件 | 测试目标系统是否存在jboss、weblogic、tomcat等中间件漏洞 |
| CMS | 测试目标系统是否存在dedecms、phpcms等CMS漏洞 |

**3.安全自查与检查工作要求**

从信息安全等级保护、关键业务信息安全、关键信息基础设施安全、人员安全管理培训等方面对涉疫系统和其他系统相关单位网络与信息安全工作建设的各项情况进行专项安全检查，在招标人授权下，协助对各单位进行网络信息安全检查，包括安全检查方案、自查报告及表格、现场检查方案等制定，检查已抽检形式进行，检查内容不限于文件审阅、渗透测试、现场上机检查等，确认各相关单位可能存在的安全问题，并协助推动整改。

交付物：安全检查工作方案、检查记录、检查报告。

服务范围：招标人所要求的涉疫系统和其他系统相关单位。

**4.安全监测与安全加固协助工作要求**

综合运用资深网络安全经验和丰富的威胁情报知识库，对主要网络安全设备的安全日志、流量进行关联分析，并对网络安全威胁的定位，帮助精准检测网络中的攻击行为。同时，对识别到的威胁进行主动响应，制定合理的建议并指导事发单位采取措施降低威胁可能造成的影响，快速闭环处置网络安全事件。

交付物：风险评估报告、风险整改方案、差距分析报告、主机/终端漏扫报告、漏洞加固方案、复检报告等。

服务内容：对招标人指定的信息系统存在的网络安全风险、补丁漏洞进行修复、加固评估，出具修复方案并指导完成修复。

服务质量及效率要求：首次扫描发现的所有中高危漏洞原则上在3个月内完成加固；新扫描发现的中高危漏洞原则上在24小时内给出解决方案，在7天内完成加固。

**5.基础渗透测试与安全加固协助工作要求**

 根据指定的涉疫系统和其他系统信息资产情况，进行每月一次的基础渗透测试工作，定期进行安全状况体检，及时发现系统的安全隐患，进行整改。先制定渗透测试方案，在征得相关单位同意后，通过现场+远程方式模拟入侵者，使用主流攻击技术对目标网络环境、信息系统、数据库等进行模拟非破坏性攻击测试，旨在发现潜在的各类风险、威胁及漏洞。针对性给出整改防护措施，并全程协同招标人相关人员进行风险排除和漏洞加固。

交付物：渗透测试报告、复检报告等。

服务工具要求：提供一套渗透测试工具。

**6.系统基线制定工作要求**

针对已经发现的安全漏洞进行分析总结，形成具体的管理要求和操作指引，并下发给各单位进行落实，让同类漏洞不再重复出现。基线制定所需核查的项目应包含但不限于以下内容：

网络设备： OS安全、帐号和口令管理、认证和授权策略、网络与服务、访问控制策略、通讯协议、路由协议、日志审核策略、加密管理、设备其他安全配置等；

操作系统：系统漏洞补丁管理、帐号和口令管理、认证、授权策略、网络与服务、进程和启动、文件系统权限、访问控制、通讯协议、日志审核功能、剩余信息保护、其他安全配置等；

数据库：漏洞补丁管理、帐号和口令管理、认证、授权策略、访问控制、通讯协议、日志审核功能、其他安全配置等；

中间件：漏洞补丁管理、帐号和口令管理、认证、授权策略、通讯协议、日志审核功能、其他安全配置等。

交付物：《安全配置基线》

服务范围：招标人指定的涉疫系统和其他相关系统

**7.预案完善工作要求**

 完善招标人指定的涉疫系统和其他相关系统网络安全事件应急预案，建立标准应急管理体系制度文档，参考《中华人民共和国突发事件应对法》、《国家突发公共事件总体应急预案》、《国家网络与信息安全事件应急预案》、《广东省网络与信息安全事件应急预案》等相关规定和网络安全法，建立信息安全事件分级标准及应急流程。

交付物：网络安全突发事件总体应急预案

服务范围：招标人指定的涉疫系统和其他相关系统

**8.应急响应工作要求**

 提供应急专家协助责任单位进行应急处置工作，确保安全事件得到有效解决。建立应急保障团队（提供应急保障团队人员名单与联系方式），提供多种方式（现场支持、远程支持等）的安全事件应急服务。一年内有效的安全事件应急响应，当安全威胁事件发生后，迅速采取措施和行动，阻止和降低安全威胁事件带来的严重影响。全天候 7×24 小时的技术支持，半小时内响应，2小时内到现场服务，帮助控制安全事件扩散，给出应对安全方案。

组建高级别网络信息安全专家队伍，为招标人指定的涉疫系统和其他系统及时处理解决网络信息安全有关的疑难事宜。

交付物:《应急响应报告》（如未发生安全事件，则无需提供）

服务范围：招标人指定的涉疫系统和其他系统相关单位

### 五、项目商务要求

（一）服务期限：2022年12月1日前完成交付

（二）付款方式：以合同约定为准

（三）质量考核验收标准及违约金

1.质量考核验收标准：完成合同内容并提交相关工作成果，中标方承担项目验收产生的相应费用。

2.违约金：以合同约定为准

### 六、投标报价

1.本项目服务费采用包干制，应包括服务成本、法定税费和企业的利润。由企业根据招标文件所提供的资料自行测算投标报价；一经中标，投标报价总价作为中标单位与采购人签定的合同金额，合同期限内不做调整。

2.投标人应根据本企业的成本自行决定报价，但不得以低于其企业成本的报价投标；评标时，评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。

3.投标人的投标报价，应是本项目招标范围和招标文件及合同条款上所列的各项内容中所述的全部，不得以任何理由予以重复，并以投标人在投标文件中提出的综合单价或总价为依据。

4.除非政府集中采购机构通过修改招标文件予以更正，否则，投标人应毫无例外地按招标文件所列的清单中项目和数量填报综合单价或总价。投标人未填综合单价或总价的项目，在实施后，将不得以支付，并视作该项费用已包括在其它有价款的综合单价或总价内。

5.投标人应充分了解项目的位置、情况、道路及任何其它足以影响投标报价的情况，任何因忽视或误解项目情况而导致的索赔或服务期限延长申请将不获批准。

6.投标人不得期望通过索赔等方式获取补偿，否则，除可能遭到拒绝外，还可能将被作为不良行为记录在案，并可能影响其以后参加政府采购的项目投标。各投标人在投标报价时，应充分考虑投标报价的风险。