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，按照谈判文件的要求提交纸质文件正本1份、副本5份（含电子文件）所有谈判应答文件应于递交截止时间之前送达谈判文件规定的地址。 |
| 5 | 履约保证金 | \_\_\_\_\_万元或合同金额的0%，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。 |

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 | 为深圳市市场监督管理局官网，域名：amr.sz.gov.cn和深圳信用网，域名：www.szcredit.org.cn 提供7\*24小时云防护服务（包括提供无限制访问流量、抗DDOS攻击服务、原厂技术支持服务），每月提供1次云防护分析报告。 |
| …… |  |

注：上表所列内容为不可负偏离条款

三、招标项目概况

1、项目概况:为切实做好我局2020年度信息安全绩效考评工作，积极推进信息管理体系和制度建设，构建安全高效的信息安全运维及服务工作，提升全局信息安全服务、风险评估、渗透测试、网站安全防护、应急响应等方面的能力与水平，创建安全健康的网络环境，促进我局信息系统的稳定和安全发展，特对2020年“深圳市市场监督管理局信息安全服务”项目进行公开招标。

2、（二）预算金额: 人民币96.035万元，最高投标限价: 人民币96.035万元

3、项目工期要求：本项目服务期限自2020年9月12日起至2021年9月11日止。本项目属于长期服务项目，合同期限为自合同签订之日起一年。到期后采购人可根据中标供应商履约情况延续合同期限，最长不超过3年；

四、项目技术要求

**一、信息安全绩效和联合检查工作**

按照深圳市党政机关信息安全绩效考评和联合检查工作的要求(具体要求以市党政机关信息安全绩效考评和联合检查主管单位该年度发布的相关文件为准)配合甲方完成自查、整改、文档资料汇编及上报工作。其中绩效考评工作需每季度向我局提交服务器、用户终端及网站应用层的漏洞扫描报告；年度联合检查工作需在检查前一个月完成年度所有工作并将资料汇编成册。

**（一）信息安全绩效考评工作**

1、信息安全防护

每季度一次对局大楼用户终端及核心机房服务器、对外网站的信息安全漏洞扫描和漏洞整改工作。交付物包括但不限于《服务器扫描计划》、《服务器漏洞扫描结果报告》、《网站应用层漏洞扫描扫描计划》、《网站应用层漏洞扫描扫描结果报告》、《计算机终端漏洞扫描结果报告》。

2、信息安全渗透测试防护和处理

每季度一次对局自有信息系统开展渗透测试检测，以黑客角度手工方式挖掘我局现存漏洞。交付物包括但不限于《应用系统渗透自查报告》。

3、信息安全事件防护

为了进一步加强我局的信息防护能力，减少信息安全事件的发生概率，并配合我局处理存在信息安全风险的终端。交付物包括但不限于《应用系统安全事件处理记录》、《终端安全事件处理记录》。

**（二）年度联合检查考评工作**

年度考评工作主要是配合我局完成《2020年深圳市党政机关信息安全联合检查指标及评分标准》各项要求的自查和整改工作，并在检查前一个月完成包含各项汇报材料，取证截图及相关制度执行记录、培训记录等的《年度信息安全联合检查迎检资料汇编》。具体包括:（检查内容以该年度发布的年度联合检查考评指标为准）

| **序号** | **类别** | **工作内容** | **说明** |
| --- | --- | --- | --- |
| 1 | 安全管理 | 组织管理：信息安全管理架构 | 配合用户方梳理网络安全和信息化领导机构成立正式发文和相关资料 |
| 2 | 人员管理 | 配合用户方梳理信息安全关键岗位人员设立文件、关键岗位责任书和关键岗位人员在编情况 |
| 3 | 全员安全意识培训 | 配合用户方编写信息安全意识培训教材，为用户方全体人员开展信息安全意识培训 |
| 4 | 专业人员安全技能培训 | 配合用户方制定本年度专业岗位技术人员的信息安全专业技能培训计划 |
| 5 | 服务外包管理 | 检查服务外包人员是否签署保密合同、接入网络并具有登记记录、进入机房并具有进入机房审批记录。 |
| 6 | 组织机构和安全制度落实 | 配合用户方梳理信息安全组织机构，并落实相关全制度 |
| 7 | 等级保护测评及整改 | 配合用户方开展等级保护备案工作，协助用户完成第三方测评机构的进行工作。 |
| 8 | 个人信息和重要数据 | 配合用户方制定个人信息和重要数据制度落实情况，检查重要数据的分类分级以及数据脱敏等技术手段措施 |
| 9 | 应用系统注册用户实名制管理 | 检查网站或信息系统注册用户实名制情况 |
| 10 | 商用密码管理 | 整理用户方商用密码产品的证明材料 |
| 11 | 安全运营 | 资产登记造册 | 配合运维部门完成用户终端资产的梳理工作 |
| 12 | 安全防护技术落实 | 配合用户方落实网络安全审计和网页防篡改等事项 |
| 13 | 安全隐患排查 | 每季度至少开展一次漏洞扫描工作，并将最新的服务器、网站和终端安全扫描报告报送至采集责任单位 |
| 14 | 设备口令安全管理 | 配合用户落实设备口令的更改频率、口令复杂度 |
| 15 | 设备和信息系统加密保护措施 | 配合用户落实设备和信息系统等管理员密码采用密文存储和加密协议远程登录 |
| 16 | 安全保密工作落实 | 配合用户方开展信息安全保密自查工作 |
| 17 | 计算机安全集中管理 | 检查用户单位是否采用计算机安全集中管理。 |
| 18 | 安全监管 | 渗透检测 | 具体详见“绩效考评”对应章节 |
| 19 | 信息安全事件防护 | 具体详见“绩效考评”对应章节 |
| 20 | 信息安全问题整改 | 1、收到市信息安全主管单位通报后，协助用户方对信息安全问题进行核实和整改2、协助用户方对上一年度联合检查现场检查发现问题进行核实和整改 |
| 21 | 下属单位安全检查工作开展 | 制定下属单位的检查方案，并配合完成对下属单位的安全检查 |
| 22 | 联合检查材料汇编 | 整理和汇编联合检查年度检查所需材料 |

**二、日常信息安全运维工作**

1、网站安全准入检查

按需配合我局完成新上线或改版信息系统的上线检查工作，并输出《信息系统安全准入检测报告》。

2、安全通告

每月对我局现有资源（含网络设备、安全设备、操作系统、数据库、中间件、网站组件和控件）的漏洞更新情况进行收集整理，并汇编为《月度安全通告》。

3、安全巡检

每周一次对我局服务器、安全设备及网络设备进行安全巡检抽查工作，根据服务器清单每周依次轮流抽查10台服务器、2台网络设备及2台安全设备，填写《安全巡检记录》。

4、下属单位信息安全抽查

每半年一次通过渗透测试、信息系统安全漏洞扫描等技术手段对我局下属单位的信息系统进行安全抽查，抽查完毕后输出《下属单位信息安全抽查报告》。

5、信息系统暗链及后门木马查杀

每半年一次对我局对外信息系统进行暗链扫描及后门木马查杀，并输出《应用系统暗链扫描记录》、《应用系统网页后门查杀记录》。

6、信息安全技术咨询

在信息安全措施、安全策略、安全问题、安全管理体系等方面为我局日常运维以及相关信息化安全项目（含金信工程）提供信息安全技术咨询服务。

**三、信息安全制度建设工作**

基于我局已发布的信息安全管理制度以及信息安全联合检查的要求，配合我局推进制度的完善及落地执行工作。

**四、对外网站安全监控工作**

为我局及下属单位对外网站提供7X24小时的网站安全监控服务，监控服务要求如下：

　　1、网站安全监控服务应支持实时对网站暗链扫描和挂马检测，要求采用硬件式监控平台，且要与市信息安全测评中心所用的安全绩效考核监控平台品牌型号及版本一致；

　　2、监控平台需支持7X24小时对网站可用性监控，支持检测和监控网站首页响应速度，判断网站是否掉线，支持DNS、Ping、HTTP请求等多种方式探测网站连通速度；支持检测域名劫持。；

　　3、监控平台需支持同时对所有对外网站的实时监控；

　　4、在发现安全问题后，需在半小时内以短信、电话和邮件等多种方式告知我局；

5、交付物：《网站监控周报》。

**五、网站云防护服务**

为加强我局深圳信用网和官网的应用站点安全风险防范水平，有效防止外部黑客对网站及单位业务系统进行渗透，提供以下域名网站云防护服务：

（1）深圳市市场监督管理局，域名：amr.sz.gov.cn；

（2）深圳信用网，域名：[www.szcredit.org.cn](https://www.szcredit.org.cn) www.szcredit.com.cn；

云防御平台技术要求如下：

（1）智能DNS：可提供智能DNS域名解析，支持NS和cname方式。

（2）web防火墙：可防护SQL注入、命令注入、跨站脚本、跨站请求伪造、信息探测等攻击。

（3）防火墙策略集控制：支持子防护策略集打开关闭；子防护策略集如下：专家防护策略集，扫描器/爬虫防御策略集，异常HTTP请求防御策略集，SQL注入防护策略，POST请求SQL注入防护策略，Webshell防护策略，XSS防护策略，POST请求XSS防护策略，命令/代码执行防护策略，文件包含/注入防护策略，特殊/其他攻击防护策略。

（4）防火墙策略白名单：对指定的策略不进行拦截。

（5）智能攻击防御：可精准识别多种自动化扫描和攻击软件，并阻断其所有请求，减少90%以上的恶意攻击。

（6）WebShell防护：可防止黑客上传、访问WebShell（网站后门）。

（7）后台锁：禁止非授权IP访问网站后台管理地址或重要页面。

（8）防盗链：保护网站图片、压缩包等资源文件不被其它站点盗用。

（9）URL白名单：可以设置不经过防护的URL地址（URL数≤60）。

（10）IP地址黑白名单:可设置不进行防护的IP地址（IP白名单）、不允许访问的IP地址（IP黑名单）。

（11）端口设置：支持网站非标准端口，自助设置协议和端口；

（12）网站概况显示：提供网站访问情况信息展示，包括请求数、总流量、网站浏览人数，搜索引擎引导量，遭受攻击次数等，并能按时间端统计的网站访问量。

（13）安全报告：查看网站安全状况，包括各种攻击发生次数，攻击IP、来源（国家）等；可显示对网站的安全评级，如安全、危险等等，可显示历史攻击次数等；可显示CC攻击详细情况；可显示攻击情况，包括时间、攻击URL，攻击者IP及归属地，攻击类型等；提供一年内自定义报表功能。

（14）实时攻击显示：提供实时攻击视图，在视图中实时显示攻击源IP，国家，目标域名，目标所在地等。

（15）报表下载：默认支持当日、前一天、最近30天和最近一年的报表统计下载。

（16）日志下载：提供最近7天内的攻击和访问日志自助下载服务。

（17）日志审计：提供用户在平台上的操作日志和登录日志，并提供查询功能。

（18）共享证书节点：提供共享证书节点，SSL证书自助上传功能。

（19）清洁流量：清洁流量≥5TB/主域名.年。

（20）产品架构：为云防御架构，SaaS服务方式，无需部署任何软硬件在网站服务器本地，用户无需运营维护升级，全部云端完成，保证高危漏洞出现时在2-6小时内构建安全防护规则，保证网站的安全运行。

（21）售后服务方式与能力：提供7\*24小时的服务咨询、故障受理等服务，并能及时反馈处理进展；提供本地化服务支持，出现问题需要现场服务时，可做到1小时内响应；提供线上微信、QQ、电话等客服支持。

**六、应急响应技术支持服务**

提供7x24小时重大安全事件的应急响应工作，应急响应主要针对突发的网站安全故障、网络安全事件、应用系统安全事件、主机安全事件、黑客攻击事件等进行诊断、分析并协助解决。在完成应急事件响应处理后的3个工作日内向我局提供事件的处理记录及问题整改建议。

**七、驻场服务**

至少安排2名5年以上信息安全相关工作经验的驻场人员，协助配合我局完成本项目的信息安全绩效工作和信息安全日常工作；

驻场人员每周工作五天，与我局工作人员共同考勤，考勤记录作为验收材料之一。

五、项目商务要求

一、项目服务期限：本项目服务期限自2020年9月12日起至2021年9月11日止。本项目属于长期服务项目，合同期限为自合同签订之日起一年。到期后采购人可根据中标供应商履约情况延续合同期限，最长不超过3年。

二、付款方式：合同签订后支付40%合同款，余下60%尾款按合同执行进度支付。

三、验收要求

合同执行完成须由采购方对项目执行情况进行验收，中标人须提交以下材料（但不限于）以备验收：

《服务器扫描计划》，每季度一份，共4份；

《服务器漏洞扫描结果报告》，每季度一份，共4份；

《网站应用层漏洞扫描扫描计划》，每季度一份，共4份；

《网站应用层漏洞扫描扫描结果报告》，每季度一份，共4份；

《计算机终端漏洞扫描结果报告》，每季度一份，共4份；

《应用系统渗透自查报告》，每季度一份，共4份；

《应用系统安全事件处理记录》，按实际所需；

《应用系统暗链扫描记录》，每半年一份，共2份；

《应用系统网页后门查杀记录》，每半年一份，共2份；

《终端安全事件处理记录》，按实际所需；

《信息系统安全准入检测报告》，按实际所需；

《月度安全通告》，每月一份，共12份；

《安全巡检记录》，每周一份，共48份；

《下属单位信息安全抽查报告》，每半年一份，共2份；

《网站监控周报》，每周一份，共53份；

《年度信息安全联合检查迎检资料汇编》，每年一份，共1份。

四 .其他要求

本项目预算控制总金额为人民币96.035万元，超过本预算控制总金额及货物需求表中列明的条目控制单价和总价的投标报价将作废标处理。