网络安全服务项目

需求公示附件

**一、项目基本情况**

（一）采购方式：竞争性磋商

（二）项目名称：网络安全服务项目

（三）采购预算：808000.00元

（四）最高限价：808000.00元

（五）采购内容：网络安全服务项目，具体详见采购文件。

**二、本项目供应商资格条件要求**

（一）符合政府采购法第二十二条规定，提供政府采购法实施条例第十七条规定资料。

1.具有独立承担民事责任的能力：提供法人或其他组织的营业执照等证明文件，或自然人身份证明；

2.具有良好的商业信誉和健全的财务会计制度：

供应商是法人的，提供2023年度或2024年度经会计师事务所出具的审计报告（成立不满一年的提供其基本开户银行出具的2025年1月至投标截止时间前任意时间的银行资信证明），审计报告应盖有会计师事务所单位章和注册会计师的执业专用章，并附会计师事务所的营业执照及执业证书；自然人或其他组织，没有经审计的财务报告，可提供其基本开户银行出具的2025年1月至投标截止时间前任意时间的银行资信证明（须附基本户银行开户许可证）；

3.具有履行合同所必需的设备和专业技术能力：

提供具有履行合同所必需的设备和专业技术能力的证明材料或承诺函（承诺函格式自拟）；

4.具有依法缴纳税收和社会保障资金的良好记录：

提供2024年1月至今任意3个月依法缴纳税收和社会保障资金的相关材料；成立不满3个月的供应商，提供承诺依法缴纳税收和社保的承诺函，承诺函须由法定代表人签名并加盖供应商公章（承诺函格式自拟）；（依法免税或不需缴纳税收的应提供相关证明材料）

5.参加本次投标活动前三年内，在经营活动中没有违法违规记录：

提供参加本次投标活动前3年内在经营活动中没有重大违法记录的书面声明（格式文件详见投标文件范本）；

6.法律、行政法规规定的其他条件：

（1）供应商须承诺：在“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）等渠道查询中未被列入失信被执行人名单、重大税收违法失信主体名单、政府采购严重违法失信行为记录名单中，如被列入失信被执行人、重大税收违法失信主体名单、政府采购严重违法失信行为记录名单中的供应商取消其投标资格，并承担由此造成的一切法律责任及后果）。（格式文件详见投标文件范本）

（2）根据《省发展改革委 省法院 省公共资源交易中心关于推进全省公共资源交易领域对法院失信被执行人实施信用联合惩戒的通知》黔发改财金（2020）421号文件要求，采购人或代理机构在递交投标文件截止时间后现场根据贵州信用联合惩戒平台反馈信息，查询供应商是否属于法院失信被执行人，如被列入取消其投标资格。

（二）本项目所需特殊行业资质或要求:/

（三）本项目不接受联合体投标。

（四）本项目是否专门面向中小企业采购：是。本项目所属行业：软件和信息技术服务业。

**三、****采购范围**

（一）项目概况

主要采用现场+远程方式，提供漏洞扫描、安全检查与分析服务、安全加固、渗透测试、代码审计、应急演练、应急响应、网站监测、风险评估、安全培训、预警通告、蜜罐服务、网站云防护等安全服务。提供服务内容如下：

安全保障服务清单

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 运维项 | 运维内容 | 运维对象 | 运维指标 | 交付物 |
| 1 | 漏洞扫描 | 漏洞扫描服务是对主机操作系统、数据库、网络设备、中间件、WEB应用系统开展安全漏洞扫描，检查当前网络中是否存在高风险漏洞,确保各平台安全风险漏洞及时发现和整治。提供对主机操作系统、数据库、网络设备、中间件、WEB 应用系统等扫描出来的漏洞需要安全专家进行漏洞验证、危害性、修复建议、修复后再次评估漏洞是否存在等的整个人工服务。 | 贵州省机关事务管理局门户网站、贵州省公共机构能耗监管平台、贵州省公共机构节能业务综合服务(SaaS)平台、贵州省党政机关国有资产集中管理平台、贵州省机关事务云5个系统（102个资产（互联网、政务外服务器）） | 4次/年 | 《漏洞扫描报告》《漏洞扫描复测报告》 |
| 2 | 安全检查与分析服务 | 提供对信息系统配套相关安全设备进行定期检查，评估云安全设备运行状态，工作状态、授权状态、运行状况等进行的全面检测，排除设备潜在的故障，并在检测后形成完善的安全设备运行报告。已提前发现设备在运行过程中存在的问题为目的，对整体信息化安全防护系统提出合理的安全建议。以预防为先为原则，对设备现状进行分析并配合整改，以提高安全设备的利用率。掌控信息系统的安全现状，提前发现信息系统运行过程中存在的安全隐患，根据巡检过程中发现的问题进行针对性治理，使得业务持续稳健运行。要求专业的工程师对厂家已经实施的安全产品进行深度检查及验证，是否防护到位，策略是否严格部署，产品软件系统及特征库更新，安全产品是否存在弱口令等。 | 贵州省机关事务管理局门户网站、贵州省公共机构能耗监管平台、贵州省公共机构节能业务综合服务 (SaaS)平台、贵州省党政机关国有资产集中管理平台、贵州省机关事务云5个系统所有安全产品（共部署在互联网的7台，信创节点8台安全产品） | 12次/年 | 《网络安全设备巡检报告》 |
| 3 | 安全加固 | 基于核查情况进行基线加固工作，根据专业安全防护基线配置要求，针对不同目标系统，通过打补丁、修改安全配置、增加安全机制等方法，合理进行服务器安全性加强。安全加固工作主要是通过人工的方式进行，也可以借助特定的安全加固工具进行。加固操作前应该做好相应充分的风险规避措施，加固活动会有跟踪记录，以确保系统的可用性。定期开展安全加固服务，对系统最大可能的排查安全隐患，尽可能避免安全风险的发生，降低入侵风险并能够满足安全合规要求，提供基线安全加固报告。 | 贵州省机关事务管理局门户网站、贵州省公共机构能耗监管平台、贵州省公共机构节能业务综合服务 (SaaS)平台、贵州省党政机关国有资产集中管理平台、贵州省机关事务云5个系统（200个资产） | 2次/年 | 《终端安全加固报告》 |
| 4 | 渗透测试 | 根据已经发现的安全漏洞，主要以通过人工模拟黑客攻击的方式对指定的远程或者本地信息系统的安全脆弱性进行检测，深层次发现各类系统、应用存在的安全问题，及时发现信息系统的漏洞和风险。定期开展专业的渗透测试服务，可以使得信息系统的管理人员了解入侵者可能利用的途径，直观的了解系统真实的安全强度。能够真正未雨绸缪，主动发现安全问题并在第一时间完成有效防护，让攻击者无机可乘，进而避免由于网络黑客攻击造成重大损失。 | 贵州省机关事务管理局门户网站、贵州省公共机构能耗监管平台、贵州省公共机构节能业务综合服务 (SaaS)平台、贵州省党政机关国有资产集中管理平台、贵州省机关事务云5个系统 | 5系统/次 | 《渗透测试报告》《渗透测试复测报告》 |
| 5 | 代码审计 | 以发现程序错误，安全漏洞和违反程序规范为目标的源代码分析，寻找系统中存在的薄弱环节和业务逻辑问题、漏洞等。代码审计采取自动化工具或者人工审查的方式，通过对编程项目中源代码的全面分析，旨在发现错误，安全漏洞或违反编程约定的安全缺陷，检查程序源代码是否存在安全隐患，或者有编码不规范的地方。代码审计过程需要对程序源代码逐条进行检查和分析，发现这些源代码缺陷引发的安全漏洞。防御性编程范例的一个组成部分，能够试图在软件发布之前减少错误。提供代码修订措施和建议，提供代码审计报告。 | 贵州省机关事务管理局门户网站、贵州省公共机构能耗监管平台、贵州省公共机构节能业务综合服务 (SaaS)平台、贵州省党政机关国有资产集中管理平台、贵州省机关事务云5个系统 | 5系统/次 | 《代码审计报告》 |
| 6 | 应急演练 | 安全服务人员配合客户方制定应急演练方案，并参与应急演练；安全服务人员对信息安全事件应急演练流程的经济性、合理性和可行性进行评估；安全服务人员对相关人员进行应急操作培训、提高应急人员的工作熟练程度；安全服务人员参与组织相关专家对安全应急演练的成效进行评判，并协助编制应急演练总结报告。 | 单位相关工作人员 | 1次/年 | 应急演练过程文档、应急演练方案、脚本、《应急演练PPT》、《应急演练签到表》 |
| 7 | 应急响应 | 提供7×24小时的远程安全应急响应，接到安全事件通知后，立即以远程方式对安全事件进行分析、抑制、溯源，如果远程无法进行应急，则指派经验丰富的安全服务工程师，赶到用户现场进行应急处理。最大程度降低信息安全事件带来的损失。 | 所有上云业务系统 | 1年 | 《应急响应报告》 |
| 8 | 网站监测 | 对单位云上业务系统做7\*24小时安全监控，在网站出现异常情况时（被攻击、篡改、挂马），进行实时告警，处置。降低网站被攻击后带来的信息安全风险，满足《网络安全等级保护2.0》和《网络安全法》的相关要求，落实信息安全等级保护的法律义务。 | 贵州省机关事务管理局门户网站、贵州省公共机构节能网、贵州省机关事务云3个系统 | 3 系统/次 | 《网站监测报告》 |
| 9 | 风险评估 | 安全风险评估服务是从风险管理角度，依据有关信息安全技术与管理标准，对信息资产所面临的威胁、存在的弱点、造成的影响，以及三者综合作用所带来风险的可能性的评估。基于全面的风险评估，准确了解信息安全现状，明晰信息安全需求。基于风险评估结果，针对性制定信息系统安全策略和风险解决方案。结合技术与管理，指导未来的信息安全建设和投入，建立自身的信息安全管理框架。 | 所有上云业务系统 | 1次/年 | 《网络安全风险评估报告》 |
| 10 | 安全培训 | 安全问题“三分技术、七分管理”，作为安全管理的主要执行者/人员，在面临信息安全威胁的严峻挑战时，提高安全意识和安全技能，成为了一项必要的工作。提供信息安全意识培训、信息安全技能教育培训，从而真正提升受训人员的安全技术和实际动手能力。提升相关人员的信息安全意识、保密意识；落实网络安全法对信息安全教育培训的要求；提升参训的人员的信息安全技能、了解和掌握基本的信息安全知识。培训时长：1天 | 单位相关工作人员 | 2次/年 | 《安全培训PPT》 《安全培训方案》《安全培训签到表》 |
| 11 | 预警通告 | 提供的内容包括安全事件、安全公告、病毒信息、漏洞信息，以便第一时间得到漏洞的修补办法，防止安全事件的发生。有效的预防安全事故发生，并可以及时做出针对措施。 | 所有上云业务系统 | 12次/年 | 《网络安全预警通告》 |
| 12 | 蜜罐服务 | 通过业务仿真构建蜜网，诱惑攻击行为进入蜜网，实现攻击捕获，延缓攻击者对实际业务网络的攻击，全程记录攻击轨迹和行为，实现攻击行为的快速取证溯源，保护真实网络资产，同时以技术手段实现对攻击者的追踪。欺骗防御系统打破了现有攻防不对称的局面，结合其他安全系统共同构成安全防御体系。 | 贵州省机关事务管理局门户网站、贵州省机关事务云 | 2系统/次 | 设备部署相关过程文档 |
| 13 | 网站云防护 | 对门户网站、机关事务云、贵州省公共机构节能网做7\*24小时业务系统流量清洗。包含DDOS防护能力、云WAF服务、WEB SHELL防护、云DNS服务、网站加速服务、端口隐藏服务、地域访问控制、邮件通知、防护报告。 | 贵州省机关事务管理局门户网站、贵州省机关事务云、贵州省公共机构节能网 | 3系统/次 | 设备部署相关过程文档 |

**四、商务要求**

（一）服务期及服务地点

**服务期：自合同签订之日起一年；**

**服务地点：采购人指定地点。**

（二）验收标准、规范及验收方式

**1.符合行业标准、国家相关标准，并符合采购文件及合同的相关要求；**

**2.服务结束后，由成交供应商提交验收申请，并提供包括但不限于以下：《漏洞扫描报告》《终端安全加固报告》《渗透测试报告》等相关验收资料，具体按照省级主管部门相关要求提供验收资料。**

（三）付款方式

**合同签订后，采购人收到供应商提交的增值税普通发票后【30】个工作日内向成交供应商支付合同金额的70%。项目完成后，经采购人验收合格支付剩余的合同金额，具体细则以合同约定为准。**

（四）投标有效期

90日历天（从投标截止之日算起）在此期限内，所有响应文件均保持有效。

（五）售后服务

网络安全服务完成后，满足条件组织项目验收。

成交供应商应做好平台运维保障工作，提供7×24小时响应服务。对于系统服务中断，需在2个小时内确定故障原因并解决。

项目开展后，成交供应商必须保证项目正常执行，不得以任何理由中止实施，如发生，由此产生的法律责任和全部损失由成交供应商承担。

（六）投标报价说明

投标报价为验收合格并交付使用价。供应商投标报价中应包含但不限于本项目服务内容费用及所需服务人员的所有费用、系统运维费、办公费用、培训费、加班费、通讯服务费、验收费、公司管理费及利润、增值税及各项税费等完成本项目所需的一切费用，采购人不再另行支付费用。

（七）现场踏勘

投标供应商自行踏勘。承担踏勘现场的责任、风险和费用。

（八）服务承诺

1.投标供应商须书面承诺（承诺函格式自拟，并加盖投标供应商公章）：

（1）与参与本项目的其他投标供应商不存在单位负责人为同一人或者存在直接控股、管理关系；

（2）项目服务团队人员若有岗位变化，须提前3个工作日以书面形式报采购人，并经采购人同意后，才能替换为同等条件或优于的人员；

（3）本项目中定制化开发的产品、知识产权等归采购人所有（含软著），采购人在使用该成果或其任何一部分时不受第三方提出知识产权的指控。如果任何第三方提出侵权指控，供应商须与第三方交涉并承担可能发生的一切法律责任和费用；

（4）若中标后，在项目执行过程中所收集的数据及所有程序软件等文件的知识产权归采购人所有，未经供应商允许不得泄露或用于其他项目及商业经营，供应商对数据及文件负有保密责任，在签订合同时需与采购人签订相应的保密协议。

（5）不会将本项目以任何形式分包、转包出去。

（九）其他要求

1.投标人应对其提供的投标文件及相关资料的真实性负责，在签订合同之前或合同履行期间，如发现供应商在招投标过程中有任何弄虚作假或违法违规行为的，一经查实，采购人予以取消其投标资格或中标/成交资格，且保留将此行为上报上级监督管理部门的权利，给采购人造成的损失，中标人/成交人应当予以承担赔偿责任。

2.违法转包、违规分包的处罚条款:《政府采购法实施条例》第七十二条明确，不得将政府采购合同转包。《政府购买服务管理办法》（财政部令第102号）第二十六条也明确，不得将服务项目转包给其他主体。违法转包的企业将受到处罚，如列入不良行为记录名单，在一定时间内禁止参加政府采购活动，没收违法所得等。

3.其他未尽事宜，待签订合同时双方再议。

