

2、投标报价明细表

项目编号： SDGP371500000202402000745

单位：元

序号	服务名称	具体内容	单位	数量	单价 (元)	合价 (元)
1	网络安全体系建设	梳理采购人网络安全现状，分析查找网络安全薄弱环节，明确网络安全体系建设思路和主体内容，找准网络安全保障工作着力点和突破口，研究总结网络安全工作要点，厘清各方的安全保密责任，适应密码法、等保2.0等新要求，构建全方位的网络安全架构体系。	年	1	50000.00	50000.00
2	信息安全咨询	提供信息安全相关的咨询服务，如上线系统安全要求、安全政策解读、安全标准理解、安全事件处置、应急体系建设等。在对采购人网络安全建设现状进行调研分析的基础上，结合实际，明确任务目标、时间安排和保障措施，制定可执行可落地的任务分工落实表及定期检查要求，并开展宣贯推广活动，全面增强全机关干部网络安全责任意识，推动政策落地增效。	年	1	20000.00	20000.00
3	主机安全检查服务	安全服务商应采用专业的基线配置核查工具及安全配置规范对操作系统、网络设备、中间件、数据库的配置开展基线核查工作，并根据配置核查结果输出详尽的基线描述和修补方案，协助采购人满足等级保护、内控审计等规范要求 and 检查。	年	1	15000.00	15000.00
4	网络安全巡检服务	服务内容:协助完成机房环境及服务器、存储等外设的使用情况的检查，检查主机操作系统及应用软件运行状况，检查安全产品及配套软件运行状况，检查日志服务器运行情况，更新事件库、漏洞库、病毒库等，并对各项配置加以优化，做好日常巡检记录，编写或填报安全巡检报告、月度安全情况通报等。检查安全策略是否有效，配置是否安全，是否	年	1	10000.00	10000.00

		存在安全隐患和可疑事件,系统、设备运行是否正常。定期升级安全设备、系统的软件版本或策略库版本。				
5	漏洞扫描服务	要求使用漏洞扫描工具对信息系统涉及的网络设备、操作系统、应用系统及数据库等进行漏洞扫描,以测试系统在网络访问控制、网络入侵检测、网络设备防护、主机弱口令、主机身份绕过鉴别、应用弱口令及身份鉴别绕过、应用访问控制、应用软件容错等方面存在的安全问题。在得到扫描结果后,需进行数据清洗及分析,汇总形成脆弱性安全检测分析报告,输出详尽的漏洞描述和修复方案。	年	1	25000.00	25000.00
6	渗透测试服务	对目标网站的渗透测试,除使用产品和工具扫描外,更重要的需要进行人工渗透,渗透内容包括但不限于以下项:配置管理、身份鉴别、认证授权、会话管理、输入验证、错误处理和业务逻辑。需要对发现的漏洞进行验证,在修复后进行复测。	年	1	30000.00	30000.00
7	风险评估	安全服务投标人为招标人主要提供包括脆弱性风险评估服务、病毒等恶意程序风险评估服务、遭受网络攻击风险评估服务、内部非法外联风险评估服务等。	年	1	80000.00	80000.00
8	应急响应	在采购人发生信息窃取、黑客攻击、恶意入侵、病毒感染、流量异常、拒绝服务攻击以及其他不能提供正常业务的安全事件时,第一时间到达客户现场,展开对此安全事件的应急响应处理工作,在最快的事件内恢复客户业务系统的正常运行,协助客户溯源并提交相关材料。	年	1	10000.00	10000.00
9	网络安全检查	根据专项检查要求,对采购人及下属基层院的网络安全责任制落实情况、网络安全技术防范措施情况、网络安全日常管理和网络安全应急工作情况等内容进行预检查,并给出预检查报告。报告内容包含被检查对象信息、安全风险与问题以及整改建议等内容。	年	1	20000.00	20000.00
10	攻防演练	邀请不少于4支国内顶尖攻击队伍,每队伍不少于3人,开展为期	年	1	100000.00	100000.00

		不少于3天的攻防演练活动,对业务信息系统的各项资产进行漏洞发现、扫描及形成安全应急预案,在演练结束后,针对攻防演练中发现的业务信息系统中存在的漏洞与缺陷,组织对网络攻防演练进行全面总结,公布问题、分析原因、形成预案、加强整改等。须提供攻防演练平台详细功能截图。				
11	应急演练	演练场景不少于1个,培训人数不少于30人,场地内人均面积不少于2平米;安全服务商应标方案中须根据市人民法院业务实际情况,提供不少于2个演练场景设计,具体演练场景须中标方与招标人协商确定。投标人需编写应急预案和演练脚本;组织开展应急演练活动,提供完整方案,包括但不限于时间、地点、人员、流程等;组织应急演练培训,加强人员防范意识,形成视频教育推广材料。投标人应在投标文件中提供详细的应急演练脚本和实施方案。	年	1	30000.00	30000.00
12	重保服务	在重要活动、节假日或国家、省市级攻防演习期间,需提供安全服务工程师前往市人民法院现场开展实时监测工作,响应防守任务和安全事件的处置,防守期间需借助安全防护设备和安全检测工具对应用系统的数据流量以及敏感行为进行监测分析,研判处置、成果上报、工作汇报等工作,从而保障信息系统的安全性,强化防守效果。	年	1	10000.00	10000.00
13	网络安全培训	邀请不少于2名国内知名网络安全专家讲解网络安全形势,每次培训不少于1天,分享网络安全事件,通过对日常工作和生活中的实际案例展开剖析,向参与培训的人员介绍网络安全的重要性,从而提升全员对于网络安全的理解,强化个人安全防范意识,使全体员工充分了解既定的安全策略,并能够配合切实执行。	年	1	25000.00	25000.00
14	安全加固	通过针对IT环境的网络架构、网络设备、安全设备、主机系统和数据库系统等前期风险评估、漏洞扫描、安全巡检、日常监测等来源的安全问题,提出安全加固	年	1	13000.00	13000.00

		整改或者网络安全优化方案，并结合实际安全需求对安全漏洞实施加固测试和加固整改工作，以实现IT资源的安全性。				
总 价		438000.00元				

注：格式仅供参考，可自行调整。

本表中未列明的但在实际服务过程中必须的服务内容及费用由投标人承担。

投标人名称（公章）： 山东正中信息技术股份有限公司

法定代表人（负责人）或授权代表签字或盖章： _____

日期： 2024 年 12 月 31 日