陕西省政务大数据服务中心2025年度陕西省数字政府网络安全管理运营服务项目中标（成交）明细

汇成项目管理有限公司受陕西省政务大数据服务中心委托，采用公开招标进行采购2025年度陕西省数字政府网络安全管理运营服务项目（项目编码：HCXM-GK-2511-01）项目，中标（成交）供应商名称及中标（成交）结果如下：

一、合同包1（信息技术咨询服务（网络安全管理监督服务））

1.1、中标（成交）供应商：陕西省信息化工程研究院

1.2、中标（成交）总价： 1,158,000.00 元

1.3、中标（成交）标的明细：

服务类

品目号	品目名称	服务名称	服务范围	服务要求	服务期限	服务标准	单价（元）	数量	单位	总价（元）
1-1	信息技术管理咨询服务	信息技术咨询服务（网络安全管理监督服务）	包含网络安全管理监督咨询服务、网络安全管理评价规范服务、网络安全管理运营服务供应链管理服务、网络安全管理技术运营合规审计服务、地市政务云网安全摸查分析服务、安全管理推广服务、应急预案服务、应急演练服务等	完全响应招标文件中的服务要求	自合同签订后，符合服务条件之日起8个月	完全响应招标文件中的服务标准	1,158,000.00	1.00	项	1,158,000.00

二、合同包2（网络安全管理技术运营服务(工具支撑及基础运营服务)）

1.1、中标（成交）供应商：杭州安恒信息技术股份有限公司

1.2、中标（成交）总价： 10,026,000.00 元

1.3、中标（成交）标的明细：

服务类

品目号	品目名称	服务名称	服务范围	服务要求	服务期限	服务标准	单价（元）	数量	单位	总价（元）
2-1	平台运营服务	网络安全管理技术运营服务（工具支撑及基础运营服务）	满足采购人要求的30项服务的对应服务范围	满足采购人要求的30项服务对应的服务内容及服务要求	自合同签订后，符合服务条件之日起8个月（第1、2、3、4、26、27、28项服务自符合服务条件之日起3个月），满足采购人要求的30项服务对应的服务时间要求	满足采购人要求的30项服务对应的服务标准要求，满足国家相关合规要求	10,026,000.00	1.00	项	10,026,000.00

三、合同包3（终端行为分析服务）

1.1、中标（成交）供应商：西安安迈信科科技有限公司

1.2、中标（成交）总价： 410,000.00 元

1.3、中标（成交）标的明细：

服务类

品目号	品目名称	服务名称	服务范围	服务要求	服务期限	服务标准	单价（元）	数量	单位	总价（元）

品目号	品目名称	服务名称	服务范围	服务要求	服务期限	服务标准	单价（元）	数量	单位	总价（元）
3-1	技术测试和分析服务	终端行为分析服务	终端行为分析服务、终端合规监控服务	开展以下服务项前必须提交详细的各项服务的实施方案，经采购人审核批准后方可开展服务，且服务全程须接受采购人与信息技术咨询服务（网络安全管理监督服务）方的监管，遵从各项技术规范要求；服务产生的各项交付物须经信息技术咨询服务（网络安全管理监督服务）方审核后方可提交采购人进行审核。 1、终端行为分析服务 提供终端行为分析服务，针对省数据和政务服务局、省数据和政务服务中心、政务云网、公共支撑等运维终端在日常工作中的安全行为进行监控分析，确保不发生安全行为事件。服务期内提供≥500点行为分析服务。按月交付分析报告。 提供1套终端行为分析服务工具，兼容国产化办公环境，兼容信创云部署环境，可支持与网络安全协调指挥平台对接，并提供包括终端准入管理、基线安全、威胁情报检测、黑客入侵分析等能力，对终端安全行为分析风险及时通报并处置，避免对政务云网运行造成安全风险威胁，完成风险问题的跟进闭环。 工具支持能力如下： 终端资产管理：可针对业务终端进行安全管理，包括但不限于终端资产环境信息采集、进程管理、性能监控、账号管理、应用管理等；可查看和管理所有终端的漏洞情况，并进行漏洞结果查看和导出；基线安全：提供对终端操作系统、数据库、中间件等基线安全检查，并提供安全建议；终端防病毒：支持常见类型的病毒实时防护、定时查杀。风险自评估：可评估终端安全风险，包括但不限于弱口令、高危漏洞、风险进程、高危端口、风险账户等；黑客入侵防护：可针对黑客常见的等入侵行为进行检测、告警和阻断；主机访问控制：可针对终端访问提供细粒度的访问控制，可基于黑白名单或IP地址、端口、协议、流量方向等控制因子进行访问控制；威胁情报检测：可对访问IP、域名、可疑文件等进行威胁情报匹配检测；数据防泄漏：可识别常见敏感内容，支持OCR识别，支持红头文件、印章识别，可管控即时通讯、拷贝、网盘、剪贴板、邮件、FTP等渠道，提供敏感行为阻断、审批、审计等，可备份敏感文件备查，支持对敏感数据的分级管控，可自定义终端水印，对拍照、打印等。 2、终端合规监控服务 提供终端合规监控服务，提供终端合规监控服务，针对省数据和政务服务局、省数据和政务服务中心的管理终端提供安全保密合规监控服务，进行终端涉密信息监测，接收网络攻击窃密和涉密信息检测告警事件，并上报相关监测数据，对窃密事件告警进行核实，掌握自身安全保密风险。服务期内为省数据和政务服务局提供≥50个点，为省数据和政务服务中心提供≥150个点的合规监控服务。一次性交付终端保密自监管系统工具，提供季度合规监控服务报告。 提供1套保密安全自监管服务工具，含互联网自监管平台、客户端、监测引擎等，考虑保密工作的特殊性，由于系统特殊性，需按照一次性服务工具方式交付，支持为局、中心独立划分管理组织，局、中心可分别管理各自的保密终端和掌握各自的终端保密自查情况。 工具支持能力如下：网络出口安全保密检测能力：支持在互联网出口部署互联网出口保密检测硬件工具，实现传输涉密检测、攻击涉密检测、指定对象审计、网络行为审计等；传输涉密检测：支持对网页、电子邮件、即时通讯、社交网络、HTTP、FTP、SMB协议等在线传输行为检测，检测其中涉及的敏感词，实现精准告警；攻击涉密检测：支持识别网络窃密木马、远程木马、僵尸网络、网络蠕虫、间谍程序、黑客后门、渗透行为、恶意程序/文档攻击等基于网络的攻击窃密行为，并进行告警；指定对象审计：支持对IP、域名、URL、用户邮件账号等指定对象的审计，可针对性审计对应对象会话；网络行为审计：支持对会话访问情况、网络Web访问、邮件传输、DNS域名请求、及时消息、文件传输等网络行为的全量审计；终端保密检测能力：支持终端保密检测组件，兼容国产化终端环境部署，支持托盘图标展示，可支持一键自查、敏感文件告警、终端异常行为告警等能力；一键自查：支持对涉密敏感信息的一键自查能力，可基于文件、文件操作记录、上网记录、移动介质、终端详情等维度进行自查，并输出详细的自查结果报告；敏感文件告警：支持对敏感涉密文件、疑似文件、非密文件的列表管理，可监控疑似、涉密文件的重命名、删除、复制、剪切等操作，并进行告警，支持对文本、图片、网页、音视频、压缩包等常见格式文件进行抓取，支持图片OCR识别、支	合同签订后，合同服务自符合条件之日起8个月	以招标文件和最终签订合同为准	410,000.00	1.00	项	410,000.00

品目号	品目名称	服务名称	服务范围	服务要求	服务期限	服务标准	单价（元）	数量	单位	总价（元）
				持音视频内容检测；终端异常行为告警：支持对终端的出网流量进行审计，对涉及涉密文件、疑似文件外流的进行告警，支持基于预设行为策略对终端、人员、应用、数据、账号等维度进行数据统计和数据挖掘，基于预设行为基线实现用户异常行为研判告警。						

四、合同包4 （网络和数据安全风险评估服务）

1.1、中标（成交）供应商：奇安信网神信息技术（北京）股份有限公司

1.2、中标（成交）总价： 590,000.00 元

1.3、中标（成交）标的明细：

服务类

品目号	品目名称	服务名称	服务范围	服务要求	服务期限	服务标准	单价（元）	数量	单位	总价（元）
4-1	测试评估认证服务	网络和数据安全风险评估服务	网络安全风险评估：服务期内交付符合要求的风险评估报告不少于20份； 数据安全风险评估：服务期内交付内容包括《数据安全风险评估总体方案》、8份符合要求的单系统《风险评估报告》及相关过程资料，确保评估工作过程规范、结果可溯。 完全满足招标文件服务要求范围	网络安全风险评估：完成采购人管理的核心系统及上云重要应用系统从资产威胁、弱点、影响、衍生风险多个维度评估，从安全技术和管理方面，按照国标完成风险评估，输出评估报告（含方案、报告、过程资料），并在协调指挥与防控运营平台在线流转，对风险修复结果进行二次验证。服务期内评估系统20个，经审批后开展服务，服务期内每系统评估≥1次，交付评估报告≥20份。 数据安全风险评估：完成采购人指定或按需申请系统的数据安全风险评估服务，服务期内评估系统≥8个，经审批后开展服务。从技术和管理两方面开展评估，调研安全脆弱性、识别风险点、量化系统风险隐患、提出控制措施、输出评估报告；报告通过协调指挥与防控运营平台进行流转，形成风险告警和处置闭环管理，对处置后风险完成二次验证，服务期内指定的每系统完成至少1次。交付不限于评估方案、报告、过程资料文档。服务期内评估系统8个，经审批后开展服务，服务期内每系统评估≥1次，交付评估报告≥8份。 足招标文件服务要求	我司提供网络和数据安全风险评估服务满足招标文件中交付要求服务期限：服务期限为自合同签订后，符合服务条件之日起8个月。	符合国家和政府行业标准服务要求	590,000.00	1.00	项	590,000.00

五、合同包5 （网络安全测试服务）

1.1、中标（成交）供应商：陕西省网络与信息安全测评中心

1.2、中标（成交）总价： 1,499,940.00 元

1.3、中标（成交）标的明细：

服务类

品目号	品目名称	服务名称	服务范围	服务要求	服务期限	服务标准	单价（元）	数量	单位	总价（元）

品目号	品目名称	服务名称	服务范围	服务要求	服务期限	服务标准	单价（元）	数量	单位	总价（元）
5-1	测试评估认证服务	网络安全测试服务	响应招标文件关于服务范围的一切要求。	开展以下服务项前必须提交详细的各项服务的实施方案，经采购人审核批准后方可开展服务，且服务全程须接受采购人与信息技术咨询服务（网络安全管理监督服务）方的监管，遵从各项技术规范要求；服务产生的各项交付物须经信息技术咨询服务（网络安全管理监督服务）方审核后方可提交采购人进行审核。在服务期间采购人根据实际情况产生的相关合理需求，供应商应及时响应，不增加额外服务费用。 1、渗透测试服务 完成采购人管理的自有系统、各上云业务单位系统≥100次系统的人工渗透测试（每系统做一次记数量一次），经采购人审批后开展服务。深度测试、评估、分析业务安全隐患和漏洞可利用程度，输出测试报告并给出处置建议；报告通过协调指挥与防控运营平台在线管理和流转下发，提供风险处置的二次验证；对暂时无法处置风险需给出风险控制建议和指导，并加强后期监控；测试范围不限于业务相关的移动APP、Web站点、小程序、CS客户端等，测试类型不限于信息收集类、配置管理类、认证类、会话类、授权类、数据验证类、系统应用漏洞等；服务期内按需申请测试，交付整体实施方案、单系统测试报告，报告提交时间测试完成后一周内。供应商对渗透测试的结果承担责任，渗透测试过的系统在随后的攻防演练中被攻破（“0day”漏洞除外），或被安全主（监）管部门通报，且漏洞发布时间早于测试完成时间的，按照违约条款处置。 2、源代码安全审计服务 完成采购人指定或按需申请系统的源代码安全审计服务，服务期内评估系统≥20个。提供专业的代码审计工具和代码组件成分评估工具，采用工具扫描和人工分析确认相结合的方式，对被测系统的开发语言、框架、代码漏洞、逻辑结构缺陷、代码缺陷、开源软件代码、组件等进行分析，审计内容包括但不限于输入验证、身份鉴别、授权管理、安全加密、错误处理、日志记录、逻辑结构分析等方面，开源组件识别内容包括但不限于软件成本名称、版本、已知漏洞等级、许可协议、漏洞利用难度等，并对软件依赖关系进行分析。发现源代码存在的安全漏洞和软件组件成分存在的已知安全漏洞，对软件组件漏洞及代码质量问题进行重点检查，兼容CNVD、CNNVD、Github等漏洞情报信息，覆盖常见的组件漏洞类型，对开源软件许可证进行分析，关联分析许可协议风险和许可依赖，出具整体实施方案、源代码审计报告和代码组件成分评估报告，并通过网络安全协调指挥及防控运营平台下发，提供修复建议协助开发人员修复安全问题，在业务方修复安全风险问题后，完成复测验证，确保安全风险问题完全修复。对因客观原因暂时无法修复的问题，给出安全建议，协助进行风险规避或降低，并记录。投标需提交使用工具的功能证明材料，不限产品截图、官网说明、第三方证明材料等。所采用的源代码安全审计和软件组件成分评估工具需为非开源的商用工具，在服务前需提供服务方采购或租用相关工具的证明材料。响应招标文件关于服务要求的一切要求。	自合同签订后，符合服务条件之日起8个月。	响应招标文件关于服务标准的一切要求。	1,499,940.00	1.00	项	1,499,940.00

汇成项目管理有限公司

2026年01月08日