开标一览表（服务类）

项目名称： 贵州省农业农村厅2025年网络安全项目　　项目编号： P52000020250005FN　　品目号：/

品目号	服务名称	服务标准	服务时间	单价（元）	合计金额（元）
/	贵州省农业农村厅2025年网络安全项目	验收方式和验收标准按照本项目实施方案、实施方案评审报告、采购文件、响应文件及《信息技术服务质量评价指标体系》（GB/T33850-2017），以及《贵州省省级政务信息系统建设管理办法》（黔府办函〔2023〕2号）的规定执行； 2.验收合格后由甲方出具验收报告。若验收不合格，则所有责任及复检相关费用由中标人承担； **3.验收时间：**服务期结束后，由中标供应商书面提交验收申请，采购人组织相关单位或人员验收。	合同签订后12个月。	1，978，000	1，978，000
…					
服务时间：合同签订后12个月。					
投标总价：人民币大写： 壹佰玖拾柒万捌仟元整　　元（人民币小写：1，978，000元）					
投标申明：无					
其他：无					

备注备注:1.本表所填单价均应包括其它所有费用，投标人须填写合计金额；

2.《中小企业声明函》格式详见附表，中小企业声明函中内容与开标一览表不一致时，以开标一览表内容为准。

3.投标人不能以价格折扣、价格优惠等方式对开标一览表的投标报价进行修改或调整。

投标供应商名称（盖章）：贵州省邮电规划设计院有限公司

日　期：2025 年 07 月 08 日

报价明细表（服务类）

项目名称：贵州省农业农村厅2025年网络安全项目　　项目编号：P520000202500005FN　　单位：元

序号	服务内容	服务明细	单项价格
1	漏洞扫描	使用系统漏洞扫描工具对数据库、操作系统、中间件等进行漏洞、端口、弱口令扫描，通过文件扫描、 后门程序扫描、网络设备与防火墙漏洞扫描、域名扫 描、Web站点扫描、主机扫描、数据库扫描、CGI问题检测等，查找网络设备、服务器主机、数据和用户账号/口令等安全对象目标存在的安全风险、漏洞和 威胁，检查当前网络中是否存在高风险漏洞,确保安 全风险漏洞及时发现，并根据扫描报告给出漏洞整改 或修复建议。 服务备注：按月针对省厅本地以及云端10个业务系统（包含网络设备和安全设备等）开展漏洞扫描， 共12次； 人工安全服务，不提供单独设备，提供12份《漏洞扫描报告》	12000
2	基线核查	参照等级保护的安全基线标准，对省级政务外网 监测平台业务子系统主要从三个方面：安全漏洞、安 全配置、重要状态等，开展操作系统基线、数据库基 线、中间件基线、网络设备基线、安全设备基线检查，出具基线检查报告并提出整改建议。 服务备注：针对平台每月完成1次服务，共计 12次，共出具12份报告； 人工安全服务，不提供单独设备，提供12份《基线核查报告》	12000
3	安全巡检服务	对现有的安全设备开展巡检，检查并记录系统平 台各安全组件（包括防火墙、日志审计、堡垒机、数据库审计等）的运行情况；从硬件运行状态、设备的 配置与策略、访问控制、日志记录与分析、权限管理、规则更新与补丁管理、固件与软件版本、日志管理等 多个维度对目标的运行状态进行分析，得出一段时间 内目标系统及相关设备的安全运行状态。 服务备注：每季度一次，共计4次。 人工安全服务，不提供单独设备，提供4份《安全巡检报告》	20000
4	应急演练服务	通过开展应急演练，提高应对突发事故的组织指 挥、快速响应及处置能力，最大限度地减少网络与信 息安全突发公共事件的危害和影响，提高各部门密切 协同，形成共同维护网络安全的强大合力，严密防范 网络安全风险隐患。要求对目标系统、人员、软硬件 设备、基础架构，进行多维度、多手段、对抗性模拟 攻击，进行演练，旨在发现可能被入侵的薄弱点，并 以此为跳板将攻击渗透结果最大化，进而检验现有防 御体系的短板。 服务备注：一年2次，根据实际业务情况按照省 级范围开展。应急演练针对单位整体安全状态，不针 对单个系统，单次演练根据单位情况选择下列其中一 种演练模式：恶意程序事件、网络攻击事件、数据安 全事件、信息内容安全事件、设备设施故障事件、违规操作事件、安全隐患事件、异常行为事件、不可抗 力事件和其他事件	50000

		人工安全服务，不提供单独设备，提供《应急演 练方案》、《应急演练总结报告》、《专项应急预案修订 版》	
5	安全意识培训	每半年一次针对农业农村厅工作办公人员提供 安全意识培训，通过讲解法律法规、日常工作及生活中基本安全知识以提升全体人员网络安全意识、基础 安全技能和应急响应能力。培训内容包括但不局限于 相关法律法规、日常办公安全意识、应急知识等。 服务备注：一年2次 单位整体安全培训，拍照、视频等	10000
6	渗透测试	针对省厅本地以及云端10个业务系统进行模拟 黑客攻击渗透测试，发现系统存在的安全漏洞。根据已经发现的安全漏洞，模拟黑客的攻击方法对系统和 网络进行非破坏性质的攻击性测试，深层次发现各类 系统、应用存在的安全问题。 服务备注：每半年针对平台进行渗透测试，共2次，共出具2份报告 人工安全服务，不提供单独设备，提供2份《渗透测试报告》	80000
7	日志审计分析核查	对于网络和系统等安全日志进行统一接入管理，对防火墙等安全设备产生的安全日志进行收集，综合 对这些日志进行关联分析，提高日志的安全可用，使 得安全日志变可读，为安全溯源和管理提供一定基础，提出安全告警事件解决方案，并对安全日志分析 反映出的技术和管理两方面的脆弱性进行深入分析， 提出合理有效的安全风险控制解决办法。 服务备注：持续一年 人工安全服务，不提供单独设备，全年内按需提供《日志审计报告》	60000
8	安全运营服务	通过对势感知平台、本地政务外网防火墙和终端安全检测平台等安全设备开展日常安全运营服务，提 供7*8小时全天候专家威胁监测服及处置服务，提供 7*24小时全时段的日志分析服务，确保安全威胁被 实时发现并迅速处置，最大限度减少潜在损害和业务中断。 提供7*24小时安全事件应急响应服务，专业安全人员1小时内到达本单位现场提供专业的安全事 件分析、协助本单位处置事件直至完全闭环，补充本地人员能力不足现状。 在业务关键期、重要活动、重大会议，如国庆，两会，春节期前完成事前安全巡检、事中值守保障、 事后总结汇报的工作，实时监控汇报网络状态，必要 时提供现场支撑。 服务备注：持续一年 安全运营服务，不提供单独设备，提供《首次安 全威胁分析报告》、《资产信息确认表》、《漏洞举证报 告》、《威胁处置报告》、《威胁狩猎报告》、《事件处置 报告》、《节假日值守快报》、《安全运营周报》、《安全 运营月报》、《安全运营半年度报告》、《安全运营年度 报告》	200000
9	敏感数据监测服务	通过对数百个威胁情报源的监控，结合大数据和 AI算法，从暗网情报、代码泄露、敏感文件、黑产舆情、资产失陷五个维度，帮助本单位排查互联网上 是否存在敏感数据	15000

		泄露问题，降低数据泄露带来的业 务影响和品牌保护影响，减少监管单位通报压力，弥补在外部信息监控上的安全能力短板 服务备注：一次 交付物：人工安全服务，不提供单独设备，提供1份《敏感数据检测报告》	
10	网站数据监测服务	为网站提供持续网站监测服务，包括对网页篡 改、敏感词、网站挂码/黑链进行实时监测，持续监 控网站业务的可用性，帮助实时掌控网站的安全态势。 服务备注：每季度一次，共计4次	150000
11	态势感知安全检测与响应模块体系服务	依托于态势感知等服务工具，采取服务交付模式，本次预算服务时间为一年，全面赋能贵州省农业 农村厅网络安全态势感知，实现：在单位本地建立一 套主动威胁的检测和响应体系，以实现精准、全面、快速的发现现代网络中的新型APT攻击、潜伏威胁等 各种高级威胁，大幅降低本单位的威胁检测、响应、 处置难度，尽可能减少攻击事件对本单位造成的损失，进一步提高本单位网络对突发安全事件检测和响 应能力。通过该体系建设，统一本地网络安全数据， 解决现有网络安全的如下问题： 1、单位现有网络安全建设以被动响应的防御体系建设为主，缺乏主动的威胁检测和响应能力，无法应对当前安全攻防形式及监管要求。 2、现有安全建设碎片化，海量检测数据相互割裂，无法发现潜伏的真正威胁事件，且海量的告警极易带 来威胁的漏报和告警处置疲劳。 3、现有的安全响应复杂，威胁溯源和处置链条长，无法实现流程化处置和快速响应。 建设后实现如下能力： 1、解决本单位原有网络安全数据信息孤岛问题， 通过自动化多源数据取证分析实现威胁研判。 2、通过多源数据分析技术，能够有效降低风险检 测误报率。 3、通过服务工具自动检测结合网络安全专家研判，可以实现多数时间自动运行，减少本单位接入处置次 数。 4、通过统一的主动威胁的检测和响应体系建设， 结合较为精准的检测效果以及网络安全专家服务，降低本单位整体网络安全的建设成本、维护成本和使用成本。 针对厅本级未上云系统： 1、农机购置补贴产品自主投档平台(虚拟化平台部署，共6台虚机，单台16核64G,日常运行业务流量 500M) 2、贵州省农产品质量安全电子监控系统网络信息技术服务与应用系统(2台服务器，单台8核32G,日常 运行业务流量100M) 3、贵州省农机安全监理信息管理系统(4台服务器， 单台8核32G,日常运行业务流量200M)贵州省兽药安全信息化监管系统(6台服务器，单台16核32G日常 运行业务流量600M) 4、贵州省动物及动物产品电子出证信息化管理系 统(6台服务器，单台16核32G日常	707000

		运行业务流量 600M) 业务流量总和：约2000M 服务器资产总和(服务器及虚拟机IP数量):35个（上述5个系统共25个，厅级其他业务支撑资产数量 10个) 厅本级PC终端数量：1500台 服务要求：持续一年 交付物：以服务形式交付，服务相关工具自备（包 括但不限于本地已有的相关网络安全设备），建立一套主动威胁的检测和响应体系，体系功能项包括： 1、资产管理功能：解决单位以往资产分散、不集 中等一系列管理问题，具有识别IT资产、梳理访问 关系和建立责任人员组织架构的功能。 2、攻击面管理功能，实现单位系统漏洞、脆弱性的全生命周期管理。 3、一手网络安全数据检测功能，原态势感知平台 联动其他安全组件，均为收集经过安全组件处理的流 量和端点二手数据，本次增加聚合分析流量和端点一手数据的能力，提供问题溯源的攻击故事线能力，切实解决本单位目前告警数量多，溯源困难的问题； 4、威胁情报能力，（1）、提供丰富的云端威胁情报能力；（2）、提供内生情报管理，包括恶意IP地址、 恶意URL、恶意样本、恶意域名、垃圾邮件等自定义 威胁情报，网络安全专家7*24小时响应，为本单位 安全运营降低人力成本和门槛； 5、增加响应处置的剧本能力，能够提前编排安全 事件处理流程和步骤，重点应用于重保时期，能够联 动相关组件，具备自动化响应与处置能力； 6、实现单位网络安全产品的统一管理与统一调度， 能够与第三方日志、第三方应用的对接，收集网络流量数据、主机终端数据、安全设备告警数据、情报数据；	
		态势感知安全检测与响应体系网络侧遥测源，需要采集的网络流量检测设备的流量(2000M)	
		态势感知安全检测与响应体系业务侧遥测源，需要采集的业务行为数据的服务器数量(35个)	
		态势感知安全检测与响应体系端点侧遥测源，需要采集的端点行为数据的PC终端数量(1500个)	

		态势感知安全检测与响应体系基础平台服务(平台性能要求：至少2颗CPU、至少256G内存、至少40T存储空间):可容纳180天安全告警、事件、漏洞、资产、配置类数据的存储，30天网络安全日志存储，包含一年服务平台升级费用、特征库升级费用、检测引擎升级费用， 安全事件深度挖掘服务：海量灰度规则+多引擎分析：基于云端数据湖，对海量线索和数据进行灰度规则和私有引擎二次分析，网络安全专家研判后生成 报告； 网络安全专家事件研判服务：针对态势感知安全 检测与响应体系产生的安全事件，网络安全专家介入做研判，进一步保障事件检出的准确性； 隐藏威胁检测服务：基于网络安全专家的经验固化成检测模型，对于未知不确信的告警进行深度调查关联，自动化生成安全事件并推送； 高级漏洞管理功能：漏洞分层筛选基于漏洞、弱 口令的可利用情况、漏洞危害、攻击者利用频次、是否涉及关键业务级暴露资产等要素做分层筛选。网络 安全专家实时跟进分析热点漏洞、紧急漏洞、热点攻 击，形成产品的热点威胁检测能力并给出处置建议， 以此来评估热点威胁的影响情况以及辅助处置加固。 漏洞缓解修复建议针对重点高可利用漏洞，提供详细 可落地的处置指导。存在缓解措施的，关联防火墙、 EDR等产品的协同缓解措施，如防火墙规则、EDR补 丁修复等。	
12	攻防演练服务	以攻防演练平台为基础，通过组织攻防两端针对 业务系统（（针对厅本级未上云系统：农机购置补贴 产品自主投档平台、贵州省农产品质量安全电子监控 系统网络信息技术服务与应用系统、贵州省农机安全 监理信息管理系统、贵州省兽药安全信息化监管系统、贵州省动物及动物产品电子出证信息化管理系 统）、主机、网络设备、内网环境安全以及数据等采取必要的攻击行为，以提权、控制业务、获取数据为目的，检验参演单位的人机结合、协同处置等网络安 全方面的综合防护能力。 攻防演练活动组织筹备和保障：在攻防演练活动前 期，根据本单位需求，设计攻防演练活动整体方案， 安排工作组负责活动筹备，保障攻防演练活动顺利进 行，同时在活动结束后向用户做总结汇报； 厅本级及下级参赛队员培训：在攻防演练活动前 期，根据本单位需求，培训下级单位参赛人员，分两个班级培训，每个班级五个工作日培训时长； 攻防演练活动裁判：在攻防演练活动现场，裁判 负责裁定攻击队的攻击行为是否有效，评判各攻击队分数，及时发现并终止违规行为等； 专业攻击队：在攻防演练活动前期，根据本单位需求，提供专业攻击队服务，通过专业手段进攻农业农村厅厅本级未上云系统，三人攻击小队，服务时长5天，共15人天； 攻防演练管控平台：提供攻防演练平台，有效对实网演练及安全渗透测试过程中的监管、分析、裁决、复盘等全生命周期活动进行管控，提高实网演练活动 组织效率，保障实网演练中业务和资产的安全，促进 “关基”业务安全性及安全人员能力提升。	300000

13	贵州省农业农村厅网站基础共性服务项	网站平台维护、异常处理、设备巡检、建立客户 信息保密机制、数据备份。	20000
14	贵州省农业农村厅2025年度厅本部中心机房和视频会议系统基础运维技术服务	1、硬件设备维保服务设备清单 （1）多点控制单元MCV8000U 1台深圳市捷视飞通科技股份有限公司2018年购买 （2）录播服务器FRS20001台深圳市捷视飞通科技股份有限公司2018年购买 （3）电视墙服务器TVS28001台深圳市捷视飞通科技股份有限公司2018年购买 （4）高清视频会商终端MCV3000B2台深圳市捷视飞通科技股份有限公司2018年购买 （5）高清摄像头HCM710 4台深圳市捷视飞通科技股份有限公司2018年购买 （6）数字音频处理器TYCHOT1208/TC 1台深圳市东微智能科技股份有限公司2018年购买 提供以上设备的原厂商针对本项目硬件设备延 保服务声明函，并加盖原厂商公章。要求在本项目服 务期内，提供免费维修，不能维修的，免费更换同等 档次的产品。 2、系统软件版本维护 确保软件版本是最新版本的，升级优化前要向采购人进行升级备案，且升级后保障系统正常运用使 用。 3、巡检服务 硬件设备每季度提供一次巡检服务。巡检内容：包含硬件设备通电情况检查、设备运行情况检查、线 缆连接情况检查设备功能检查、故障处理设备报修送修等服务； 4、会议保障 每次视频会议召开前一天，提供1名熟悉系统的 工程师进行系统的调试和所有会场的点名，同时确保 视频会议召开期间，进行现场的保障，确保会议的顺 利召开。当有重大会议召开时，要求安排不低于2名熟悉系统的工程师进行会议的调试和保障。	220000
1	安全巡检	安全巡检服务是指对政府机关、企业、银行、学校等单位运行的信息系统所涉及的机房、网络及 安全设备、主机系统、应用系统等定期进行全面的 专项安全巡检，是预防式的服务，可以提前发现问题，降低安全事故的发生几率。 定期对信息化系统开展安全巡检工作，可以充分掌控企业信息系统的安全现状，提前发现信息化 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。 次数：每季度一次，共计4次。	20000
2	应急演练	应急演练服务是一项针对单位整体安全状态 保障的服务，该项服务形式多样，可根据用户实际 情况进行调整。行业、单位或部门通过采取安全演 练的方式，反思、整改，吸取教训弥补不足，总结 经验推动工作，进一步完善网络信息安全工作方案 及应急预案，提高工作能力。 通过应急演练活动，行业、单位或部门建立健全应用系统和网络运行应急工作机制，验证相关组织、人员对应用系统及网络运行突发事件的组织指 挥能力和应急处置能力，同时验证单位现有应急预 案的可行性，并对应急预案进行及时更新完善，进 一步提高应对突发紧急安全事件的能力。	50000

		次数：一年2次。	
3	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。可及时发现在硬 件、软件、和协议在安全策略上的漏洞和风险并针对性加固、按时进行扫描工作可有效预防安全事件发生。 次数：一年12次。	12000
4	日常维护服务	对“云安全设备租赁”中所列设备提供日常维护，包括检查硬件设备情况、软件运行情况、局域网线路状态等，并记录检查情况，及时处理硬件故 障，保证系统的稳定运行。设备巡检每月一次，对所有安全产品设备进行全面巡检，并制作巡检档 案。巡检内容包括但不限于安全产品设备情况检查、软件运行情况检查、数据线路状况检查、系 统性能和优化建议等。对存在故障隐患的由运维供应商负责调整优化，巡检完毕提供巡检报告，每年度提供年终服务总结报告。	10000
5	渗透测试服务	渗透测试服务：对已经识别的漏洞进行逐条验 证。如是否存在：注入漏洞、失效的身份认证和会 话管理、安全配置错误、流程缺陷、国际已知的高 风险爆发的漏洞手动验证等。从而获得其业务系统 操作权限或提升权限并控制系统。 次数：每半年针对平台进行渗透测试，共2次，共出具2份报告。	10000
6	代码审计服务	由具备丰富的编码经验并对安全编码及应用 安全具有很深刻理解的安全服务人员，根据一定的编码规范和标准，针对应用程序源代码，从结构、脆弱性以及缺陷等方面进行审查，最终输出代码审计报告，完善应用程序，提升自身安全水平。	10000
7	安全加固服务	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。	10000
投标总价大写：壹佰玖拾柒万捌仟元整 小写：1978000			1978000

注：1.供应商须按“报价明细表 ”的格式详细报出投标总价的各个组成部分的报价，否则作无效投标处理。

2.“报价明细表 ”各分项报价合计应当与“开标一览表 ”报价合计相等。

供应商名称（盖章）：贵州省邮电规划设计院有限公司

法定代表人或授权代表（签字）：

投标日期：2025 年 07 月 08 日