SJHXXFW2026057

网络安全服务项目

合

同

书

采购人名称：　　陕西省结核病防治院

供应商名称：　　中移建设有限公司陕西分公司

签约日期：　　2026 年 6 月 10日

扫描全能王
3亿人都在用的扫描App

合同编号：

签订地点：陕西省西安市

签订时间：2026 年 6 月 10 日

采购人（甲方）：陕西省结核病防治院（陕西省第五人民医院）

供应商（乙方）：中移建设有限公司陕西分公司

根据《中华人民共和国政府采购法》及实施条例、《中华人民共和国民法典》和甲方网络安全服务项目（采购项目编号：DQA-2026019-CS）的磋商文件、磋商响应文件等有关规定，为确保甲方采购项目的顺利实施，甲、乙双方在平等自愿原则下签订本合同。

一、合同文件

下列文件是构成本合同不可分割的部分：

（1）合同协议书；

（2）专用条款

（3）成交通知书；

（4）磋商文件；

（5）响应文件；

（6）根据实际情况需要增加的内容。

二、服务内容

1. 乙方应按照合同的规定，提供符合项目招标（采购）文件中要求的服务，具体包括：

序号	服务内容	服务内容概要	服务期限	单价（元）	合计（元）
1	线上安全托管服务	7×24h 安全监测、SLA 保障、漏洞扫描、脆弱性管理、安全告警处置、安全设备对接、日志分析、安全通告、月度/季度运营报告	一年	165000.00	165000.00

扫描全能王
3亿人都在用的扫描App

2	线下安全技术支撑服务	驻场安全工程师、资产梳理、风险评估、漏洞检测、基线核查、渗透测试、弱口令检查、新系统安全评估、应急响应、应急演练、现场安全支撑。	一年	230000.00	230000.00
具体服务内容详见附件一：服务内容。					

三、服务期限

自合同生效之日起 1 年。合同期满后，甲方将对乙方的服务质量进行考核，根据考评结果及满意度决定是否续签合同，总服务期不超过三年（含本年度），年度服务金额不超过本合同价格。

四、服务费用及支付方式

1. 服务费总金额为人民币叁拾玖万伍仟元整（¥395000.00）（含税，税率 6%）。该费用已包含乙方提供服务过程中产生的人工费、零部件费（非人为损坏且在服务范围内）、交通费等所有费用。

2. 支付方式为分期付款，具体安排如下：

第一笔付款：服务期满半年后，乙方提交书面验收申请，甲方验收合格并收到乙方开具的全额增值税发票后 30 个工作日内，支付合同总金额的 50%（¥197500.00）；

第二笔付款：合同期满后，乙方提交书面验收申请及书面服务成果，甲方验收合格后 30 个工作日内，乙方提交付款申请后，支付剩余 50%（¥197500.00）。

3. 甲方付款前，乙方须提供符合甲方要求的发票，否则，甲方有权暂不付款并不承担任何违约责任。

五、成果及验收

1. 服务成果：详见附件一。

2. 验收标准：符合附件一规定、满足甲方要求。

六、违约责任

1. 甲方未按约定支付费用逾期超过 30 日的，每逾期 1 日按逾期金额的 0.5% 支付违约金。合同另有约定除外。

2. 乙方违反本合同约定，未按甲方要求完成服务事项、提交服务成果的，

扫描全能王
3亿人都在用的扫描App

每延迟一日，支付合同金额千分之五的违约金；逾期超过10日的，甲方有权解除合同，并要求乙方支付合同金额10%的违约金。违约金不足以弥补甲方损失的，乙方承担补足责任。

3. 未经甲方同意，乙方不得将任何服务转委托给第三方。否则，甲方有权解除合同，并要求乙方支付合同总价10%的违约金，违约金不足以弥补甲方损失的，乙方承担补足责任。

4. 甲方有权定期检查。若发现乙方提供的技术服务质量不满足合同约定标准，乙方应无条件整改。若乙方检查不合格累计达到3次，或合同期满时验收不合格的，乙方须返还甲方已支付的全部费用，并向甲方支付技术服务报酬的10%作为违约金。若违约金无法弥补甲方损失的，乙方承担补足责任。因乙方故意或过失，导致甲方向第三方承担赔偿责任的，甲方全部损失由乙方承担。

5. 乙方及其工作人员应对技术服务合同签订、履行过程中了解到的涉及到甲方商业秘密的文件资料以及其他尚未公开的有关信息承担保密责任，并采取相应保密措施。乙方违反该条保密义务的，应承担一切法律责任，并向甲方支付相当于合同金额10%的违约金，违约金不足以弥补甲方损失的，乙方承担补足责任。

6. 有任何第三方因本项目知识产权向甲方提起侵权诉讼的，甲方由此受到的损失，由乙方承担全部赔偿责任（包括但不限于实际损失、间接损失、因维权包含的所有费用）。

七、解决合同纠纷的方式

1.在执行本合同中发生的或与本合同有关的争端，双方应通过友好协商解决，经协商在7天内不能达成协议时，则采取以下第（1）种方式解决争议：

（1）向甲方所在地有管辖权的人民法院提起诉讼；

（2）向西安仲裁委员会按其仲裁规则申请仲裁。

八、合同生效及其他

1. 合同经双方法定代表人或授权委托代理人签字并加盖单位公章（合同专用章）后生效。

2. 合同执行中涉及采购资金和采购内容修改或补充的，须经政府采购监管

扫描全能王
3亿人都在用的扫描App

部门审批，并签订书面补充协议报政府采购监督管理部门备案，方可作为主合同不可分割的一部分。

3. 本合同一式陆份，甲方叁份，乙方叁份。

扫描全能王
3亿人都在用的扫描App

签署页

甲方：陕西省结核病防治院（盖章）	乙方：中移建设有限公司陕西分公司
法定代表人（授权代表）：	负责人（授权代表）：
地址：陕西省西安市长安区太乙宫镇上湾村甲字 1 号	地址：西安市新城区环城北路 70 号
开户银行：中国工商银行西安正大公	开户银行：中国建设银行西安北关支行
账号：37000209090892008856	账号：61050175110000000619
电话：029-85899294	电话：029-82131019
签约日期：2026年 6 月 10 日	签约日期：2026 年 6 月 10 日

扫描全能王
3亿人都在用的扫描App

附件一：服务内容

线上安全托管服务

1）提供20个核心资产（数据中心资产IP数量）提供7*24h连续性的安全保障。不论是白天、黑夜、节假日做到7*24h在线服务，配置一名经验丰富的安全专家作为专属服务经理，组建专属服务团队，实时响应采购人发生的网络安全相关问题。

▲2）提供以下服务效果的SLA：

一般事件：从安全日志产生到通告<1h、遏制影响时间<4h、经确认后，准确率达99%、事件闭环率100%；

一般威胁：从安全日志产生到通告<2h、遏制影响时间<4h、经确认后，准确率达99%、威胁闭环率100%；

重大事件：从安全日志产生到通告（MTTD）<30mim、遏制影响时间<1H、经确认后，准确率达99%、事件闭环率100%；

重大威胁：从安全日志产生到通告（MTTD ）<1h、响应处置时间（MTTR）<1h、经确认后，准确率达99%、威胁闭环率100%；

应急：满足重大事故应启动应急响应机制，工作时间15min之内云端专家进行响应，非工作时间30分钟之内云端专家进行响应，2h上门处置。

3）安全现状评估：系统与Web漏洞扫描：对操作系统、数据库、常见应用/协议、Web通用漏洞与常规漏洞进行漏洞扫描。弱口令扫描：实现信息化资产不同应用弱口令猜解检测，如：SMB、Mssql、Mysql、Oracle、smtp、VNC、ftp、telnet、ssh、tomcat等。

▲4）脆弱性管理：针对服务资产的系统漏洞和Web漏洞进行全量扫描，并针对发现的Web漏洞进行验证，验证漏洞的真实性及分析发生后可造成的危害；对漏洞进行分析并输出可落地的修复方案，通过工单系统跟踪修复情况。可以对服务范围内发现的每一个高危可利用漏洞提供防护规则，并且承诺防护率达到99%。

5）安全问题处置：提供7*24h威胁分析和鉴定服务，安全告警上传至服务

扫描全能王
3亿人都在用的扫描App

云端平台依托平台的大数据分析和威胁检测能力实时监测用户网络安全状态，对平台监测到的安全威胁进行分析鉴定，自动生成服务工单，识别到真正的安全威胁。

6）服务：提供服务成果展示门户：具备服务质量可视化展示，采购人能通过可视化的数据，清晰地了解服务提供商的服务水平，至少包括脆弱性闭环率、脆弱性平均响应时长、脆弱性平均闭环时长、威胁闭环率、威胁平均响应时长、威胁平均闭环时长、事件闭环率、事件平均闭环时长。

▲7）安全设备对接与数据采集：服务提供商安全托管服务云端平台应当支持对接采购人网络中已部署的主要安全设备，包括安全态势感知、威胁检测探针等，支持实时接收安全设备检测到的安全事件信息、安全日志数据提供 7*24h 的安全托管服务。

8）安全合规性要求：服务提供商云端平台应当做好严格的安全防护，并严格按照《信息安全技术—网络安全等级保护基本要求》（GB/T 22239-2019）完成等级保护测评工作。

9）服务交付物：服务期间内，提供包括但不限于以下汇报材料和内容：《项目启动会 PPT》《首次分析与处置报告》《漏洞管理举证报告》《漏洞清单》《服务资产表》《安全服务运营报告》《应急响应报告》《事件分析与处置报告》《安全运营报告》《安全通告》《综合分析报告》《季度汇报 PPT》《年度汇报 PPT》等。

线下安全技术支撑服务

1）关键系统安全风险评估

针对采购人所有重要应用系统，依据 GB/T20984 风险评估规范，进行管理和技术脆弱性识别，确认相关的安全管理制度、安全管理机构和人员、安全管理要求等管理方面是否存在脆弱性；识别资产开放的端口服务、软硬件版本、中间件版本、数据库版本等内容，针对发现的漏洞、版本等信息，分析重要应用系统存在的风险，提供加固指导意见。

服务频次：（1 次/年）

服务成果交付：《关键系统安全风险评估报告》

扫描全能王
3亿人都在用的扫描App

2）资产梳理

对采购人信息系统涉及的资产进行周期性识别，同时对各类资产服务端口现状进行嗅探与分析，结合服务工程师调研补充信息，最终完成资产底图绘制，形成清晰可见的资产分布、服务端口状态、以及维护管理信息于一体的 TI 资产安全状态库。资产状态库中包括但不限于：设备型号、设备功能、互联情况、资产使用年限、资产所有人等相关信息。

服务频次：（1 次/年）

服务成果交付：《资产梳理报告》《资产底图》

3）漏洞检测

通过评估工具以自动化扫描的方式对评估范围内的基础 IT 设备进行安全扫描，发现目标存在的安全风险、漏洞和威胁。扫描工具应采用主流安全扫描工具，扫描工具应使用最新版本，更新漏洞库，对发现的安全隐患进行分析，同时提供具有专业性、针对性的安全加固、整改建议，形成安全加固报告，并对修复的漏洞进行回归性测试。

服务频次：（1 次/年）

服务成果交付：《漏洞扫描报告》。

4）基线核查

通过评估工具对评估范围内的基础 IT 设备进行基线扫描，并通过人工辅助确认两种方式结合完成安全检查工作。基线核查项要求满足国家和行业的安全配置规范， 对于不满足项提供整改建议。

服务频次：（1 次/年）

服务成果交付：《基线核查报告》。

5）渗透测试服务

针对医院 HIS、LIS、PACS、EMR、财务系统等关键系统，采用模拟常见黑客所使用的攻击手段对目标系统进行模拟入侵，发现系统中存在可被利用的弱点，并验证存在弱点可能对业务造成影响，验证弱点被利用可能造成的危害。渗透测试采用内部测试和外部测试相结合的方式，对系统实现全面的测试。开展渗透测

扫描全能王
3亿人都在用的扫描App

试后，记录渗透测试过程并将所发现的安全隐患形成渗透测试报告。

服务频次：（1 次/年）

服务成果交付：《渗透测试报告》。

6）弱口令检查

通过在线检查和离线破解的手段对采购人内外网系统和应用进行弱口令检查。服务提供商应提供符合行业的弱口令字典，弱口令字典应包含常规弱口令、易猜解口令、高重复率口令等。

服务频次：（1 次/年）

服务成果交付：《弱口令检查报告》。

7）新上线系统安全评估

按照网络安全法律法规及相关监管要求，对计划新上线的系统开展漏洞检测、安全配置核查、渗透测试、代码审计等安全检查，及时识别新系统中存在的漏洞及安全风险，在系统上线前采取加固整改措施；在系统开发厂商完成整改后针对初次安全检测发现的问题进行逐一复测，验证安全加固的有效性，保障系统低风险上线运行。

服务频次：（1 次/1 个业务系统）

服务成果交付：《新上线系统安全评估报告》。

8）应急响应安全服务

在合同期限内向采购人提供 7*24h 的网络安全应急响应服务，一旦采购人发生突发性的安全事件后，应急响应人员应该在 1h 内立即到达采购人用户现场，协助采购人完成不限于以下工作：事件范围损失控制，取证，事件处理，外部攻击源追溯，内部脆弱性分析；并提供相关文档翔实记录分析判断过程及结果，包括使用软件记录应急响应顾问在其主机上的所有操作，便于审计和考核。

在安全事件处理完毕后，服务提供商应协助采购人进行事件原因调查，以及系统恢复等后期工作，以建立正常的业务运行环境；服务提供商应在事件处理完毕 1 周内对事件的起因、处理过程、处理方法、处理结果等进行总结，提交完整的《安全事件分析及处理总结报告》。

扫描全能王
3亿人都在用的扫描App

服务频次：（按突发性事件次数）

服务成果交付：《安全事件分析及处理总结报告》。

9）应急演练

协助采购人修订网络安全应急预案、编制应急演练计划、确定演练方案、实施网络安全演练、应急演练报告。

服务频次：（2 次/年）

服务成果交付：《应急演练预案》《应急演练实施方案》《应急演练总结报告》。

10）安全驻场服务

提供 1 名安全服务工程师，配合采购人完成日常安全运行工作，保障业务系统安全稳定运行，不限于安全系统/设备的版本（或规则库、漏洞库、特征库）的更新升级、漏洞整改跟踪、安全日志备份维护、安全策略调整优化、资产台账日常维护、重要时期安全自查和安全值守、安全日志分析及其他采购人交办的网络安全工作。

服务成果交付：《重要时期值守日报》《安全日志分析报告》。

上述服务成果均提交纸质版 1 份，电子版 1份。

扫描全能王
3亿人都在用的扫描App