JZB-2024-072

河南省教育资源保障中心网络安全等级保护及网络安全服务项目

包 2：网络安全服务

合　　同

甲方：河南省教育资源保障中心

乙方：河南安服网络科技有限公司

甲乙双方根据豫财磋商采购-2024-585 磋商文件、乙方响应文件及河南省科教仪器设备招标有限公司发出的中标通知书（成交通知书），依照《中华人民共和国民法典》及有关法律、法规，经双方协商一致就“河南省教育资源保障中心网络安全等级保护及网络安全服务项目，包 2：网络安全服务”达成以下合同条款：

一、工程概况

项目名称：河南省教育资源保障中心网络安全等级保护及网络安全服务项目，包 2：网络安全服务

服务地点：河南省教育资源保障中心

服务内容：网络安全服务

合同总价：人民币 476400.00 元（大写：肆拾柒万陆仟肆佰元整）

资金来源：财政拨款

服 务 期：1年，自合同签订之日起至2025年3月19日止。

二、合同文件及解释顺序

合同条款及附件应能相互解释、互为说明，且双方认识一致，除合同另有约定外，其组成和解释顺序如下：

1、补充合同协议书（如有）；

2、本合同协议书及附件；

3、磋商文件、附件，响应文件及其它优惠条件承诺书；

4、技术规范；

合同履行中甲、乙双方有关项目洽商、变更等书面协议或文件均视为本合同的组成部分。

三、 合同文件适用的法律及标准

1、适用法律法规

本合同文件适用的法律为国家、河南省现行的法律、行政法规。

2、适用的标准规范

双方约定本项目适用现行有效的国家、行业标准、规范、规程。没有国家和行业标准、规范的，双方协商标准。

四、 本合同建设内容

详见附件一；

五、双方的权利和义务

1. 双方的权利和义务

1） 双方有责任在合作过程中，自觉遵守国家的有关法律、法规。

2） 双方应共同遵守合同中的各项条款。

3） 双方应精诚合作、共同配合完成合同各项内容。

2. 甲方的权利和义务

1） 指派专人负责对本项目实施质量监督和办理本合同中协商的事宜。

2） 负责本项目实施中需要甲方协调的事宜。

3） 为乙方提供本项目所必须的文件、资料等相关信息，对乙方在项目建设过程中呈报的有关文档和报告及时批复。

4） 对于合同期内乙方工作人员的安全问题由乙方自行负责，甲方不承担任何责任。

3. 乙方的权利和义务

1）指派专人成立项目工作组，负责对本项目实施需求调研、开发、测试、运行、工期等控制和办理本合同协商事宜。

2）按本合同确定的工程进度、质量、内容，认真、按时、保质完成各项工作，并及时向甲方汇报与确认。

3）及时响应甲方的服务要求，提交项目中所需的各项文档和相关方案。接受甲方的检查、监督和统一安排等。

六、系统试运行和验收

甲、乙双方共同组织验收。

1. 标准：本合同、磋商文件、响应文件及国家有关规范、法律。

2. 在项目具备验收条件时，乙方先进行系统自检、系统测试（压力、性能、功能等综合测试），在自检通过后向甲方出具自检和测试报告，得到确认后甲方应尽快安排试运行，试运行期限为 30 日。

3. 试运行期满后，乙方向甲方提交试运行报告并提出验收申请，甲方应当在收到申请后尽快完成验收。

4. 项目验收时，乙方需向甲方提交磋商文件中提到的竣工文档和相关资料等，并配合甲方做好验收材料整理工作。因乙方未提供相关资料影响项目验收的，相关责任由乙方承担。

七、付款方式

1. 乙方提供的服务达到验收标准，验收合格后，甲方在 10 个工作日内支付合同金额的 100%，即：人民币肆拾柒万陆仟肆佰元整（￥：476400.00）。 该价款包含了税款、技术服务费、人工服务费、培训费等全部费用，除此之外，甲方不再支付其他费用。甲方付款之前，乙方应先向甲方交付相应金额的符合甲方财务管理要求的发票。因发票交付迟延的，甲方付款期限相应顺延。

乙方指定收款账户信息：

名称：河南安服网络科技有限公司

开户行：中国民生银行郑州农科路支行

银行账户：637916054

统一社会信用代码：91410100MA45L0FX9A

企业规模：小型企业

2. 在本合同签订之前，乙方应向甲方指定的账户支付本合同总价款 5%的履约保证金。在本合同服务项目验收合格无问题后 10 个工作日内，甲方将前述履约保证金无息一次性退还给乙方。如乙方在履行合同过程中存在违约行为或者验收不合格的，甲方有权扣除履约保证金，不予退还。前述履约保证金不足以弥补因乙方违约给甲方造成的损失的，乙方还应继续赔偿。

八、技术培训及售后服务

1. 根据项目情况，根据需要项目启动初期培训、项目实施中培训和项目实施后的培训。培训人员涉及用户方领导、用户方系统管理员及系统操作人员。培训方式：集中培训和单独培训，培训需甲方确定受训人员，由乙方进行培训，乙方提供场地、培训讲师和教材，并承担相关费用。培训内容涉及系统的实际操作、系统运行注意事项、系统日常维护等。

2. 售后服务

乙方应安排具备运行保障能力的工程师驻场提供技术支撑服务。紧急事件应立即做出响应，并在 1 小时内给予解决；一般事件应在 1 小时内做出响应和安排，并在 4 小时内给予解决。

对本项目的服务承诺：提供本地化的驻场服务和一年免费售后服务，具体详见中标单位响应文件承诺。

九、争议与索赔

1. 甲、乙双方对本合同的条款在理解上发生争议时，应本着友好协商的态度修改、补充有关条款；双方在履行合同时如发生争议，亦应友好协商解决，如协商不成，任何一方均可向甲方所在地人民法院提起诉讼解决。

2. 如需索赔，按法律程序及合同约定解决。

十、违约责任

本合同签订后，甲方无正当理由逾期履行付款义务的，每逾期一日应按照应付未付金额的万分之五向乙方支付违约金。乙方未按约定期限全面履行合同义务、或者乙方所交付货物/所提供服务出现质量问题经甲方通知整改后未按期按要求整改完成的、或者乙方提供的服务无法满足或全部满足合同附件约定的功能目的和要求的、或者有违反合同约定的其它违约行为的，每逾期一日乙方应按照合同总价款的万分之五向甲方支付违约金，逾期超过 10 个工作日的，甲方有权立即通知乙方解除本合同，并有权要求乙方返还甲方已付全部款项，赔偿因此给甲方造成的全部损失，包括但不限于律师费、诉讼费、保全费、保全担保费、评估鉴定费、拍卖费、差旅费等依法维权产生的支出。

十一、不可抗力

1. 如果双方中的任何一方因为战争、严重的火灾、台风、洪水、地震等属于不可抗力的原因而被迫停止或推迟合同的履行，则合同履行相应顺延，顺延的时间等于不可抗力发生作用的时间。

2. 受影响的一方应将不可抗力的出现尽快通过电传或传真通知另一方。在不可抗力出现 14 天内，受影响的一方应提供有关权威机构出具的证明文件并通过快件或挂号信等书面方式寄至另一方以便其核实和确认。

3. 受影响的一方在不可抗力终止或被排除后应尽快通过电传或传真通知另一方，并以书面形式正式告知另一方。

4. 如果不可抗力持续作用超过 120 天，双方将通过友好协商解决未来的合同履行问题。

十二、合同份数及生效

本协议一式 四 份，甲方 贰 份、乙双方 贰 份，具有同等法律效力。本协议自甲乙双方法定代表人或委托代理人签字并加盖公章之日起生效。

甲方（盖章）：河南省教育资源保障中心

法定代表人（或代表）签字：

2024.8.14

地　　址：河南省郑州市金水区顺河路 17 号

联系电话：　0371-69691651

开 户 行：交通银行郑州顺河路支行

帐　　号：411621999011002924369

乙方：（公章）河南安服网络科技有限公司

法定代表人（或代表）签字：

2024年7月14日

地　　址：郑州高新技术产业开发区金菊街 30 号 1 幢 1 单元 15 层 301 号

联系电话：13633770503

开 户 行：中国民生银行股份有限公司郑州农科路支行

帐　　号：637916054

附件 1：

序号	服务内容
1	**安全监测服务：** 1、安排技术团队提供网络安全监测服务，其中有 2 名专职名技术人员提供驻场技术服务，做好技术保障工作；其他技术人员采用远程、电话、电子邮件、即时通讯、现场服务等方式，按要求做好服务工作； 2、▲能提供专用的即时通讯工具（非 QQ、微信类互联网常用即时聊天软件）用于安全监测的日常沟通、告警通报和威胁预警推送，防止关键信息泄露，聊天内容及传输文件存储于私有云服务器端，方便后期查询和追溯（提供相关即时通讯工具软件著作权证书）； 3、监测服务期间，需提供 APT 威胁感知类工具免费使用，APT 威胁感知类工具至少包括流量采集探针，分析平台，漏洞扫描设备等安全工具组件。 4、流量采集探针要求内存不少于 64G，存储空间不少于 4TB，流量日志采集性能不低于吞吐量 8G，并发连接数不低于 700W，支持常见协议和文件识别并还原，用于取证分析、威胁发现； 5、流量采集探针能够支持基于 IP 地址的旁路阻断，能够与分析平台联动在实时镜像的流量中发现恶意 IP 并实现实时阻断。 6、分析平台组件要求内存不少于 256G，存储空间不少于 48TB，日志处理性能不低于 17000 eps； 7、提供漏洞扫描工具，支持扫描 IP 地址最大支持 1024 个，支持扫描 A 类、B 类、C 类地址，系统扫描支持 50 个 IP 地址并行扫描。标准 1U 机架式，1T 硬盘，标准配置 6 个 10/100/1000M 自适应电口，2 个扩展插槽，2 个 USB 口，1 个 Console 口，单电源。报价中包含三年漏洞特征库升级，三年硬件维修服务。 8、▲分析平台组件能对网络内资产进行识别和管理，并能够与专业互联网漏洞平台进行对接，实时获取与内部资产相关的漏洞情况。（提供加盖公章的互联网漏洞平台对接的功能截图证明）； 9、▲分析平台组件能提供云端威胁情报平台的查询验证能力，支持查询 IP、域名威胁类型分类，流行度评估，创建时间、更新时间、过期时间查看，支持开源情报判定对比、相关样本分析、情报拓线分析、历史 A 记录信息、注册信息（包含域名注册人、注册人所属组织、管理员邮箱、电话、传真、所属国家、服务运营商等），支持查看关联域名，域名数字证书等信息，能够进一步的对发现的威胁告警提供验证分析。（提供加盖威胁情报平台厂商公章的威胁情报平台网站截图证明，并提供平台 URL 地址）； 10、驻场人员每天定时将网络中各类威胁告警编制分析报告并上报，分析报告内容包括：

普通 IOC 告警分析、传感器漏洞分析、暴力破解分析、网站后门分析、数据库安全分析，邮件安全分析、APT 深度告警分析等，并提供告警处置意见，协助客户对发现的威胁及漏洞进行处置；

11、▲对发现的系统、应用漏洞，驻场人员能提供统一的自动化打补丁工具，协助应用、系统厂商提供系统加固工作，补丁工具支持具备蓝屏修复功能，对打补丁出现问题的应用系统进行回滚恢复。（提供加盖打补丁工具厂商公章的功能截图证明）；

12、网络安全态势推送服务，能根据日常的监测情况，对网络风险进行预测，定期统计潜在风险资产数、受攻击资产数、失陷资产数以支持对重大网络安全事件（如永恒之蓝，Struts 2 漏洞利用等新生大面积爆发的严重事件）进行威胁预警；

13、服务人员能够对重大网络安全事件的追踪生成预警包，通过预警包导入监测工具，完成网络安全事件的影响面评估，并持续的跟进事态的发展，快速完成重大网络安全事件的预警及处置；

14、提供自动化渗透工具，定期对针对目标系统提供渗透测试，进行对抗性的模拟攻击，测试发现系统、技术、人员和基础架构中的存在有可能被黑客利用的安全漏洞，并生成并提供相应的分析渗透测试报告。

15、▲服务器资产梳理服务：提供服务器安全管理工具，通过自动、手动方式，定期对现有 Windows、Linux、信创等服务器资产的软硬件信息进行盘查清点，包括但不限于 CPU 品牌及核数、内存、硬盘容量、硬盘分区数、硬盘空间、硬盘使用率、账户数、软件应用数、web 站点数、web 服务数、web 框架数、数据库数、端口数、网络连接数、启动服务数、安装包数、计划任务数、环境变量数、内核模块数、证书数、注册表数、类库数等信息；（提供相关服务器安全管理工具软件著作权证书，并提供功能证明材料并加盖制造商公章）

16、▲资产行为分析服务：提供服务器安全管理工具，对每台服务器的网络外连行为、命令执行行为、文件行为进行分析，并形成图形化的时间轴行为基线，对于偏离行为以外的动作进行分析和告警；对服务器的应用进行学习统计，并通过加固工具添加应用白名单，对偏离白名单列表以外的应用进行告警和拦截。（提供相关服务工具功能证明材料并加盖制造商公章）。

17、▲资产隔离策略服务：提供服务器安全管理工具，梳理并部署服务器主机防火墙策略，根据防护需要设置以 IP/端口/协议/方向/域名/进服务等条件的主机防火墙策略，安装要求设置端口白名单，设置进程控制规则。发现安全事件后，支持及时对主机进行一键隔离、一键禁止暴露外网、一键禁止暴露内网等快速应急操作服务。（提供相关服务工具功能证明材料并加盖制造商公章）。

18、▲资产账号风险评估服务：提供服务器安全管理工具，提供风险账户检测服务，对服务器中复用的相同密码进行检测，可识别出某个密码被哪些服务器、哪个账户、在什么操作系统上进行了复用；提供系统级、应用级弱口令、域控弱口令扫描服务。支持 Windows 系

	统、Linux 系统、Tomcat、vsftp、Redis、pptp、rsync、SVN、jenkins、Oracle、Mysql、SqlServer、PostgreSQL、Weblogic、ES、activemq、openvpn、nginx、域控、IIS、SSH、proftp、mongoDB、tiger_vnc、OpenLDAP、Windows FTP 等不少于 25 种系统、应用的弱密码检测。（提供相关服务工具功能证明材料并加盖制造商公章）。 19、▲资产基线检查服务：提供服务器安全管理工具，定期对服务器的安全进行检测，支持包括等保三级、CIS、系统服务核查、账户安全核查、系统配置安全检查、应用配置安全检项等多种基线检测。（提供相关服务工具功能证明材料并加盖制造商公章）。 20、在护网或者重保期间，提供不少于 2 人的团队驻场，24 小时值守服务，保证网络安全事件第一时间发现、处置。 21、▲提供河南省教育厅义务教育招生服务平台 Web 安全防护特征库一年升级授权服务；需提供原厂升级授权书，服务期间安排服务工程师定期进行 Web 安全防护特征库更新，确保义务教育招生服务平台能得到实时最新的 Web 安全防护； 22、▲提供河南省教育厅义务教育招生服务平台网络威胁入侵防御特征库一年升级授权服务；需提供原厂升级授权书，服务期间安排服务工程师定期进行网络威胁入侵防御库更新，确保义务教育招生服务平台能得到实时最新的网络入侵安全防护；服务期间按月定期或根据甲方需求进行相关特征库版本检查并升级最新版本，提交服务记录报告；在重大网络保障活动之前及活动期间，安排服务工程师及时进行特征库进行升级更新；结合网络威胁态势情报及时对相关特征库及时更新升级；服务期间对于服务请求达到 100%的用户响应度，响应时间 10、分钟内；突发性服务请求响应达 100%的用户响应度，工作时间 5 分钟内响应，非工作时间（含节假日）30 分钟内响应；服务时间：7*24 小时实时响应。