合同编号：豫财竞谈-2021-95

郑州大学（服务）采购合同

甲方： 郑州大学

乙方： 河南融浩通信工程有限公司

本合同于 2021 年 12 月 8 日由甲乙双方按下述条款签署。

一、合同内容及要求：

合同内容：根据网络安全等级保护相关标准，中心系统建设完成后须满足等级保护标准 2.0 满足的第三级系统安全保护要求，并能够提供定制化的安全增值服务，具体内容详见竞争性谈判文件。

合同要求：见竞谈文件第三章。

二、本合同总价款（大写）为：壹佰肆拾陆万伍仟圆整（小写￥1465000 元）

三、质量要求或服务标准，乙方对质量负责的条件和期限：

质量要求：满足采购人要求。

项目采购需求及相关要求：如下。

河南省超级计算中心（国家超级计算郑州中心）以应用需求为导向，立足河南、服务全国，为全省企业、高等院校、科研机构等各类企事业单位提供强大计算服务和数据处理服务，依托完善的生态与良好的兼容性，面向众多不同领域与行业应用需求，提供高性能计算、人工智能、大数据、行业应用等软件资源服务，重点围绕数字经济、社会管理、精准医学、生物育种、环境治理、高端装备、人工智能、国土资源管理等方面开展重点特色应用；随着河南省超级计算中心（国家超级计算郑州中心）当前业务的不断发展，用户业务接入量的不断扩大，所面临的安全威胁与安全需求也越来越复杂多样，考虑到中心核心业务系统等级保护建设（三级）的目标和常态化的安全服务需求，本次服务应基于当前超算中心的业务发展方向和等保建设差距健全超算中心安全保障体系，要求本次服务依据信

息安全防御体系建设有关的法律法规和技术标准，切实提升超算中心常态化安全运维能力，促进核心业务系统达到等级保护建设（三级）的能力。

序号	服务项	服务内容要求
1	安全服务对象	1套先进计算平台、4套HPC管理系统、1套CAE调度系统、1套统一登录系统、1套消息管理系统、6套高性能计算存储管理系统、1套共享文件系统、1套智能运维平台、1套消防监控系统、1套动环监控系统、1套安防监控系统、2套人工智能训练平台、1套工单管理系统、1套DNS域名解析服务平台、2套云平台、1套用户资源申请审批系统、2套ansys调度系统、1套用户管理系统；
2	系统安全风险持续监测服务	服务要求：要求在服务期内以现场服务的方式，采用专业安全监测工具和人工结合的手段对目标业务系统的安全状态进行全天候7*24小时监测； 服务内容：采用专业的安全监测工具和人工结合的方法，通过部署于各信息节点的监测引擎对甲方指定的系统和平台进行可用率和安全性监测，以保障甲方系统和平台业务持续性，从而向甲方提供系统和平台安全的保障。服务需提供安全监测工具（千兆电口≥6个；支持旁路镜像模式部署及分布式部署，支持与现网威胁感知大数据平台进行数据推送服务（需提供现网威胁感知大数据平台厂商API开放服务承诺），持监测流量状态，基于时间维度记录并展示流入、流出流量情况，并记录流量的总流入流出情况。支持流量监测的开关控制。支持沙箱分析功能，分析结果包括但不限于文件名称、文件MD5、受感染主机、威胁指数、传播次数、动态检测结果、静态检测结果、病毒检测结果。支持跳转展示沙箱分析详情，展示文件的静态检测、动态检测、病毒检测结果。支持文件上传分析，分析维度包括但不限于文件名、文件类型、处理状态、检测结果、上传时间、检测完成时间、文件MD5。支持跳转展示文件上传分析详情，展示文件的静态检测、动态检测、病毒检测结果。并支持文件下载。支持邮件威胁分析，分析结果展示发件人、收件人邮箱地址、威胁指数、攻击类型、地址欺骗、恶意URL链接、敏感字。支持检测常见的邮件协议类型：SMTP、POP3、IMAP。工具自身具备流量采集及协议解析还原能力，支持解析的协议包括但不限于HTTP、FTP、TLS、SMB、DNS、DCERPC、SSH、SMTP、IMAP、MODBUS、DNP3、ENIP、NFS、IKEV2、KRB5、NTP、DHCP、RFB、RDP、SNMP、TFTP、SIP、HTTP2、POP3等 。工具支持基于虚拟执行的动态检测技术，可以基于软件在虚拟环境的行为及通用漏洞利用特征，分类识别各种病毒及未知恶意代码。）；
3	系统安全事件应急防御服务	服务要求：要求在服务期内以现场服务的方式，采用专业安全防御工具和人工结合的手段对目标业务系统的安全事件进行全天候7*24小时防御；

		服务内容：采用专业的安全防御工具和人工结合的方法，通过部署于各信息节点的监测引擎发现的安全事件进行应急响应处理，以保障甲方系统和平台业务持续性，从而向甲方提供系统和平台安全的保障。服务中需提供安全防御工具（千兆电口≥8个，千兆光口≥2个，攻击防御性能≥600Mbps。支持SQL注入、跨站脚本攻击、会话劫持等攻击防护；支持Web服务器加固：服务器信息隐藏、网络爬虫检测和阻止；支持Web流量优化：负载均衡、Web加速、SSL卸载，有效保障交互过程中数据的安全性和完整性。）；
4	安全日志分析服务	服务要求：要求在服务期内以现场服务的方式，采用专业日志分析工具和人工结合的手段对目标业务系统相关的安全日志进行7*24小时审计和分析； 服务内容：采用专业日志分析工具和人工结合的综合审计方法进对现网防火墙、IPS、WAF等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，从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。服务需提供日志分析工具（千兆电口≥6个，日志分析处理能力≥2000条/秒，支持网络设备、安全设备、数据库、操作系统、应用系统等各类资产的日志收集，支持Syslog、Syslog-ng 、SNMP Trap、文件、WMI、FTP、数据库等方式采集日志，支持根据设备类型，按日期展示日志的接入情况，包含不同级别日志数量统计，支持自定义审计类型配合不同的审计分析策略，支持与现网运维平台进行数据推送服务（需提供现网运维平台厂商API开放服务承诺）；
5	数据库安全审计服务	服务要求：在服务期内以现场服务的方式，采用专业数据库安全审计工具和人工结合的手段对目标业务系统的数据库进行全面7*24小时安全审计； 服务内容：采用专业日志分析工具和人工结合的综合审计方法，通过对访问数据库的行为、内容等进行采集、存储、分析，实现完全独立于数据库的审计功能，并生成合规报告，便于事故追根溯源，提高数据资产安全。服务需提供数据库安全分析工具（千兆电口≥6个， SQL处理能力≥20000条/秒、入库量≥10000条/秒、日志存储能力≥20亿条，支持国际主流数据库、国产数据库、非关系型数据库等，能够扫描网络中的开放的服务，自动发现网络中存在的数据库系统，能够自动或手动将这些服务进行安全防护，支持将扫描到的服务进行概要化图表展示和报表导出，支持SQL命令的细粒度审计和分析，并记录详细的用户行为信息，可以对网络中存在的SQL注入、缓冲区溢出、权限提升等漏洞攻击行为进行审计和告警。）；
6	运维行为安全审计服务	服务要求：在服务期内以现场服务的方式，采用专业网络安全审计工具和人工结合的手段对目标业务系统的网络运维安全进行7*24小时全面审计； 服务内容：采用专业网络运维行为审计工具和人工结合的综

		合审计方法，通过对目标业务系统进行账号集中管理、身份统一认证、资源按需授权、过程全面审计和控制，通过事前预防、事中控制和事后审计来全面超算中心目标系统的运维安全管理问题。服务需提供网络运维安全审计工具（最大字符连接≥100个，最大图型连接≥50个，支持通过动作流配置提供广泛的应用接入支持，无论被接入的资源如何设计登录动作，通过动作流配置即可实现单点登陆和审计接入，支持 unix 资源、windows 资源、网络设备资源、数据库资源、C/S 资源、B/S 资源， 支持一对一、一对多、多对多授权，如将单个资产授权多个用户，一个用户授予多个资产，用户组向资产组授权，支持监控正在运维的会话，信息包括运维用户、运维客户端地址、资源地址、协议、开始时间等，并可以实时阻断，支持运维审计自查询功能，用户可查看自身的运维审计历史。）；
7	安全检测升级服务	服务要求：服务期内提供安全检测相关工具的升级服务，提升现网安全检测能力； 服务内容：对现网的安全检测工具并发扫描数提供扩容升级服务，要求扩容2K扫描权限，提供厂商升级服务授权；对现有态势感知系统进行系统升级服务实现安全检测联动能力，提供厂商升级服务授权；
8	攻防演练服务	服务要求：要求服务期内依托专业的安全服务厂商团队提供1年1次现场攻防演练服务； 服务内容：充分利用现有安全检测与防御手段，结合安全监测与分析经验，协助实时检测与分析攻击行为，快速响应处置，抑制攻击事件，现场服务人员不少于 5 人；服务商应为本项目组配置具有丰富经验的实施团队。其中项目经理至少具备：项目经理需具有CISP、CISSP、PMP、ISO27001 Foundation、Security+、CISAW、等保测评师、监理工程师等资质中的至少3个，需提供证书复印件；服务商实施团队中至少2人具备CISP认证，需提供证书复印件；至少1人具备信息安全等级测评师认证，需提供证书复印件；
9	等保测评服务	服务要求：要求服务商在服务期内依托具备国家信息系统安全等级保护测评认证资质的安全测评机构（需要提供安全测评机构的服务授权函并加盖公章），根据《GB/T 22239—2019 网络安全等级保护基本要求》（若有新发布的等级保护相关标准，按照新标准展开测评）完成至少2个三级，3个二级信息系统等级保护测评服务，并完成相关系统的测评、整改及定级、备案工作； 服务内容：（1）安全技术测评：包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心等五个方面的安全测评；（2）安全管理测评：安全管理制度、安全管理制机构、安全管理人员、安全建设管理和安全运维管理等五个方面的安全测评；（3）系统整体测评：安全控制点间、层面间、区域间、系统结构安全等四个方面的安全测评；

		测评工作实施时，必须保证现有系统 24 小时的不间断、稳定、安全运行，在此要求下完成全部安全等级测评工作； 开展测评工作时间，应尽量避开业务高峰期。工具测试期间，应安排在夜间或法定节假日期间，制定切实可行的工具测试方案。对出现意外宕机等应提供应急保障方案，确保关键环节能正常工作； 测评人员应具有信息安全等级保护测评师证书，提供复印件并加盖公章；
10	等保差距分析服务	服务要求：要求服务商在完成等保备案前提供现场技术服务； 服务内容：依照《信息安全等级保护安全建设整改工作指导意见》（公信安[2009]1429 号），严格遵循《信息安全等级保护安全建设整改工作指南》各项要求，在系统测评工作的基础上，严格按照GB/T 20984、GB/T 31509、公安部等级保护标准对平台相关的网站和业务系统，进行模拟黑客的安全渗透测试和差距分析，对系统存在的安全漏洞进行准确查找，完成后提供详细的渗透测试报告，并在报告中给出漏洞修复建议；渗透测试指标范围需要包括用户账号测试、通用型漏洞测试、S2专项等特定型漏洞测试、逻辑漏洞测试、中间件getshell漏洞测试，基于渗透测试结果输出差距分析评估报告； 等保差距分析服务完成后要求服务方向用户方输出《系统渗透测试报告》、《等保差距分析评估报告》，报告必须为人工编写； 渗透测试人员应具有网络安全等级测评师以及国家注册信息安全专业人员证书（CISP）证书，提供复印件并加盖公章；
11	等保安全整改服务	服务要求：要求提供现场技术服务，基于《系统渗透测试报告》、《等保差距分析评估报告》对存在安全漏洞进行修复、配置隐患进行优化； 服务内容：加固内容包括但不限于系统补丁、防火墙、防病毒、危险服务、共享、自动播放、密码安全。在修复漏洞后，对漏洞修复情况进行复测；复测工作需要在甲方规定的时间内完成；安全加固服务完成后要求服务方输出《安全加固报告》（含加固前后漏洞对比）、《加固前漏洞扫描报告》、《加固后漏洞扫描报告》以及《安全加固应急及回退方案》，报告必须为人工编写；
12	信息安全管理制度服务	服务要求：安全管理制度服务，以ISO27001为基准，包括现有安全管理制度收集、进行差距分析、构架安全制度框架、编写安全管理制度、安全制度改进等一系列服务； 服务内容：依托专业的安全服务厂商提供本服务为超算中心梳理现有安全制度，找出差距点，并修订或编写必须的信息安全管理制度，提升超算中心的安全管理水平；
13	计算专区安全提升服务	服务要求：要求在服务期内配合超算中心基于超算当前用户业务、数据的需要，对超算中心计算专区进行安全提升服务； 服务内容：对现有的超算计算集群基于业务规划、实际需求及安全提升的需要，进行超算计算专区的改造服务，服务中

		涉及超算高速网络交换机（具备≥40个200Gb/s双向带宽HDR网络端口、≤90ns的延时、≥16Tb/s聚合带宽、辅助工具连接的线缆等）的接入服务，以满足实际改造需求为准；
14	安全运维可视化服务	服务要求：在服务期内提供对现网安全数据、结果、态势的可视化服务； 服务内容：提供2套7*24小时实时安全运维可视化及展示的能力，可视化呈现在甲方指定物理位置，尺寸≥75寸，支持多种音效模式，支持HDMI服务输入，USB输入服务，支持USB流媒体播放，支持H.265/H.264/MPEG-4等视频解码，支持MP3/AAC/AC3/Dolby/DTS等音频解码，支持JPG,PNG,BMP，支持WiFi，2.4GHz/5GHz（802.11a/b/g/n/ac）；
15	安全驻场服务	服务要求：服务期内依托相关安全工具和平台提供三年5*8的现场驻场安全服务，常驻现场人员≥2人； 服务内容：驻场人员现场进行安全巡检，通过人员访谈、现场勘查、文档查看等手段了解管理弱点；对网络、安全、业务等如路由器、交换机、防火墙、服务器、数据库、存储、中间件等的运行状况、资源利用情况、网络连接情况等进行检查，检查系统健康状态，同时利用工具扫描、人工审计、基线检查、配置分析等方式对信息系统的技术脆弱性进行评估，并给出脆弱性评估报告。对于发现的漏洞及可能造成的风险给出详细的、按危害等级排序的总结报告（系统性安全巡检1次/月；基础安全巡检1次/天）；
16	定制化本地培训服务	服务要求：在服务期内提供原厂商专业讲师本地培训服务及日常攻防实验学习平台服务，要求服务期内本地培训服务每年不少于2次； 服务内容：（1）培训课程应包括但不限于网络安全架构设计和网络安全设备的部署；WINDOWS、LINUX等常见操作系统安全、SQL-SERVER、ORACL等常见数据库安全、常见应用系统安全、常见网络设备安全；网络攻击及系统安全检查和防范加固；恶意代码检查和清除；WEB应用威胁及安全防护技术；安全事件应急响应和入侵检查；网络攻击入侵预警、监测、防护、恢复技术措施；安全域和边界整合、边界访问控制措施；虚拟化与云计算安全技术；信息安全风险评估及信息安全规划；其他定制化的安全培训等；全方位提高网络管理人员安全运维技术与管理能力，培训内容完善、合理、科学，讲师具有培训证书；（2）攻防实验学习平台服务支持满足20人同时在线实时学习攻防知识，开启、关闭、还原实验环境，下载实验工具，完成实时测验，支持对靶场机资源调度和管理，对虚拟出的多个仿真业务场景进行添加、删除、开启、关闭等支持在线注册实时学习各类攻防课程技术，配套实验教学的攻防实战工具资源库，可用于各类安全攻防测试，并在服务期内人员通过测试获得相应的攻防认证证书。

四、服务约定：

1、**服务完成时间：**

等保测评分析服务：自合同签订之日起 30 日历天内完成。

后续监控服务：自验收之日起 1095 个日历天。

2、**服务地点：**郑州市高新区长椿路与枫杨街交叉口郑州大学河南省超级计算中心。

3、**服务方式：**质保期内，自验收合格起，乙方提供三年的免费售后服务 ；提供三年 5*8 小时安全保障服务。

五、验收标准、方法：

验收标准：完成等保差距分析服务，提供相应材料、报告；提供后续服务方案及服务承诺书。

1、等保差距分析服务，提供如下检测报告：

(1) 《先进计算平台等保差距分析报告》
(2) 《先进计算平台安全检测报告》
(3) 《云平台等保差距分析报告》
(4) 《云平台安全检测报告》
(5) 《官网等保差距分析报告》
(6) 《官网安全检测报告》
(7) 《工单系统等保差距分析报告》
(8) 《工单系统安全检测报告》
(9) 《PBS 调度系统等保差距分析报告》
(10) 《PBS 调度系统安全检测报告》

2、提供后续服务方案及服务承诺书；

验收方法：专家评审。

六、结算方式及期限：

验收合格审计后，甲方向乙方支付合同总价款的 80%，即人民币（大写）：壹佰壹拾柒万贰仟圆整（￥1172000 元）；质保期满后，甲方向乙方支付剩余 20%的货款，即人民币（大写）：贰拾玖万叁仟圆整（￥293000 元）。

七、免费质保约定：

1、质保期内，自验收合格起，我公司提供一年的免费技术服务，其中服务内容涉及：系统安全风险持续监测服务、系统安全事件应急防御服务、安全日志分析服务、数据库安全审计服务、运维行为安全审计服务、安全检测升级服务、攻防演练服务、等保测评服务、等保差距分析服务、等保安全整改服务、信息安全管理制度服务、计算专区安全提升服务、安全运维可视化服务、安全驻场服务

和定制化本地培训服务等 15 项内容。

2、我公司针对本项目提供三年 2 人 5*8 小时安全驻场运营保障服务。

3、质保期满后，我公司提供免费咨询服务，为用户提供永久咨询服务。

八、售后服务承诺

乙方承诺对本项目的售后服务坚持以河南省超级计算中心（国家超级计算郑州中心）应用需求为导向，基于当前超算中心的业务发展方向和等保建设差距健全超算中心安全保障体系，依据信息安全防御体系建设有关的法律法规和技术标准，切实提升超算中心常态化安全运维能力。

在本项目建设过程中，乙方除响应招标文件中所有的条款及履约合同内容外，并对项目售后服务做出如下承诺：

1、在质保期内针对本项目，乙方将提供 2 人三年 5*8h 的现场服务，若涉及到服务系统出现故障，自接到甲方报修电话时，我方现场工程师实时响应，30 分钟内解决故障问题，如在规定时间内无法解决问题，联系相关服务系统或设备厂商远程协助或临时提供系统备件，4 小时内解决解决故障。

2、质保期满后，我公司提供免费咨询服务，为用户提供永久咨询服务。

3、针对超算中心举办或者政府要求的重大活动，免费提供网络系统的安全保障服务。

4、乙方将对重大故障提供 7*24 小时的现场支援，一般故障提供 5*8 小时的现场支援。

5、对甲方相关人员实施免费的现场培训或集中培训措施，保证甲方相关人员能够独立操作、熟练使用、维护和管理有关设备。

6、为保障用户业务系统的正常运行，在售后技术支持服务期间，乙方开通电话、传真、邮件等多种联系方式，响应用户服务请求，必要时直达用户现场。

7、热线联系方式：0371-55331805。

九、履约担保

承包人提供履约担保的形式：以转账的方式提供；

履约担保金额：合同价的 5%；

履约担保期限：履约担保的有效期始于工程开工之日，终止日期则可以约定为工程竣工交付之日。履约担保金在签订合同前交学校财务，工程竣工验收合格

交付使用后履行手续退还。

十、违约责任：

1、乙方违约：乙方提供的服务内容不符合约定的质量要求，甲方有权解除或终止合同，并要求乙方按合同总价款的5%支付违约金，给甲方造成经济损失的，乙方还应如数赔偿；乙方未按约定期限交付标的物，每迟延一天须按合同总价的1%向甲方支付违约金。如果乙方对合同迟延履行超过合理期限，甲方有权解除或终止，并且要求乙方赔偿由此造成的经济损失。

2、甲方违约：甲方未能按双方约定的方式和期限支付货款，按有关法律规定对乙方承担违约责任。

3、双方其他违约责任按《中华人民共和国民法典》的有关规定处理。

十一、解决合同纠纷的方式：双方在执行合同时产生纠纷，协商解决；协商不成，向甲方所在地人民法院提起诉讼。

十二、其它约定事项：无

十三、本合同未尽事宜，甲乙双方可协商签订补充协议，与本合同具有同等法律效力。

十四、本合同正本贰份、副本捌份，甲方与乙方各执肆份，报送招标代理机构贰份。

十五、本合同双方签字盖章后生效，随合同履行完成而自行终止。

甲方（盖章）：郑州大学

法定代表人或代理人：

单位地址：河南省郑州市高新区科学大道100号

电话：0371-67739795

开户银行：工商银行郑州中苑名都支行

户名：郑州大学

2021年12月15日

乙方（盖章）：河南融浩通信工程有限公司

法定代表人或代理人：

单位地址：郑州市金水区东风路18号汇宝花园19号楼5单元6楼东户

电话：0371-55331805

开户银行：中国工商银行股份有限公司郑州行政区支行

户名：河南融浩通信工程有限公司

2021年12月15日

帐号：1702021109014403854

签署日期：2021.12.15

帐号：1702 0291 0920 1104 207

签署日期：2021.12.15

签约地点：国家超级计算郑州中心

附：中标通知书

中 标（成交）通 知 书

河南融浩通信工程有限公司：

你方递交的郑州大学河南省超级计算中心网络及安全设备续保采购项目 投标文件，经专家评标委员会（或询价小组、竞争性磋商小组、竞争性谈判小组）评审，被确定为中标人。

主要内容如下：

项目名称	郑州大学河南省超级计算中心网络及安全设备续保采购项目
采购编号	豫财竞谈-2021-95
中标（成交） 价	1465000 元(人民币) 壹佰肆拾陆万伍仟元整(人民币)
供货期（完工期、服务期限）	1095 个日历天
供货（施工、服务）质量	满足采购人要求
交货（施工、服务）地点	采购人指定地点
质保期	自验收合格起，提供一年的免费技术服务

请你方自中标通知书发出之日起 3 日内与招标人洽谈合同事项。联系人及电话：刘海涛 13700844282

特此通知。

采购单位(盖章)　　代理单位（盖章）

2021 年 11 月 2 日

中标单位签收人：李夏晴