合同编号：HW506220111

豫财招标采购-2022-704

郑州大学国家超级计算郑州中心网络安全基础设施提升项目

采购合同

甲方：郑州大学

乙方：河南省鼎信信息安全等级测评有限公司

一、合同内容及要求：

序号	服务项目名称	服务内容	单位
1	等保测评服务	1、按照《信息系统安全等级保护测评要求》政策文件的技术要求，开展等级测评服务，遵照《信息系统安全等级测评报告模版》编制测评报告； 2、按照《信息安全等级保护安全建设整改工作指导意见》，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。 两年（现网安全等级保护认证证书到期之日前 3 个月起，每年开展一次安全等级测评）	1 项
2	等保安全整改服务		1 项
3	系统安全保障服务	提供安全服务保障，针对常见的注入攻击、跨站攻击、WEBSHELL 上传、CC 攻击、漏洞利用等攻击手段及时发现及时阻断，出具安全保障报告。 **服务期限：自签订合同之日起 3 年**	1 项
4	安全巡检服务	对安全设备、网络设备、服务器、业务系统进行安全巡检服务，可以根据约定的服务方式（现场检查，远程检查）依照标准化流程，对系统进行安全巡检，了解系统的整体工作状态。由被动服务变主动服务，通过安全巡检服务排除故障隐患，降低故障率。 **服务期限：自签订合同之日起3年**	1 项

序号	服务项目名称	服务内容	单位
5	信息安全管理制度服务	按照国家等级保护三级要求、公安部的网络安全要求及网络安全规划，以 ISO27000、ITIL 系列标准以及国际、国内最佳实践为指导，协助国家超级计算郑州中心制定信息安全管理制度。	1 项
6	应急响应服务	在服务期内，协助郑州超算中心建立安全应急预案，在中心遇到重大安全事件如网络入侵、大规模病毒爆发、遭受拒绝服务攻击等突发事件时，组织专业技术团队，提供7*24小时远程、电话、邮件及现场等方式应急响应服务，并提供应急响应报告。 **服务期限：自签订合同之日起3年**	1 项
7	定制化本地培训服务	1. 提供网络安全培训包含安全意识培训、安全技术培训、管理体系培训等。 2. 提供额外的培训服务：包括提供每年一次针对全体工作人员的网络安全意识培训，培训内容包含网络安全相关法律普及和解读、国内外网络安全形势、常见网络攻击手段、个人网络威胁防范手段等；提供2个CISP注册信息安全专业人员认证考试名额，CISP为国内信息安全领域内的权威证书，获取该证书能够让贵方信息技术人员系统的学习网络安全领域知识，有助于提高贵方网络安全技术人员的技术能力，更好的服务于信息安全岗位；提供5名全国计算机技术与软件专业技术资格（水平）考试中级、高级工程师网络培训课程。 **服务期限：自签订合同之日起3年**	1 项
8	售后服务	1.提供 7*24 热线服务，对用户提出的信息安全等级保护问题给予及时、专业的解答； 2.技术问题解答、咨询和规划等，通过热线、即时通讯、EMAIL 等方式与用户进行在线服务；	

二、合同总价款：

合同总价：人民币 525800.00 元 （大写：伍拾贰万伍仟捌佰元整）。

三、质量要求或服务标准，乙方对质量负责的条件和期限：

1、根据国家相关规范要求开展信息系统等级保护测评工作，并向招标人提出相应的整改方案与措施。

2、等保测评服务期两年（现网安全等级保护认证证书到期之日前 3 个月起，每年开展一次安全等级测评）（不包含甲方整改时间）

四、服务约定：

1、服务完成时间： 按照招标要求：等保测评服务 2 年期，安全服务 3 年期。

2、服务地点： 甲方指定地点 。

3、服务方式： 上门检测/远程检测服务。

五、验收标准、方法：（需提供三份验收资料）

1、提交安全巡检报告。

2、提交安全保障月报。

3、提交安全管理制度及培训计划。

六、结算方式及期限：

合同签订后支付 10%，完成第一次等保测评后，支付 50%，完成第二次等保测评后，支付 40%。

七、免费质保约定：

河南省鼎信信息安全等级测评有限公司为保证项目的售后质量保障，特设置了 24 小时的电话服务，以便及时的相应、回馈客户的信息安全咨询需求，及协助客户对安全方面的疑难问题的解决提供技术指导。

分别为工作时间段的服务热线，由专人的 24 小时手机支持！便于及时的联系沟通，及协调相关的资深工程师及时的为客户解决疑难问题。

八、售后服务承诺（包括服务的内容、方式、响应的时间、电话、质保期满结束后的维保等相关内容）

河南省鼎信信息安全等级测评有限公司在郑州大学国家超级计算郑州中心网络安全基础设施提升项目（标包二）中，将组建专业的**技术服务和项目管理团队**，致力于为郑州超算中心提供不止于采购需求的网络安全服务，项目服务团队人员配置及分工如下：

项目团队人员分工			
1	项目总体统筹	项目经理	郑真真
2	等保测评及安全整改服务团队	项目负责人	王新磊
		高级测评师	王新磊
			陈宇
			冯斌斌
			杨江涛
		中级测评师	齐琳
			张璐璐

			曹瑞军
		初级测评师	卢飞廷
			段昌乐
			王瑞升
3	安全巡检服务团队	高级工程师	韩培杰
		中级工程师	焦天恩
		中级工程师	龚青松
4	信息安全管理制度服务团队	高级测评师、博士	陈宇
		高级工程师	潘伟
		中级工程师	曹瑞军
5	应急响应服务团队	高级工程师	韩培杰
		中级工程师	王瑞升
		初级工程师	李露露
		初级工程师	王兵兵
6	定制化安全培训服务团队	管理体系培训	陈宇
		安全知识体系培训	潘伟
		安全意识培训	卢飞廷
		网络攻防实训	王瑞升、韩培杰

项目服务内容汇总如下：

1. 等级保护测评服务：在服务期限内，为客户指定的3个（二级）系统、2个（三级）系统，在网安全等级保护认证证书到期之日前3个月起，按照网络安全等级保护2.0测评标准，每年开展一次安全等级测评，并完成信息系统的测评、整改及定级、备案工作；
2. 等保安全整改服务：依照《信息安全等级保护安全建设整改工作指导意见》，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，对信息系统总体信息安全管理和技术方面现状进行全面的分析，制定网络安全等级保护安全建设整改方案，**整改方案同时考虑本项目标包一所采购网络安全设备类型与功能特性，协助设备供应商完成设备部署**

及策略配置；

3. 系统安全保障服务：服务期内，针对指定系统部署网络安全技术工具，提供安全服务保障，针对常见的注入攻击、跨站攻击、WEBSHELL上传、CC攻击、漏洞利用等攻击手段及时发及时阻断；每月出具安全月报；提供专业技术人员以7*24小时远程、电话、邮件及现场等方式提供应急响应支持；
4. 安全巡检服务：在服务期内，组织现场巡检人员2-3人，通过人员访谈、现场勘查、文档查看等方式，利用工具扫描、人工审计、基线检查、配置分析等方式，对路由器、交换机、防火墙、服务器、数据库、存储、中间件等信息资产，提供每月一次的安全巡检服务，并提供巡检总结报告；
5. 信息安全管理制度服务：以等保2.0管理制度要求为基准，结合ISO/IEC 27001、**《网络安全法》**、**《关键信息基础设施保护条例》**等法律法规，梳理郑州超算中心现有安全管理制度，完成差距分析、安全制度框架构建、安全管理制度编写与改进等一系列服务；
6. 应急响应服务：在服务期内，协助郑州超算中心建立安全应急预案，在中心遇到重大安全事件如网络入侵、大规模病毒爆发、遭受拒绝服务攻击等突发事件时，组织专业技术团队，提供7*24小时远程、电话、邮件及现场等方式应急响应服务，并提供应急响应报告；
7. 定制化培训服务：提供面向技术主管与管理层的管理体系培训和网络攻防实训等培训内容，满足组织超算中心培训服务要求；

除以上服务内容之外，我司额外提供以下增值服务与措施：

1. 向贵方提供有关测评设备的数据资料，具体包含：物理环境数据、通信网络数据、区域边界数据、计算环境数据、安全管理中心数据等数据资料；
2. 提供额外的网络安全相关的培训服务，具体包含：
   1）提供每年一次针对全体工作人员的网络安全意识培训，培训内容包含网络安全相关法律普及和解读、国内外网络安全形势、常见网络攻击手段、个人网络威胁防范手段等；
   2）提供2个CISP注册信息安全专业人员认证考试名额，CISP为国内信息安全领域内的权威证书，获取该证书能够让贵方信息技术人员系统的学习网络安全领域知识，有助于提高贵方网络安全技术人员的技术能力，更好

的服务于信息安全岗位；

3）提供5名全国计算机技术与软件专业技术资格（水平）考试中级、高级工程师网络培训课程；

3. 提供3个河南鼎信数据安全、网络安全方向实习岗位名额。

针对以上所列服务内容和措施，我公司承诺，以最好的质量标准认真贯彻和执行，满足国家超级计算郑州中心网络安全基础设施提升项目要求，助力客户完成项目建设工作。

序号	姓名	职务	职称	职责	联系电话
1	鼎信	客服	\	综合服务热线	0371-55958679/80
2	王新磊	项目负责人	高级	项目进度、质量总负责、应急咨询	13598802916
3	陈宇	培训讲师	高级	项目实施总负责、应急响应、应急处置	18637101827
4	齐琳	项目组长	中级	网络层面(应急响应、应急处置)	18697322185
5	张璐璐	质量负责人	中级	安全咨询	18539269815
6	李名博	售后经理	\	渗透测试	18539573607
7	卢飞廷	应急保障专员	初级	应急支援(应急响应、应急处置)	15638216622
8	郑真真	销售总监	\	商务事务协调	15516986068

九、履约担保

承包人提供履约担保的形式：以现金或转账的方式提供；

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无息退还。

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：协商和解，如双方协商不成，可将争议交由有管辖权的人民法院处理。

十二、其它约定事项：d

十三、本合同未尽事宜双方协商可补充之。

十四、本合同正本贰份、副本捌份，发包人与承包人各执肆份，报送招标代理机构贰份。

十五、本合同自签定之日起生效，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：郑州市高新区科学大道 100 号

电话：0371-67781128

开户银行：工商银行郑州中苑名都支行

户名：郑州大学

帐号：1702021109014403854

签定日期：2022.12.15

2023.2.14

乙方（盖章）：河南省鼎信信息安全等级测评有限公司

法定代表或代理人：张小军

单位地址：郑州市金水区东风路南文博东路东 4 号楼 5 层 502、503 号

电话：0371-55958679

开户银行：中国建设银行股份有限公司郑州农科路支行

户名：河南省鼎信信息安全等级测评有限公司

帐号：4100 1507 0100 5020 6723

签定日期：2022.12.15

2023.2.14

签约地点：郑州大学

第五章 采购需求及项目概况

标包二要求

序号	服务项	服务内容及要求
1	等保测评服务	测评范围：指定3个系统（二级）、2个系统（三级）； 服务期限：两年（现网安全等级保护认证证书到期之日前3个月起，每年开展一次安全等级测评） 服务内容：按照网络安全等级保护2.0测评标准进行安全等级测评； 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、安全计算环境和安全管理中心等五个方面的安全测评； 安全管理测评：安全管理机构、安全管理制度、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控制测评； 在安全等级测评过程中，每个工作阶段、流程、内容及成果交付严格遵循《信息安全技术 网络安全等级保护测评要求》和《信息安全技术 网络安全等级保护测评过程指南》文件，根据本项目信息系统已完成的定级备案安全等级，开展相应级别的安全等级测评工作，根据测评结果出具相应的单项和整体测评报告，测评报告需得到项目单位的确认，并报送网安部门。测评报告编制的内容及格式严格遵照《网络安全等级保护测评报告模版（现行版）》进行； ★服务要求：要求服务商根据 《网络安全等级保护基本要求》开展信息系统等级保护测评，并完成信息系统的测评、整改及定级、备案工作；测评技术团队符合《网络安全等级保护测评机构管理办法》对测评机构和测评人员管理的要求，供应商必须具备公安部第三研究所颁发的网络安全等级测评与检测评估机构服务认证证书，项目负责人由公安部培训考核认证通过的网络安全高级等级测评师承担，通过信息安全专业认证、具备良好的教育背景、受过专业的技术培训、拥有丰富的网络安全服务工作经验，对网络安全等级测评过程中可能会面临的各类技术问题及时提供解决方案。
2	等保安全整改服务	服务要求：依照《信息安全等级保护安全建设整改工作指导意见》，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，对信息系统总体信息安全管理和技术方面现状进行全面的分析，制定网络安全等级保护安全建设整改方案，方案内容包含但不限于：网络安全背景、政策与技术标准依据、当前风险分析、安全需求分析、总体安全策略、安全建设整改技术方案设计、安全建设整改管理体系设计、信息系统安全产品选型及技术指标建议、安全建设整改项目实施计划、项目预算，整改后可能存在的其他问题。
3	安全保障服务	★系统保障服务内容：服务期内，针对指定系统提供安全服务保障，针对常见的注入攻击、跨站攻击、WEBSHELL 上传、CC 攻击、漏洞利用等攻击手段及时发及时阻断；每月出具安全月报；提供专业技术人员以 7*24 小时远程、电话、邮件及现场等方式提供应急响应支持； 服务期限：自签订合同之日起 3 年 服务工具要求： 1、部署环境要求：管理后台：管理后台为B/S架构，支持所有操作系统和主

		流浏览器的访问； 2、支持Windows、Linux、红旗、中标麒麟等全系列操作系统，通用WEB容器支持，支持IIS、nginx、Apache、Tomcat、Weblogic、WebSphere、东方通、jboss全部版本插件防护； 3、SQL注入防护、XSS跨站脚本防护、漏洞利用攻击防护可根据不同检测对象（URL、Cookie、Post）进行具体防护规则的配置（开启与关闭）；禁止下载特定类型文件，可自定义设置禁止下载的特定文件类型；终端浏览实时防护可自定义设置网页木马的文件类型，将对设置列表中的网页类型进行基于行为的木马实时检测；HTTP相应内容保护则针对自定义列表中的错误页面返回类型进行错误页面的替换与跳转，以防止因HTTP错误页面泄露系统、数据库等重要敏感信息； ★4、支持堡垒锁防护，将整个磁盘除例外目录和例外文件格式外，全部文件设置为只读模式；（提供功能截图） ★5、采用实时应用程序自我保护（RASP）技术，实时监测并拦截漏洞攻击。能够在运行时结合上下文采取相应的保护方案。实现对应用及系统的动态监控与防御，大幅度降低误报率；（提供功能截图） ★6、支持基于沙箱的WEBSHELL查杀技术，下一代WEBSHELL检测技术，污点传播理论与沙箱技术，取代传统基于特征码的查杀技术，支持ASP、ASPX、PHP、JSP等常用WEB脚本语言，支持对于加密及变形的WEBSHELL有效查杀；（提供功能截图） 7、“登录防护”功能，针对Windows及Linux操作系统的远程登录进行限制及防护，用户可对“用户名”、“IP地址范围”、“时间范围”进行具体设置，并通过选择“允许登录”、“禁止登录”等相应的处理方式进行防护。 8、具有防暴力破解技术，能有效防御针对RDP、SSH服务的暴力破解。 9、“服务器巡检”功能，可以巡检webshell、二进制后门、弱口令3个维度。巡检支持定时巡检，Webshell巡检支持自定义巡检路径、自定义巡检文件类型；弱口令巡检支持自定义弱口令字典；
4	安全巡检服务	服务要求：服务期内提供安全巡检服务，巡检现场人员1-2人，每月1次； 服务期限：自签订合同之日起3年 ★服务内容：巡检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。
5	信息安全管理制度服务	★服务要求：安全管理制度服务，以等保2.0管理制度要求为基准，结合ISO/IEC 27001，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，并修订或编写必需的信息安全管理制度，提升超算中心的安全管理水平。
6	应急响应服务	★服务要求：要求服务技术团队善于发现系统漏洞，具备CNVD原创漏洞证书；擅长及时判断安全事件级别，进行紧急分析处理、灾难恢复和入侵追踪和取证，由至少2名具备信息安全保障人员认证证书（安全运维专业级）的技术人员提前收集现场系统情况，为后续应急做技术准备；由至少2名具备信息安全保障人员认证证书（应急服务专业级）的技术人员在发生安全事件时，两小时内提供现场应急响应； 服务期限：自签订合同之日起3年 服务内容：建立安全应急预案，遇到重大安全事件如网络入侵、大规模

		病毒爆发、遭受拒绝服务攻击等突发事件时，提供专业技术人员以7*24小时远程、电话、邮件及现场等方式提供应急响应支持，且快速恢复系统的保密性、完整性和可用性，确定安全威胁的破坏严重程度，阻止和降低安全威胁带来的影响，分析原因并提供相应的解决方案。
7	定制化本地培训服务	服务期限：自签订合同之日起3年 ★服务内容：1、面向技术主管与管理层的管理体系培训：对技术主管和管理层的培训重点是网络安全知识体系和安全意识，在网络安全知识体系的基础之上关注降低风险的对策。 2、网络攻防实训：针对常见的网络攻防技术手段，组织动手实践，让培训对象深刻理解网络攻防的基本理论，掌握常用的网络攻防技术手段和工具软件，具备处理常规安全事件的能力。