**LX25042浙江海洋大学信息化建设与管理中心网络安全运营服务采购项目**

**采购（报价）文件**

**（竞价采购）**

**竞价编号：\*\*\*\*\*\*\*\*\*\*\*\***

**报价单位：\*\*\*\*\*\*\*\*\*\*\*\***

**联 系 人：\*\*\*\*\*\*\*\*\*\*\*\***

**联系电话：\*\*\*\*\*\*\*\*\*\*\*\***

**日 期：2025年\*\*月\*\*日**

编制：浙江海洋大学采购中心

**竞价采购填报要求**

1、本采购文件（以下简称“文件”）作为供应商在政采云竞价系统报价的必要附件。供应商报价除满足政采云系统要求外，还需满足本文件的所有要求，并承诺响应后上传。

2、供应商报价时需按要求对商品进行响应，货物（或服务）名称、品牌及型号、价格需与文件上填报相一致，否则视为响应无效。本文件价格单位为元，如有小数，需保留小数点后两位。

3、供应商需核对报价商品是否符合项目的技术参数要求，符合技术参数要求的需在供应商响应处填写“响应”或填写技术要求对应内容。若条款要求中为“不小于”“不大于”“≥”“≤”“至少”等不确定参数时，供应商响应需填写“响应”并明确有关参数。响应内容不符合要求，未按要求响应（空白），“不响应”或填写与文件要求无关的内容，均视为报价无效。

4、文件“其他事项”栏作为供货商供货（或提供服务）的补充内容由供应商自行填报，其他事项栏填写不够的也可以附件形式另行附加材料。补充内容不得与本文件其他条款和内容相背或冲突，否则我方有权不予采纳并将视作报价无效处理。

5、文件“附件”为供应商资质或商务响应的支撑文件，在报价时需一并上传附件，否则视为报价无效。

6、供应商需对报价的材料或响应内容进行承诺，并签字盖章，未按要求的视为报价无效。

7、报价材料（含附件）各页均需加盖公章或骑缝章，签章文件扫描后以PDF格式添加到报价系统的附件中（文件的命名形式为：采购项目名称+报价文件+企业名称；附加的证明文件或材料命名形式为：报价文件附件）。

8、本次竞价结果需供应商报价三家（含）以上且为有效报价时竞价有效，采购人选择符合要求的最低报价供应商作为预成交供应商。（1）采购人通过评估政采云系统排名前三的供应商，若存在报价不符或响应虚假、后期供货（或服务）不及时或货物（或服务）不符合要求的等不满足采购文件要求的情况，采购人有权选择符合要求排名次低位的供应商作为成交供应商。（2）若系统排名前三的供应商均不满足采购文件要求，采购人有权重新组织采购，或竞争性谈判或磋商方式确定供应商。（3）若经过两轮公开竞价无效或仍不能确定供应商的，采购人可采用单一来源、竞争性谈判或磋商方式确定供应商。

9、以下情况采购人有权处理：（1）如果本次采购的货物为国家规定的政府采购节能产品、环保产品目录中的商品，供应商报价商品不符合上述要求的，将视作无效报价处理。（2）为推进建设资源节约型、环境友好型社会，采购人有权优先采购环境友好、节能低耗和易于资源综合利用的原材料、产品和服务。（3）供应商合同履行阶段如有存在违背采购法规和政策情况，按《浙江海洋大学合同履行异常管理细则》要求处理。

10、报价人对技术参数有不明之处可联系需求人电话：沈老师17816009205（限技术咨询）。

**项目联系和质疑：**对项目或文件要求有疑问或质疑的致电或邮件联系杜老师，电话/ 传真：0580-8180378；邮箱：627195050@qq.com；地址：浙江舟山市定海区临城街道海大南路1号。

1. **供应商参与报价必要条件：需为政采云供应商。**可通过政采云[网址](http://www.zcygov.cn）供应商。)**[www.zcygov.cn](http://www.zcygov.cn）供应商。)**[注册或](http://www.zcygov.cn）供应商。)通过**浙江政府采购网（https://zfcg.czt.zj.gov.cn/）**“用户入驻”栏按要求进行供应商登记并注册。
2. **采购信息获取及报价途径：**①**政采云（前台）—行业馆—科研馆**—**极速竞价**在**“最新竞价”**中搜索项目名称或“浙江海洋大学”进行信息获取或报价（报价时确保为登录状态）。②**政采云（登录状态）—交易中心—竞价管理（点选“未响应”）**进行搜索报价。
3. **报价商品需为已发布商品或已上架待发布商品。**商品报价或竞价相关操作问题可咨询政采云相关工作人员（进QQ群，群号698591622）。相关操作视频也可在政采云“采云学院”选择学习。

**特别说明：以下为采购人的友情提醒，凡涉及政采云账号注册或报价操作事宜请联系政采云公司。**

1. **商品（服务）类型和报价**

| **序号** | **商品名称** | **商品品牌及型号** | **数量/单位** | **单价限价（元）** | **单价报价****（元）** | **金额（元）** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | MSS安全托管服务 |  | 30个 | 4000 |  |  |
| 2 | 重保服务 |  | 7人天 | 1000 |  |  |
| 3 | 敏感数据泄露监控服务 |  | 1次 | 10000 |  |  |
| 4 | 钓鱼演练服务 |  | 1次 | 6000 |  |  |
| 5 | 渗透测试服务 |  | 1次 | 8000 |  |  |
| 6 | 应急响应服务 |  | 1年 | 5000 |  |  |
| 7 | 主机漏扫服务 |  | 4次 | 3000 |  |  |
| 8 | 应用漏扫服务 |  | 4次 | 3000 |  |  |
| **合计总价：小写 元，大写 圆整。** |  |

1. **技术参数要求**

| **序号** | **商品名称** | **技术要求** | **供方响应** |
| --- | --- | --- | --- |
| （一） | MSS安全托管服务 | 期限及频率：1年服务期，7\*24小时 |  |
| 服务范围：深信服安全运营中心接入学校现有深信服的态势感知平台、下一代防火墙、终端安全EDR等组件进行联动，基于现有的网络安全设备及深信服安全运营中心、专业技术团队对30个主机资产开展7\*24小时MSS安全运营服务。 |  |
| 服务内容 | 1、资产识别与梳理：借助安全工具对学校资产进行识别和梳理，并在后续服务过程中根据识别的资产变化情况触发资产变更等相关服务流程，确保资产信息的准确性和全面性。结合安全工具发现的资产信息，首次进行服务范围内资产的全面梳理（梳理的信息包含支撑业务系统运转的操作系统、数据库、中间件、应用系统的版本，类型，IP地址；应用开放协议和端口；应用系统管理方式、资产的重要性以及网络拓扑），并将信息录入到安全运营平台中进行管理；当资产发生变更时，安全专家对变更信息进行确认与更新。 |  |
| 1. 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、mysql、tomcat等基线配置核查：检查支撑信息化业务的主机操作系统、数据库、中间件的基线配置情况，确保达到相应的安全防护要求。检查项包含但不限于帐号和口令管理、认证、授权策略、网络与服务、进程和启动、文件系统权限、访问控制等配置情况。蠕虫病毒事件：需确认文件是否被感染，定位失陷的代码并进行修复针对漏洞利用攻击行为、Webshell上传行为、Web系统目录遍历攻击行为、SQL注入攻击行为、信息泄露攻击行为、口令暴力破解攻击行为、僵尸网络攻击行为、系统命令注入攻击行为及僵尸网络攻击行为进行分析评估，判断攻击行为是否成功以及业务风险点失陷主机分析：需对失陷主机进行分析研判（如后门脚本类事件），并给出修复建议。潜伏威胁分析：需分析内网主机的非法外联威胁行为，判断是否存在潜伏威胁，并给出解决建议。含：对外攻击、APT C&C通道、隐藏外联通道等外联威胁行为。 |  |
| 3、问题处置对发现的问题进行处置，包含内网脆弱性问题，病毒类事件，入侵行为，勒索、挖矿类事件等。 |  |
| 4、脆弱性管理（1）脆弱性扫描与验证：提供不少于每月一次针对服务范围内的资产的系统脆弱性和Web漏洞进行全量扫描，并针对发现的脆弱性进行验证，验证脆弱性在已有的安全体系发生的风险及分析发生后可造成的危害（2）优先级排序：提供客观的修复优先级指导，不能以脆弱性危害等级作为唯一的修复优先级排序依据。排序依据包含但不限于资产重要性、漏洞等级以及威胁情报（漏洞被利用的可能性）三个维度（3）脆弱性验证：提供脆弱性验证服务，针对发现的脆弱性问题进行验证，验证脆弱性在已有的安全体系发生的风险及分析发生后可造成的危害。针对已经验证的脆弱性，自动生成工单，安全专家跟进修复状态，各个处理进度透明，方便学校清晰了解当前脆弱性的处置状态，将脆弱性处理工作可视化（4）针对存在的漏洞提供修复建议，能够提供精准、易懂、可落地的漏洞修复方案（提供脆弱性修复方案样本，需包含多种修复方案以及修复过程中可能引发的其他问题的解决方案）(5)服务催单：针对服务平台生成的工单，学校可按需催单，用户可在服务平台上采用邮件等方式提醒安全专家加快协助处置，督促第一时间处理（6）脆弱性复测：需提供脆弱性复测措施，及时检验脆弱性真实修复情况。（7）脆弱性状态总览：对发现的脆弱性建立状态总览机制，自动化持续跟踪脆弱性情况，清晰直观地展示脆弱性的修复情况，遗留情况以及脆弱性对比情况，使得学校可做到脆弱性的可视、可管、可控。（8）最新漏洞预警与排查：需实时抓取互联网最新漏洞与详细资产信息进行匹配，对最新漏洞进行预警与排查。预警信息中包含最新漏洞信息、影响资产范围。（9）最新漏洞处置指导：一旦确认漏洞影响范围后，安全专家提供专业的处置建议。 |  |
| 5、威胁管理（1）结合大数据分析、人工智能、云端专家提供安全事件发现服务：依托于安全防护组件、检测响应组件和安全平台，将海量安全数据脱敏，包括脆弱性信息、共享威胁情报、异常流量、攻击日志、病毒日志等数据，经由大数据处理平台结合人工智能和云端安全专家使用多种数据分析算法模型进行数据归因关联分析，实时监测网络安全状态,发现各类安全事件，并自动生成工单（2）实时监测网络安全状态，对攻击事件自动化生成工单，及时进行分析与预警。攻击事件包含境外黑客攻击事件、暴力破解攻击事件、持续攻击事件（3）实时监测网络安全状态，对病毒事件自动化生成工单,及时进行分析与预警。病毒类型包含勒索型、流行病毒、挖矿型、蠕虫型、外发DOS型、C&C访问型、文件感染型、木马型通过全网大数据分析，发现有境外黑客或高级黑客正在攻击，立即采取行动封锁黑客行为实时针对异常流量分析、攻击日志和病毒日志分析，经过海量数据脱敏、聚合发现安全事件。 |  |
| 6、事件管理（1）基于主动响应和被动响应流程，对页面篡改、通报、断网、webshell、黑链等各类严重安全事件用户可以在平台上直接发起服务咨询，云端进行紧急响应和处置（2）实时针对异常流量分析、攻击日志和病毒日志分析，经过海量数据脱敏、聚合发现安全事件。（3）针对分析得到的勒索病毒、挖矿病毒、篡改事件、webshell、僵尸网络等安全事件，通过工具和方法对恶意文件、代码进行根除，帮助学校快速恢复业务，消除或减轻影响加固建议指导：结合现有安全防御体系，指导进行安全加固、提供整改建议、防止再次入侵。 |  |
| 交付物：《安全服务运营报告》，报告频率：每周一次《首次威胁分析与处置报告》，报告频率：一次《事件分析与处置报告》，报告频率：按需触发，不限次数《安全通告》，报告频率：按需触发，不限次数《安全运营月报》，报告频率：每月一次《勒索风险排查报告》，报告频率：每季度一次《季度汇报PPT》，报告频率：每季度一次《年度汇报PPT》，报告频率：每年一次 |  |
| （二） | 重保服务 | 期限及频率：1年服务期内7个自然日 |  |
| 服务范围：托管学校信息化中心的全量资产 |  |
| 服务内容 在重要会议或重大活动（如两会、攻防演练等）期间，依托深信服MSS安全运营平台从网络层面、服务器层面、数据层面为用户构建全方面的重要敏感时期的安全保障服务。保障网络基础设施、重点网站和业务系统安全，提供全方位的安全防守建设咨询以及事前、事中、事后的全面安全建设托管服务，确保用户的业务系统能够在重大活动期间安全平稳运行。1.对失陷主机进行分析、对弱口令等脆弱性进行分析、对安全组件进行重保策略检查。2.监测方向包括外部攻击（Web攻击、系统漏洞攻击），横向攻击（爆破、高危端口扫描）以及外联攻击成功事件（如服务器被控制如cs外联事件或dns隧道外联事件等）。3.定时分析针对全网全方向进行日志分析并且定时推送分析情况。4.实时监测Web攻击成功事件以及常见常见黑客攻击成功事件，发现即实时预警并且协助闭环处置及加固。5. 保障结束，梳理本次保障发现的问题以及每日工作情况进行总结，输出重保总结报告。 |  |
| 交付物：《重保每日值守报告》《重保工作总结报告》 |  |
| （三） | 敏感数据泄露监控服务 | 期限及频率：1年服务期内1次 |  |
| 服务范围：以浙江海洋大学、\*.zjou.edu.cn等关键字从从暗网情报、代码泄露、敏感文件、黑产舆情、资产失陷五个维度排查互联网上是否存在浙江海洋大学的敏感数据泄露问题。 |  |
| 服务内容：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，排查互联网上是否存在浙江海洋大学的敏感数据泄露问题，降低数据泄露带来的业务影响和学校师生影响，减少监管单位通报压力，弥补用户在外部信息监控上的安全能力短板。根据学校提供的敏感数据关键字导入到后端的威胁情报信息收集平台，收集相关信息，高级安全服务专家会对平台发现的相关信息进行过滤和整理，输出针对用户的定制化互联网敏感数据泄露排查报告。为保证服务质量和水平，要求开展服务使用的平台或产品为网络安全应急服务国家级支撑单位提供。 |  |
| 交付物：《敏感数据泄露监控服务排查报告》 |  |
| （四） | 钓鱼演练服务 | 期限及频率：1年服务期内1次 |  |
| 服务范围：浙江海洋大学指定师生范围 |  |
| 服务内容：通过模拟黑客邮件、短信钓鱼的攻击手段，以“黑衣人”身份通过平台向浙江海洋大学教职工、学生的邮箱或手机号发送钓鱼信息，并对被钓鱼成功的安全意识薄弱职工进行风险预警提示。依托于自主研发的钓鱼服务平台，由钓鱼服务专家基于社会工程学原理，结合师生真实业务场景、邮件使用习惯和网络环境特征，通过伪造可信身份向教职工、学生发送精心制作、逼真的钓鱼信息，欺骗用户进行点击钓鱼链接、提交数据信息、下载以及运行钓鱼附件等风险操作，同时提供统计分析演练情况的数据，以此检测职工安全意识的强弱程度。 |  |
| 交付物：《钓鱼演练总结报告》 |  |
| （五） | 渗透测试服务 | 期限及频率：1年1次（一次包含四个业务系统） |  |
| 服务范围：针对浙江海洋大学统一身份认证等4个系统开展1次模拟黑客攻击行为通过远程或本地方式对信息系统进行非破坏性的入侵测试，查找针对应用程序的各种漏洞。 |  |
| 服务内容：在可控的前提下进行最贴近于真实攻击的漏洞挖掘，弥补仅仅使用安全产品对系统分析的不足，通过渗透测试可以以攻击者的视角发现一些隐性存在的风险点或安全漏洞，1、在保证学校信息系统正常运行前提下，模拟黑客攻击行为通过远程或本地方式对信息系统进行非破坏性的入侵测试，查找针对应用程序的各种漏洞，帮助学校了解应用系统当前的安全状况，发现在系统复杂结构中的最脆弱链路并针对安全隐患提出解决办法，切实保证信息系统安全2、应在得到用户授权后方可开始实施渗透工作。3、渗透测试人员应在学校授权许可的情况下以目标业务系统为跳板进行横向渗透，发掘更深层次的漏洞并展现漏洞被利用后的危害 4、应编写渗透测试报告并提交给学校，报告应该阐明招标方业务系统中存在的安全隐患以及专业的漏洞风险处置建议现场服务工程师应具备应具备PMP、CISAW、ISO27001、ISO20000、CCSK、CISP资质（满足2项即可） |  |
| 交付物：《渗透测试报告》 |  |
| （六） | 应急响应服务 | 期限及频率：1年服务期，按实际情况开展 |  |
| 服务范围：浙江海洋大学网络安全重大事件 （对标国家标准 II 级及 III 级事件） |  |
| 服务内容：应急响应服务是指当发生外部黑客入侵、数据泄露、木马病毒等突发安全事件时，提供包括事件检测与分析、风险抑制、问题处置、协助业务恢复的服务，能够协助用户快速止损，最大化降低安全事件带来的影响。或者配合用户针对指定业务系统存在的漏洞进行测试工作。投标方应在招标方遇到重大或突发事件后按照要求的服务响应级别采取相关的措施和行动。帮助招标方正确应对安全事件，降低安全事件带来的损失和影响，并将业务以及网络恢复到正常状态。本次应急响应服务包含但不限于以下几类安全事件：1.WEB安全事件针对B/S类信息系统或网站遭受恶意入侵，利用网站进行反动信息、赌博、黄色等信息发布，传播危害国家安全、社会稳定和公共利益的内容的安全事件，包括但不限于：篡改、暗链、挂马、Webshell等2.恶意程序事件针对遭受的各类恶意程序事件进行快速处置，包括不限于病毒事件/木马事件、蠕虫事件、僵尸网络事件、勒索病毒事件、挖矿病毒事件等 3.网络攻击事件针对学校由于信息系统的配置缺陷、协议缺陷、程序缺陷，造成的信息系统异常的安全事件进行应急响应4.信息破坏事件针对学校信息系统中的信息被篡改、假冒、泄漏、窃取等而导致的信息安全事件进行应急响应，包括但不限于系统配置遭篡改、数据库内容篡改、网站内容篡改事件、信息数据泄露事件等现场服务工程师应具备应具备PMP、CISAW、ISO27001、ISO20000、CCSK、CISP资质（满足2项即可） |  |
| 交付物：《应急响应报告》 |  |
| （七） | 主机漏扫服务 | 期限及频率：1年服务期内每季度1次 |  |
| 服务范围：托管学校信息化中心的全部主机资产 |  |
| 服务内容：定期提供对托管学校信息化中心的全部主机漏洞检测，对发现的漏洞进行分析研判，提出有效的修复建议或解决方案。服务工具要求不限制扫描地址、拥有最新的规则库。要求使用工具为国内知名安全厂商品牌的产品（品牌厂家为CNNVD技术支撑单位）。 |  |
| 交付物：《主机漏洞扫描报告》 |  |
| （八） | 应用漏扫服务 | 期限及频率：1年服务期内每季度1次 |  |
| 服务范围：托管学校信息化中心的全部web应用系统资产 |  |
| 服务内容：定期对托管于学校信息化中心的信息系统提供应用漏洞检测，对漏洞扫描结果提供专业有效的整改建议方案，第一时间将发现的信息系统漏洞告知学校并及时协助用户修复；对于涉及到源代码级别的漏洞通知信息系统主办单位，并跟踪漏洞修复进程，直至完成修复漏洞；同时对漏洞的修复情况进行验证。服务工具要求不限制扫描地址、拥有最新的规则库。要求使用工具为国内安全厂商品牌的产品（品牌厂家为CNNVD技术支撑单位）。 |  |
| 交付物：《应用漏洞扫描报告》 |  |

1. **商品价格及售后服务**

 1、因MSS安全托管服务、重保服务等均基于深信服安全运营中心的平台、技术团队及我校现有深信服安全设备提供原厂安全运营服务，故要求供应商在合同签订后须提供针对本项目原厂售后服务承诺函原件，否则视为服务内容无法交付。

2、如发生重大网络安全事件，供应商应急响应服务应在接到学校需求电话后，必须在30分钟内响应。如学校需要现场技术服务支撑的，需在4个小时内到达现场，如无法履约按合总同价的1％/次作为赔偿，扣除合同余款。

3、供应商在发现学校托管的30个主机资产存在网页被篡改或敏感数据泄露等重大网络安全事故时，应立即启用应急响应机制，工作时间15分钟，非工作时间30分钟之内云端专家进行响应，首先由专家团队进行远程协助解决，如远程无法解决的则采用最快的交通工具上门处置。如未及时告知而造成重大影响，按合同价5%/次作为赔偿。

4、每次对系统进行安全评估、安全扫描、渗透测试之前必须要先提供相应的技术方案与学校方技术人员充分沟通，以确保系统的安全运行。

5、进行任何渗透测试，需要在学校方许可的时间、环境下由经验丰富的专业技术人员进行。

6、实施过程中应尽可能小的影响系统和网络的正常运行，做好备份和应急措施，不能对浙江海洋大学应用系统的正常运行产生影响，包括系统性能明显下降、网络拥塞、服务中断等，如无法避免出现这些情况应先停止项目实施，并向浙江海洋大学书面详细描述。

7、供应商所使用的信息安全类工具软件（包括web应用漏洞扫描工具、主机漏洞扫描工具等）必须为正版产品，具有公安部销售许可证书，并进行详细说明。

8、供应商须对本次安全运营服务项目实施过程的数据和结果数据严格保密，未经学校方授权，任何机构和个人不得泄露给有和本项目有关的数据和文档移交业主方后全部销毁。

1. **安装及交付时间**

交付和安装时间为合同签订 10 日之内。要求在10日内接入深信服安全运营中心，并提供针对本项目原厂售后服务承诺函原件，否则视为无法履约并解除合同。

1. **付款方式和要求**

付款方式：合同签订后，完成安装与交付要求，1个月内预付合同金额的50%，服务期期满后1个月内，验收合格支付50%。

1. **其他事项**

（此处仅填写供应商额外提供需方的服务承诺，与本采购文件询价要求相左条款的其他说明视作无效说明。若无其他服务承诺的请填写“无”）

1. **附件**（填写附件名称，如企业营业执照、资质文件等另行要求的附加的附件名称。）

1．企业营业执照（有效期以内，并加盖公章）

2．其他需要提供的材料（本文件技术参数要求中打“▲”（若有）或采购文件中有特别要求需提供材料的条款项）

3．承诺书（见后附页）

**附件特别说明：**

（1）上文“附件”为供应商资质或商务响应的支撑文件，供应商在报价时需在上述“附件”清单中注明附加的附件具体名称，并在系统报价时将以上附件一并上传，否则视为报价无效。

（2）文件要求的附件材料若无范本，格式可按要求自拟。

（3）系统填报时，附加的证明文件或材料单独以PDF格式并命名为：“报价文件附件”上传。

**承 诺 书**

我公司在参加 **xxxxxxxxxxxxxxxx**（完整项目名称） 项目的政采云竞价（询价）采购活动中，郑重承诺如下：

1. 承诺遵守《中华人民共和国招标投标法》《中华人民共和国政府采购法》等法律法规及浙江海洋大学规章制度。

2.完全接受和满足本项目采购文件中规定的实质性要求。

3.我方承诺在本次竞价（询价）活动，不存在以下情况：

（1）和其他供应商存在同一人或者直接控股、管理、利益等有关联的，其他供应商参与同一合同项下的政府采购活动的行为。

（2）承诺绝对没有也不会向生产厂家提前报备本项目采购内容等影响本项目顺利实施的行为，且绝对不会直接或间接干预中标供应商的供货或服务。

若经贵方查出有上述情况，立即取消我方竞价（询价）资格并承担相应的法律职责，自愿同意在此后一年内不参与学校的采购活动。

4.我方一旦中标，将按规定及时与采购单位签订合同。承诺严格执行合同条款，凡进入浙江海洋大学的货物、服务项目等均有完备的手续。

**我方保证本项目提交的承诺内容真实可靠，如因存在虚假响应、提供虚假材料等恶意报价的情况，或中标后却无法履行合约等情况，愿意承担由此引起的一切后果和相应的法律责任。**

报价单位名称： （加盖公章）

联系人： （签 字）

联系电话：

日 期： 年 月 日