第三章 磋商项目技术、服务、商务及其他要求

（注：带“★”的参数需求为实质性要求，供应商必须响应并满足的参数需求，采购人、采购代理机构应当根据项目实际需求合理设定，并明确具体要求。带“▲”号条款为允许负偏离的参数需求，若未响应或者不满足，将在综合评审中予以扣分处理。）

3.1、采购项目概况

本次服务项目拟完成宜宾职业技术学院网络安全运维服务，对学院网络安全系统资产进行检测和风险评估，对发现的故障和隐患进行通报及协助整改，确保正常运行；遵照国家网络安全等级保护有关规定，健全和完善学院的网络安全管理制度体系；对于学院指定的核心业务系统，模拟黑客的攻击技术和漏洞发现技术，对系统的安全作深入的探测，发现系统最脆弱的环节。同时在关键时期提供线下值守确保学院信息化系统安全稳定运行，若遇重大事件，能够提供及时的应急技术保障和事件分析服务，确保学院各项业务工作安全稳定的开展。

3.2、服务内容及服务要求

3.2.1 服务内容

采购包 1：

采购包预算金额（元）: 530,000.00

采购包最高限价（元）: 530,000.00

序号	标的名称	数量	标的金额（元）	计量单位	所属行业	是否涉及核心产品	是否涉及采购进口产品	是否涉及采购节能产品	是否涉及采购环境标志产品
1	安全运维服务	1.00	530,000.00	项	其他未列明行业	否	否	否	否

3.2.2 服务要求

采购包 1：

标的名称：安全运维服务

参数性质	序号	技术参数与性能指标
	1	一、不间断网络安全保障： 1、组建 7*24 小时在线运维服务团队，实施不间断网络安全保障服务； 2、借助安全工具对用户资产进行全面发现和深度识别，首次进行服务范围内资产的全面梳理，并将信息录入到安全运营平台中进行管理，在后续服务过程中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； 3、每月针对服务范围内的资产的系统漏洞和 Web 漏洞进行全量扫描，并针对发现的漏洞进行验证，验证漏洞在已有的

		安全体系发生的风险及分析发生后可造成的危害； ▲4、提供客观的漏洞修复优先级指导，不能以漏洞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（提供脆弱性优先级排序截图，展示优先级排序情况）； 5、最新漏洞预警与排查：投标方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； 6、对发现的漏洞建立状态追踪机制，自动化持续跟踪漏洞情况，清晰直观地展示漏洞的修复情况，遗留情况以及漏洞对比情况，使得使用方可做到漏洞的可视、可管、可控； 7、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，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； ▲8、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。攻击事件包含黑客攻击事件、暴力破解攻击事件、持续攻击事件（供应商需提供安全事件（如暴力破解）的工单截图，截图内容需展示当前安全事件的处置状态并进行电子签章）； 9、每月主动分析攻击类的安全事件：通过攻击日志分析，发现持续性攻击，立即采取行动实时对抗，当用户无防御措施时，提供攻击类安全事件的处置建议； 10、安全专家根据安全事件分析的结果以及处置方式，根据用户授权情况按需对安全组件上的安全策略进行调整工作； 11、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，帮助使用方快速恢复业务，消除或减轻影响； ▲12、所有可导出报告支持按照自定义模块进行导出，可自定义模块必须包括但不限于事件管理、攻击威胁（外部攻击趋势、TOP5 攻击 IP 等）、脆弱性管理（漏洞、弱密码）。（供应商需提供服务平台支持上述服务报告自定义导出的平台功能截图并进行电子签章）； ▲13、支持面向采购人的安全态势展示，展示出当前采购人遭受的威胁事件信息以及脆弱性信息统计，并支持服务专家按照资产类别、威胁类型进行定制化筛选查看，能直观感受到采购人当前的风险态势情况。（供应商需提供服务平台漏洞表、事件表统计信息截图，并证明支持按照资产类别、威胁类型进行定制化筛选查看并进行电子签章）； 14、支持展示出当前工单数量和工单处置状态，使得使用方能详细查看服务处置过程，查看安全事件闭环效果，掌握当前专家服务进度，监督服务质量； 15、支持面向使用方的安全状态展示，展示出使用方的业务和用户安全状态信息，使得使用方能直观感受到当前的业务

		和资产安全状态； 16、为了保证安全监测的效果，安全服务平台应具备检测规则的自定义功能，以满足日益复杂的安全趋势所带来的安全需求； ▲17、投标方需为采购人提供的服务成果展示门户，应具备服务质量可视化展示，投标方能通过可视化的数据，清晰的了解安全专家的服务水平，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，以验证投标方所承诺的服务指标（供应商需提供服务成果展示门户中服务质量监控相关的截图并进行电子签章）； ▲18、云端服务平台应当支持对接采购人网络中已部署的主要安全设备，下一代防火墙、安全态势感知、服务器杀毒软件，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*24 小时的安全托管服务（供应商需提供承诺函，格式自拟，并进行电子签章）； ▲19、为了降低采购人因网络安全事件造成的损失和影响，按照国家标准对安全事件的分类分级指南，投标方提供的安全运营保障平台需要具备如下能力（供应商需提供平台能力承诺函，格式自拟，并承诺作为合同附件进行签署,并进行电子签章）： （1）从安全日志产生到事件通告，重大安全事件通告时间小于 30 分钟，一般事件的通告时间少于 1 小时； （2）高级威胁的处置完成时间少于 1 小时，一般威胁的处置完成时间少于 4 小时； （3）通告给采购人的各类安全事件的准确率不低于 99%； （4）所有安全事件的闭环处置比例达到 100%； （5）对信息资产发现的每一个高危可利用漏洞提供防护规则，防护率达到 99%； 20、对采购人≥100 个核心信息化资产（以 IP 地址为单位）提供 7*24 小时实时网络安全威胁监测预警与响应服务，同时对现有网络环境安全做实时监测保障，能够实时监测采购人信息化资产的网络安全状态； 21、服务提供方需为采购人提供不少于 2 周（14 天）7*24h 的重大活动时期网络安全保障服务，监测结果的通告频率不低于每 2 小时 1 次； 22、服务提供方需在重要保障前期为采购人提供不少 2 周的网络安全评估及加固服务，确保在重大活动开始前对现网安全隐患进行排查，具体开始时间由采购人指定； 23、投标方需借助安全工具对 IT 资产进行全面发现和深度识别，确保资产信息的准确性和全面性，便于重要保障期间快速定位安全风险和加固； ▲24、投标方在重要保障期间提供专业的威胁情报服务，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。应能支持对资产影响范围的自动监测与排查（供应商需提供服务平台或工具截图并进行电子签章）； 25、实时监测网络安全状态，重要保障期间，提供安全大数据分析平台和安全运营服务平台，对攻击事件自动化生成工单，及时进行分析与预警。攻击事件包含黑客攻击事件、暴力破解攻击事件、持续攻击事件、高级威胁事件等； ▲26、高级安全专家威胁狩猎，在重要保障期间提供高级安全攻防专家在线值守服务，在安全运营服务平台自动生成安全威胁工单的基础上每两个小时进行一次人工威胁狩猎，主动全面的分析全网安全日志信息，提高有效攻击事件的检出率，服务方须承诺安全攻击事件产生到发现时间≤30 分钟。（供应商需提供承诺函，格式自拟，并进行电子签章）； 27、在重要保障期间，服务提供方须提供高级安全专家对发现的安全攻击行为进行快速的源 IP 封锁或行为规则封锁，同时对安全组件上的安全策略进行动态调优工作，确保安全组件上的安全策略始终处于最优水平，实时动态的抵御攻击方的攻击行为； ▲28、高级威胁攻击源情报共享服务，在重要保障期间服务提供方利用专业的技术团队和服务工具，快速获取行业内发生的攻击源 IP 等威胁消息，并同步为用户提供高级威胁和攻击行为的提前预判和攻击行为封堵，提供安全服务平台支持批量下发封锁攻击源 IP(供应商需提供服务平台操作界面截图并进行电子签章）； 29、为保障重要保障期间对大量的攻击源 IP 封锁及风险排查工作，应能在服务平台上实现攻防专家之间共享攻击源并且支持重复源 IP 的自动去重，减少安全人员操作复杂度，提高防守对抗效率； 30、为保障重要保障期间尽可能减少对正常业务访问造成影响，安全运营服务平台应能支持对待封堵 IP 和用户资产 IP 进行自动比对，当安全人员欲封堵的 IP 与用户资产冲突时给出自动提示，避免人为误拦截； 31、在出现重大安全事件后，如果 2 小时内不能解决，应委派从业五年及以上安全服务专家 4 个小时内到达现场处理； 二、现场渗透测试服务： 1、采购人授权后，投标方应通过模拟黑客攻击行为通过本地或远程方式对目标对象进行非破坏性的入侵测试； 2、渗透测试应至少包括但不限于以下范围的漏洞：WEB 应用系统渗透、主机操作系统渗透、数据库系统渗透； 3、渗透测试内容包括但不限于：身份验证类、会话管理类、访问控制类、输入处理类、信息泄露类、第三方应用类； 4、投标方渗透测试人员应针对使用不同技术手段发现不同纬度的漏洞，并进行验证，形成记录和报告； 5、投标方渗透测试人员应在采购人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； 6、投标方应编写渗透测试报告并提交给采购人，报告应该阐明采购人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； 7、渗透测试服务个数为15个信息系统，服务交付物：《渗透测试报告》； 三、安全培训服务： 1、提供3次及以上网络安全培训服务，培训主题和培训时间由采购人确定； 2、培训期间，要求投标方使用自研的培训教材包、培训素材包； 3、服务交付物：《安全培训方案》《安全培训计划》《安全培训总结》《安全培训教材》； 四、安全报告： 1、入驻期间：交付物名称：《信息化资产全面风险分析与处置报告》，报告频率：一次； 2、日常运营期间： 2.1交付物名称：《安全日报》，报告频率：每日一次； 2.2交付物名称：《安全服务运营报告》，报告频率：每周一次； 2.3交付物名称：《综合分析报告/运营月报》，报告频率：每月一次； 2.4交付物名称：《季度汇报PPT》，报告频率：每季度一次； 2.5交付物名称：《年度汇报PPT》，报告频率：每年一次； 2.6交付物名称：《安全事件分析与处置报告》，报告频率：按需触发，不限次数； 2.7交付物名称：《安全通告》，报告频率：按需触发，不限次数； 3、攻防演习期间： 3.1交付物名称：《攻防演习日报》，报告频率：每天一次； 3.2交付物名称：《攻防演习值守总结报告》，报告频率：按重保次数提供； 4、重保期间： 4.1交付物名称：《安全日报》，报告频率：每天一次； 4.2交付物名称：《安全事件防守报告》，报告频率：按需触发，不限次数； 4.3交付物名称：《安全威胁通告》，报告频率：按需触发，不限次数； 五、现场运维保障： 1、委派两名专职现场网络安全运维人员，按照采购人工作时间按时到岗，接受采购人考勤监督。派驻人员需具备3年

以上网络安全管理工作经验，以及优秀的文案写作能力；

2、负责中心机房、服务器、网络设备、安全设备的巡检和维护，并做好机房巡检台账、设备管理台账记录；

3、协助管理不少于300个服务器资产、不少于25个信息系统，并做好系统管理台账；

4、负责安全感知平台、堡垒机、防火墙、VPN、日志审计、数据库审计、备份系统、防病毒系统等网络安全设施的监控和配置；

5、配合7*24小时在线运维服务团队，在发现风险后及时本地化处置安全风险；协助采购人完成公安、教育、网信等各级网络安全管理部门交办的任务；协助采购人完善网络安全制度，积极提出相关合理化建议；在重保期间实行7*24小时驻场网络安全保障；完成采购人交办的网络安全相关工作；

★六、考核标准：

1、考核标准表：

服务内容	扣分细则
不间断网络安全保障	1、因供应商保障不到位造成重要数据被窃取、篡改、破坏，以及系统被入侵等网络安全事件，每次扣10分； 2、因供应商保障不到位造成被各级网络安全管理部门通报，每次高危扣3分，中危扣2分，低危扣1分； 3、高危漏洞未在72小时内配合修复的，每次扣1分； 4、重要安全事件未在30分钟内通知采购人的，每次扣1分。
现场渗透测试服务	未能按要求完成信息系统渗透测试服务的，每少1个扣3分；
安全培训服务	未能按要求完成安全培训的，每少1次扣2分；
安全报告	未完成《安全培训教材》、《安全培训记录》、《攻防演习日报》、《攻防演习值守总结报告》、《安全事件防守报告》、《安全威胁通告》、《安全服务运营报告》、《首次威胁分析与处置报告》、《事件分析与处置报告》、《安全通告》、《综合分析报告/运营月报》、《季度汇报PPT》、《年度汇报PPT》等，每少一次扣1分；
驻场值守服务	1、驻场人员每人次缺勤1天扣1分，迟到或早退每人次扣0.5分； 2、违反保密条款，证据确凿的，每次扣5分； 3、未完成《中心机房巡检台账》扣2-5分； 4、未完成《中心机房访客登记》扣2分；

			5、未完成《设备管理台账》扣 2-5 分； 6、未完成《信息系统管理台账》扣 2-5 分； 7、未完成采购人安排的职责范围内的工作，证据确凿，并且没有正当理由的，每次扣 2-5 分；
		2、合同续签： 合同签订时间：一年一签。合同到期后两周内由采购人组织验收，按照 3.2.2 服务要求中第六条考核标准进行验收评审，验收评审分数≥80 分，视为满足续签条件，可续签本合同，续签不超过两年。 ★七、付款方式： 1、采购包 1：付款条件说明：合同签订后，达到付款条件起 30 日内，支付合同总金额的 30.00%。 2、采购包 1：付款条件说明：合同签订后一个月内完成不间断网络安全保障部署，以及所有网络安全设备配置，由采购人网络管理部门出具证明后，达到付款条件起 30 日内，支付合同总金额的 40.00%。 3、采购包 1：余款 30%作为考核绩效。按照 3.2.2 服务要求中第六条考核标准，如果考核分数≥80 分，考核绩效为合同金额的 30%；如果考核分数≥70 且<80 分，考核绩效为合同金额的 20%；如果考核分数≥60 且<70 分，考核绩效为合同金额的 10%；如果考核分数<60 分，考核绩效不予支付。考核绩效在验收合格后 30 天内支付。	

3.2.3 人员配置要求

采购包 1：

（1）为规范和促进本项目的正常实施和推进，成交供应商须针对本项目成立独立的项目组，安排足够专业技术人员参加本项目工作。（2）在项目组织机构中应明确各岗位的职责、任职资格，确保项目顺利实施。应配备有实际业务经验的项目负责人承担本项目的管理工作，配备项目核心技术团队及技术支持团队。

3.2.4 设施设备要求

采购包 1：

详见 2.2 服务要求（如涉及）

3.2.5 其他要求

采购包 1：

为保障本项目工作合力有序开展，供应商须提供详细完善的运维服务方案，包括：①安全运维管理；②安全运维告警；③安全运维事件响应；④安全运维审核评估；⑤安全基线及系统配置等内容。

3.3、商务要求

3.3.1 服务期限

采购包 1：

自合同签订之日起 365 日

3.3.2 服务地点

采购包 1：

采购人指定地点。

3.3.3 考核（验收）标准和方法

采购包 1：

参照《财政部关于进-步加强政府采购需求和履约验收管理的指导意见》(财库(2016)205 号)以及主管部门的相关要求进行验收。由采购人组织履约验收小组，开展项目验收工作，达到国家相关标准、行业标准、地方标准或者其他标准、规范要求为标准，按照《采购文件》、《响应文件》和双方签订的《采购合同》，对成交供应商履约情况进行验收，出具验收报告。

3.3.4 支付方式

采购包 1：

分期付款

3.3.5 支付约定

采购包 1：付款条件说明：合同签订后 ，达到付款条件起 30 日内，支付合同总金额的 30.00%。

采购包 1： 付款条件说明： 合同签订后一个月内完成不间断网络安全保障部署，以及所有网络安全设备配置，由采购人网络管理部门出具证明后 ， 达到付款条件起 30 日内， 支付合同总金额的 40.00%。

采购包 1：付款条件说明：验收合格后 ，达到付款条件起 30 日内，支付合同总金额的 30.00%。

3.3.6 违约责任及解决争议的方法

采购包 1：

合同发生争议，采购人与供应商应及时协商解决。也可由当地建设行政主管部门调解。调解不成时，双方当事人同意由项目所在地县人民法院仲裁委员会仲裁，未达成仲裁书面协议的，可向项目所在地县人民法院起诉。

3.4 其他要求

★1、因系统固化原因，3.3、商务要求中 3.3.5 支付约定不适用于本项目，支付约定以 3.2.2 服务要求中第七条付款方式为准。注：1）磋商采购文件第三章 3 商务要求均为实质性要求，供应商必须全部满足，不满足或不响应的作无效响应处理。2）磋商采购文件第三章 3.4 其他要求中标注“★”项的为实质性要求，供应商必须全部满足，不满足或不响应的作无效响应处理。