政府采购项目采购需求

采购单位：筠连县妇幼保健计划生育服务中心

所属年度：2024年

编制单位：筠连县妇幼保健计划生育服务中心

编制时间：2024年10月15日

一、项目总体情况

（一）项目名称： 等级保护测评及网络安全综合服务项目

（二）项目所属年度： 2024年

（三）项目所属分类： 服务

（四）预算金额（元）：780,000.00元，大写（人民币）：柒拾捌万元整

（五）项目概况：根据《中华人民共和国网络安全法》和国家关于信息安全等级保护相关要求，需要对筠连县中医医院、筠连县人民医院、筠连县妇幼保健院承载的相关信息系统开展信息系统等级保护测评工作，以指导安全整改，提高信息系统的安全防护能力。

（六）本项目是否有为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商：否

二、项目需求调查情况

依据《政府采购需求管理办法》的规定，本项目 不需要 需求调查 。

三、项目采购实施计划

（一）采购组织形式：分散采购

（二）预算采购方式：非公开招标

采购方式：竞争性磋商

（三）本项目是否单位自行组织采购：否

（四）采购包划分：不分包采购

（五）执行政府采购促进中小企业发展的相关政策

本项目不专门面向中小企业采购

注：监狱企业和残疾人福利单位视同小微企业。

（六）是否采购环境标识产品：否

（七）是否采购节能产品：否

（八）项目的采购标的是否包含进口产品：否

（九）采购标的是否属于政府购买服务：否

（十）是否属于政务信息系统项目：否

（十一）是否省属高校、科研院所科研设备采购：否

（十二）是否属于PPP项目：否

（十三）是否属于签订不超过3年履行期限政府采购合同的项目：是

履行期限：三年

四、项目需求及分包情况、采购标的

（一）分包名称：合同包一

1、执行政府采购促进中小企业发展的相关政策

1) 不专门面向中小企业采购

2、预算金额（元）：780,000.00，大写（人民币）： 柒拾捌万元整

最高限价（元）： 720,000.00，大写（人民币）： 柒拾贰万元整

3、评审方法：综合评分法

4、定价方式：固定总价

5、是否支持联合体投标：否

6、是否允许合同分包选项：否

7、拟采购标的的技术要求

1	**采购品目**	测试评估认证服务	**标的名称**	等级保护测评及网络安全综合服务项目
	数量	1.00	**单位**	项
	合计金额（元）	720,000.00	**单价（元）**	720,000.00
	是否采购节能产品	否	**未采购节能产品原因**	无
	是否采购环保产品	否	**未采购环保产品原因**	无
	是否采购进口产品	否	**标的物所属行业**	软件和信息技术服务业

标的名称：等级保护测评及网络安全综合服务项目

参数性质	序号	技术要求名称	技术要求内容（性能指标）
			采购数量、采购标的的功能标准、性能标准、材质标准、安全标准、服务标准以及是否有法律法规规定的强制性标准 （具体参数等） 一、项目概述 根据《中华人民共和国网络安全法》和国家关于信息安全等级保护相关要求，需要对筠连县中医医院、筠连县人民医院、筠连县妇幼保健院承载的相关信息系统开展信息系统等级保护测评工作，以指导安全整改，提高信息系统的安全防护能力。 二、项目范围目标及预算 1.安全等级测评项目的服务范围包括以下信息系统：

序号	信息系统名称	定级
1	HIS	三级
2	LIS	三级
3	PACS	三级
4	EMR	三级

分别于2024年、2025年、2026年按照项目备案要求提供三次测评服务。

2.由于该四套系统属于筠连县人民医院、筠连县中医医院、筠连县妇幼保健院共同使用，《信息系统安全等级测评报告》及相关资料将对各单位分别出具；在等保测评工作完成的基础上，每年为四套系统进行一次漏洞扫描及出具相应的漏洞扫描报告。

3.项目预算3年最高限价72万，每年24万元。

三、实施依据

本次测评项目实施需遵循以下依据：

1）中华人民共和国网络安全法；

2）中华人民共和国计算机信息系统安全保护条例（国务院第147号令）；

3）信息安全等级保护管理办法(公通字[2007]43号)；

4）网络安全等级保护基本要求(GB/T 22239-2019)；

5）网络安全等级保护测评要求(GB/T 28448-2019)；

6）其它国家、省、行业信息安全等级保护有关要求和标准。

四、项目主要内容

按照相关要求，对上述待测评的信息系统进行安全现状调研，通过现场测评发现安全问题，提出安全整改建议，待整改完成后实施安全复测，并针对每个信息系统分别出具《信息系统安全等级测评报告》，确保测评报告符合公安等主管部门等相关要求。实施单位为宜宾市筠连县人民医院、筠连县中医医院、筠连县妇幼保健院。

五、须提交的交付物

交付物将作为主要验收依据，包括但不限于：

序号	文档类型	文档名称
1	项目实施过程文档	测评方案、计划
2	项目实施过程文档	信息系统安全等级保护备案表
3	项目实施过程文档	安全整改建议方案
4	项目成果文档	各信息系统安全等级测评报告
5	项目成果文档	安全优化建议方案
6	其他要求的文档	根据采购人、公安等主管部门要求

六、具体工作任务

供应商须按照采购人要求，根据国家、省、行业项目的实施依据开展测评工作。

等级测评工作内容主要包括单元测评和整体测评，其中单元测评是对测评对象的物理安全、网络安全、主机安全、应用安全、数据安全及备份恢复、安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理等的逐项测评；整体测评是在单元测评的基础上，通过进一步分析信息系统安全保护功能的整体相关性，对信息系统实施的综合安全测评。系统测评包括初测与复测，在各类系统初测后供应商需要指导用户单位、开发商、集成商、设备厂商、安全服务商等进行整改，整改完成后进行复测并出具各系统的《等级测评报告》。

1.单元测评

（1）物理安全测评指标描述

物理安全测评将通过访谈和检查的方式测评信息系统的物理安全保障情况；在内容上，物理安全测评实施过程涉及10个工作单元，具体描述方法如下表所示：

序号	工作单元名称	工作单位描述
1	物理位置的选择	通过访谈物理安全负责人，检查机房等过程，测评机房的物理场所所在物理位置是否具有防震、防风和防雨等多方面的安全防范能力。
2	物理访问控制	通过访谈物理安全负责人，检查机房的出入口、分区域情况等过程，测评信息系统在物理访问控制方面的安全防范能力。

3	防盗窃和防破坏	通过访谈物理安全负责人，检查机房的主要设备、介质和防盗报警系统等过程，测评信息系统是否采取必要的措施预防设备、介质等丢失和被破坏。
4	防雷击	通过访谈物理安全负责人，检查机房的设计/验收文档等过程，测评信息系统是否采取相应的措施预防雷击。
5	防火	通过访谈物理安全负责人，检查机房的设计/验收文档，检查机房防火设备等过程，测评信息系统是否采取必要的措施防止火灾的发生。
6	防水和防潮	通过访谈物理安全负责人，检查机房的除潮设备等过程，测评信息系统是否采取必要措施来防止水灾和机房潮湿。
7	防静电	通过访谈物理安全负责人，检查机房等过程，测评信息系统是否采取必要措施防止静电的产生。
8	温湿度控制	通过访谈物理安全负责人，检查机房恒温恒湿系统，测评信息系统是否采取必要措施对机房内的温湿度进行控制。
9	电力供应	通过访谈物理安全负责人，检查机房的供电线路、设备等过程，测评信息系统是否具备一定的电力供应的能力。
10	电磁防护	通过访谈物理安全负责人，检查机房等过程，测评信息系统是否具有一定的电磁防护能力。

（2）网络安全

网络安全测评将通过访谈、检查和测试的方式测评信息系统的网络安全保障情况。主要涉及对象为网络互联设备、网络安全设备和网络拓扑结构等三大类对象，具体为：核心交换机、汇聚交换机、接入交换机等网络互联设备；入侵检测防御系统、防病毒网关和防火墙等网络安全设备；信息系统的整体拓扑结构。

在内容上，网络安全层面测评实施过程涉及7个工作单元，具体如下表所示网络安全测评实施内容表

序号	工作单元名称	工作单元描述
1	结构安全	通过访谈网络管理员，检查网络拓扑情况、抽查核心交换机、接入交换机和接入路由器等网络互联设备，测试系统访问路径和网络带宽分配情况等过程，测评分析网络架构与网段划分、隔离等情况的合理性和有效性。
2	访问控制	通过访谈安全员，检查防火墙等网络访问控制设备，测试系统对外暴露安全漏洞情况等过程，测评分析信息系统对网络区域边界相关的网络隔离与访问控制能力。
3	网络安全审计	通过访谈审计员，检查核心交换机、汇聚交换机、接入交换机和接入路由器等网络互联设备的安全审计情况等，测评分析信息系统审计配置和审计记录保护情况。

4	边界完整性检查	通过访谈安全员，检查边界完整性检查设备，接入边界完整性检查设备进行测试等过程，测评分析信息系统私自联到外部网络的行为。
5	网络入侵防范	通过访谈安全员，检查网络边界处的入侵检查设备IDS等过程，测评分析信息系统对攻击行为的识别和处理情况。
6	恶意代码防范	通过访谈安全员，检查网络防恶意代码产品等过程，测评分析信息系统网络边界和核心网段对病毒等恶意代码的防护情况。
7	网络设备防护	通过访谈网络管理员，检查核心交换机、汇聚交换机、接入交换机和接入路由器等网络互联设备，IDS和防火墙等网络安全设备，查看它们的安全配置情况，包括身份鉴别、权限分离、登录失败处理、限制非法登录和登录连接超时等，考察网络设备自身的安全防范情况。

（3）主机安全

主机系统安全测评将通过访谈、检查和测试的方式评测信息系统的主机系统安全保障情况。本次重点测评包括各系统服务器的操作系统和数据库。

在内容上，主机系统安全层面测评实施过程涉及7个工作单元，具体如下表所示：

序号	工作单元名称	工作单元描述
1	身份鉴别	对各主机服务器和终端设备相应操作系统或数据库的身份鉴别情况进行配置检查，测评分析被测系统主机的身份鉴别能力。
2	访问控制	检查各主机服务器和终端设备相应操作系统或数据库的访问控制设置情况，包括安全策略覆盖、控制粒度以及权限设置情况等，测评分析被测系统主机的访问控制能力。
3	安全审计	访谈安全审计员，询问主机系统的安全审计策略，查看安全审计配置是否符合安全审计策略；对审计相关资源是否进行了保护。
4	剩余信息保护	检查用户的鉴别信息存储空间，被释放或再分配给其他用户前是否得到完全清除；系统内的文件、目录等资源所在的存储空间，被释放或重新分配给其他用户前是否得到完全清除
5	入侵防护	检查入侵防范措施是否检测到对重要服务器进行入侵的行为，能够记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施；操作系统应遵循最小安装的原则
6	恶意代码防范	检查主机系统是否采取恶意代码实时检测与查杀措施，恶意代码实时检测与查杀措施的部署是否符合安全策略并统一管理。
7	资源控制	检查主要服务器操作系统，查看是否设定了终端接入方式、网络地址范围等条件限制终端登录并对CPU、硬盘、内存、网络等资源的使用情况进行监控，是否可以正确示警。

（4）应用安全

应用安全层面将通过访谈、检查和测试的方式测评信息系统的应用安全保障情况。本次重点测评HIS、LIS、PACS、EMR应用系统。应用安全层面测评实施主要涉及9个工作单元，具体如下表所示：

序号	工作单元名称	工作单元描述
1	身份鉴别	检查应用系统是否采取身份标识和鉴别措施，具体措施有哪些；系统采取何种措施防止身份鉴别信息被冒用
2	访问控制	检查主要应用系统，查看系统是否提供访问控制机制；是否依据安全策略控制用户对客体的访问；是否对重要资源设置敏感标记并严格控制。
3	安全审计	检查主要应用系统，查看其当前审计范围是否覆盖到每个用户；检查主要应用系统，查看其审计策略是否覆盖系统内重要的安全相关事件，并对审计相关资源进行保护。
4	剩余信息保护	检查系统在释放或再分配鉴别信息所在存储空间给其他用户前如何将其进行完全清除（无论这些信息是存放在硬盘上还是在内存中）的描述；
5	通信完整性	检查设计/验收文档，查看其是否有通信完整性的说明，如果有则查看其是否是用密码技术来保证通信过程中数据的完整性的描述；测试主要应用系统，可通过获取通信双方的数据包，查看通信报文是否含有加密的验证码
6	通信保密性	检查主要应用系统是否能在通信双方建立连接之前，利用密码技术进行会话初始化验证；查看系统在通信过程中，对整个报文或会话过程进行加密的功能是否有效
7	抗抵赖	检查应用系统，通过双方进行通信，查看系统是否提供在请求的情况下为数据原发者或接收者提供数据原发证据的功能；
8	软件容错	检查主要应用系统，查看业务系统是否对人机接口输入或通信接口输入的数据进行有效性检验；测试主要应用系统，可通过对人机接口输入的不同长度或格式的数据，查看系统的反应，验证系统人机接口有效性检验功能是否正确并提供自动恢复功能。
9	资源控制	检查主要应用系统，查看是否对系统资源进行控制，采取了何种控制措施。

（5）数据安全

序号	工作单元名称	工作单元描述
1	数据完整性	通过访谈管理员，检查系统管理数据、鉴别信息和重要业务数据在传输过程、存储过程中完整性受到破坏后采取的恢复措施的有效性
2	数据保密性	通过访谈管理员，测试敏感数据传输和存储过程中的保密性措施的有效性，测试信息系统的数据保密性措施
3	数据备份与恢复	通过访谈管理员，实际检查数据备份与恢复功能等手段，测试信息系统的数据备份与恢复措施的有效性

在内容上，数据安全层面测评实施主要涉及3个工作单元，具体如下表所示：

（6）安全管理制度

	1	等级保护测评及网络安全综合服务项目	安全管理制度测评相关的对象包括安全主管人员、安全管理人员,总体方针、政策性文件和安全策略文件、安全管理制度、操作规程、评审等相关的文件资料,及相关记录。 在内容上，涉及工作单位3个，具体如下表所示： **（7）安全管理机构** **安全管理机构测评相关的对象包括安全主管人员、安全管理人员,部门、岗位职责文件等相关的文件资料,及相关记录。现场测评方法包括访谈，文档审查。** **在内容上，涉及工作单位5个，具体如下表所示：** **（8）人员安全管理** **测评对象主要为人事主管、人员管理制度、保密协议、岗位安全协议等相关的文件资料,及相关记录。** **在内容上，涉及工作单位5个，具体如下表所示：**

序号	工作单元名称	工作单元描述
1	管理制度	通过访谈安全主管，检查相关制度文档，检查是否制定安全策略、制度等制度
2	制定和发布	通过访谈安全主管，检查制度和相关过程文档，检查制度的制定和发布情况。
3	评审和修订	通过访谈安全主管，检查制度和相关过程文档，检查院制度的评审和修订情况。

序号	工作单元名称	工作单元描述
1	岗位设置	通过访谈安全主管，检查部门/岗位职责文件，测评安全主管部门设置情况以及各岗位设置情况
2	人员配备	通过访谈安全主管，检查人员名单等文档，测评各个岗位人员配备情况以及关键岗位轮岗情况。
3	授权和审批	通过访谈安全主管，检查相关文档，检查对重要活动的授权和审批情况。
4	沟通与合作	通过访谈安全主管，检查相关文档，检查对内、外单位间的沟通合作情况
5	审核与检查	通过访谈安全主管，检查相关制度文档和管理要求文档等过程，测评对安全工作的审核和检查情况。

序号	工作单元名称	工作单元描述
1	人员录用	通过访谈人事主管，检查制度和相关过程文档，检查人员录用情况。
2	人员考核	通过访谈人事主管，检查制度和相关过程文档，检查人员考核情况。
3	人员离岗	通过访谈人事主管，检查制度和相关过程文档，检查人员离岗控制情况。

4	安全意识教育和培训	通过访谈安全主管，检查制度和相关过程文档，检查安全意识教育和培训情况。
5	外部人员访问管理	通过访谈安全管理员，检查制度和相关过程文档，检查外部人员访问管理情况。

（9）系统建设管理

测评对象主要为安全主管、系统建设负责人,总体建设规划书、详细设计方案，实施/测试/验收文档，软件开发的管理文档/过程规范和控制记录，工程实施方案/管理制度，系统定级/测试/备案文档，服务合同/保密协议等和系统建设相关的文档,及相关工作记录。

在内容上，涉及工作单位11个，具体如下表所示：

序号	工作单元名称	工作单元描述
1	系统定级	通过访谈安全主管，查看相关定级文档，检查系统定级情况。
2	安全方案设计	通过访谈安全主管，查看相关设计文档，检查系统安全方案设计情况。
3	产品采购和使用	通过访谈安全主管，查看相关采购文档及证书，检查系统产品采购和使用情况。
4	自行软件开发	通过访谈系统建设负责人，查看相关的软件开发管理制度，检查系统软件开发是否根据相关安全规范编写
5	外包软件开发	通过访系统建设负责人，查看相关文档及合同，检查系统外包软件开发情况。
6	工程实施	通过访谈系统建设负责人，查看相关文档及合同，检查系统工程实施情况。
7	测试验收	通过访谈系统建设负责人，查看相关验收文档及合同，检查系统验收测试情况。
8	系统交付	通过访谈系统建设负责人，查看相关文档及合同，检查系统交付情况。
9	系统备案	通过访谈安全主管，查看备案相关文档，检查系统备案情况。
10	等级测评	通过访谈系统建设负责人，查看备案及测试相关文档，检查系统等级测评情况。
11	安全服务商选择	通过访谈系统建设负责人，查看相关文档及协议，检查系统安全服务商选择情况。

（10）系统运维管理

测评对象主要为包括相关管理制度、程序/手册、记录、报告、相关运维人员等。在内容上，涉及工作单位13个，具体如下表所示：

序号	工作单元名称	工作单元描述

1	环境管理	访谈物理安全负责人，检查相关文档及现场查看物理环境管理情况。
2	资产管理	访谈资产管理员，查看文档记录及标志，检查资产管理情况。
3	介质管理	访谈资产管理员，查看文档记录及标志，检查介质管理情况。
4	设备管理	访谈设备管理员，查看文档记录及标志，检查设备管理情况。
5	监控管理和安全管理中心	访谈系统运维负责人，查看文档记录，检查监控管理和安全管理中心情况。
6	网络安全管理	访谈安全主管和网络管理员，查看相关文档记录，检查信息系统是否按照相关制度实施日常网络安全管理工作
7	系统安全管理	访谈安全主管和系统管理员，查看文档记录，检查系统安全管理情况。
8	恶意代码防范管理	访谈系统运维负责人和安全管理员，查看文档记录及防恶意代码措施，检查恶意代码防范管理情况。
9	密码管理	访谈安全管理员，查看相关文档，检查密码管理情况。
10	变更管理	访谈系统运维负责人，查看相关文档记录，检查变更管理情况。
11	备份与恢复管理	访谈系统管理员、网络管理员和数据库管理员，查看相关文档，检查备份与恢复管理情况。
12	安全事件处置	访谈系统运维负责人，查看相关文档，检查安全事件处置情况。
13	应急预案管理	访谈系统运维负责人，查看相关文档，检查应急预案管理情况。

2.整体测评

在单元测评的基础上，供应商评价信息系统的整体安全保护能力有没有缺失，是否能够对抗相应等级的安全威胁。信息系统整体测评应从安全控制点间、层面间和区域间等方面进行安全分析和测评，并最后从系统结构安全方面进行综合分析，对系统结构进行安全测评，并给出合理的优化建议方案。

（1）安全控制点安全分析和测评

安全控制点间安全测评主要对同一区域同一层面内的两个或者两个以上不同安全控制点间的关联进行测评分析，其目的是确定这些关联对信息系统整体安全保护能力的影响。

（2）层面间安全分析和测评

层面间安全测评主要对同一区域内的两个或者两个以上不同层面安全控制点间的关联进行测评分析，其目的是确定这些关联对信息系统整体安全保护能力的影响。

（3）区域间安全分析和测评

区域间安全测评主要对两个或者两个以上不同物理或逻辑区域间安全控制点间的关联进行测评分析，其目的是确定这些关联对信息系统整体安全保护能力的影响。

通过对信息系统的单元测评、安全控制点之间的测评、层面分析和区域分析，从而评价信息系统面临的主要安全风险，并提出整改建议，协助进行整改方案的评审，最终使其符合信息系统所定等级应达到的安全防护要求，将信息系统的安全风险降至最低。

3.安全整改建议编制

供应商应在对项目内容充分调研了解的基础上，结合现有运维管理体系和技术状况，根据等级保护相关要求，针对实际业务需要，提出系统建设整改建议。具体应包括：信息安全管理体系、信息安全技术体系等方面，编制《信息系统安全整改建议方案》。

4.测评报告编制

安全整改完成后，供应商进行安全问题复测，并进行信息系统等级测评报告编制。测评报告编制需按照公安机关颁布最新测评报告模板，对信息系统的安全问题项进行符合度评分，并根据各测评项权重计算各层面得分、信息系统总体得分，并在报告中给出安全问题处置建议。

供应商应针对每个系统分别出具《信息系统安全等级测评报告》。

5.数据中心安全优化建议方案编制

在数据中心测评完成后，供应商应根据《信息系统安全整改建议方案》，分析当前安全形势，分析数据中心整体安全态势。做出合理的数据中心安全优化建议方案。

七、实施和保障

（一）项目进度要求

本项目测评实施要求同步实施、重点先行、阶段性成果展现相结合。具体实现进度要求如下：

1.系统梳理

组建项目组，协助采购人完成待测信息系统梳理工作，出具相应安全保护等级定级建议。

2.现场测评

进行现场测评，同时对采购人信息安全相关人员进行安全技术培训。初次测评完成后，提交初评的整改意见报告。

3.整改加固协助

协助采购人针对测评过程中发现的安全问题进行技术整改加固工作，并进行整改后的回归测评。

4.成果递交

整理测评结果，向采购人提交被测信息系统安全等级保护测评报告、定级备案证书、以及相应文档。

(二**)**项目实施要求

供应商应为本项目配置相应的实施团队，具有丰富的实施经验和技术能力。供应商负责提供的服务内容至少应包括，但不限于以下各项：

1.协助采购人完成待测信息系统梳理工作，出具相应安全保护等级定级建议。

2.等保测评包括但不限于以下对象：网络结构、网络服务、主机系统、存储备份系统、数据库、中间件、应用系统、数据安全、安全系统、系统安全策略等。

3.供应商应详细描述服务的技术方案，包括准备工作、技术措施、人员安排、时间进度、可能对系统造成的影响等。

4.安全测评工作应选择在非业务繁忙时段进行，将可能带来的影响减至最小。

5.等级保护测评完后，协助采购人整理备案材料和进行主管部门备案。

(三**)**项目管理要求

对项目进行科学严格的管理，通过系统计划、有序组织、科学指导和有效控制，促进项目全面顺利实施，供应商必须提供完整的项目管理方案，并符合以下要求：

1.供应商及其测评人员应当严格执行有关国家信息安全等级保护相关标准和有关规定，提供客观、公平、公正、有效的等级保护测评服务，并承担相应的法律责任；

2.应具备能够保证其公正性、独立性的质量体系，确保测评活动不受任何可能影响测评结果的商业、财务、健康、环境等方面的压力；

3.供应商在对被测评单位开展等级保护测评服务之前需与被测评单位签订保密协议，测评过程中向被测评单位借阅的文档资料应在测评工作结束后全部归还被测评单位，未经被测评单位允许，不得擅自复制、保留；

			4.供应商的岗位配置要至少配置项目负责人、质量负责人、技术测评人员、管理测评人员、保密安全员和档案管理员，其中项目负责人、质量负责人、保密安全员和档案管理员应独立配置，不能有兼任的情况； **5.**测评人员要求 参与此次等级保护测评的供应商其测评人员应具备并符合以下要求： （**1**）开展此次等级保护测评工作的人员仅限于中华人民共和国境内的中国公民且无犯罪记录（随响应文件提供相关证明材料）； （**2**）开展此次等级保护测评工作的人员应参加信息安全等级保护测评人员培训、考试，并取得信息安全等级保护评估中心颁发的初级及以上测评师证书人员不少于**5**名组成； （**3**）针对软件、网络、安全等方面不少于**5**名测评技术人员除具有信息安全初级及以上保护测评师证书以外，还应该持有国家或行业颁发的相关技术资格证书； （**4**）测评项目组人员在对开展等级保护测评工作之前需签订保密协议。 **6**. 测评工具要求 （**1**） 采用的测评工具必须获得正版授权，并在有效期内，不得使用盗版软件； （**2**）采用的测评工具在功能、性能等满足使用要求前提下，应优先采用具有国内自主知识产权的同类产品； （**3**）采用的测评工具的生产商应为正规厂商，具有一定的研发和服务能力，能够对产品进行持续更新并提供质量和安全保障； （**4**）测评机构所使用的测评工具不会对系统产生破坏或负面影响。 八、保密承诺 **1.**供应商必须保证保守采购人工作秘密，供应商派遣到采购人处的工作人员必须保证保守采购人工作秘密，特别是具体负责工作秘密，不得泄露采购人工作秘密。 **2.**供应商须与采购人签订安全保密承诺书。如若供应商及其派遣到采购人处的工作人员泄露采购人工作秘密，采购人有权依法依规追究供应商及相关人员的责任。

8、供应商一般资格要求

序号	资格要求名称	资格要求详细说明
1	具有独立承担民事责任的能力。	供应商需在使用投标(响应)客户端编制响应文件时，按要求填写《投标（响应）函》完成承诺并进行电子签章。
2	具有良好的商业信誉	供应商需在使用投标(响应)客户端编制响应文件时，按要求填写《投标（响应）函》完成承诺并进行电子签章。
3	具有健全的财务会计制度。	供应商需在使用投标(响应)客户端编制响应文件时，按要求上传相应证明材料并进行电子签章。
4	具有履行合同所必需的设备和专业技术能力。	供应商需在使用投标(响应)客户端编制响应文件时，按要求填写《投标（响应）函》完成承诺并进行电子签章。
5	有依法缴纳税收和社会保障资金的良好记录。	供应商需在使用投标(响应)客户端编制响应文件时，按要求填写《投标（响应）函》完成承诺并进行电子签章。
6	参加政府采购活动前三年内，在经营活动中没有重大违法记录。	供应商需在使用投标(响应)客户端编制响应文件时，按要求填写《投标（响应）函》完成承诺并进行电子签章。

序号	资格要求名称	资格要求详细说明
7	不存在与单位负责人为同一人或者存在直接控股、管理关系的不同供应商不得参加同一合同项下的政府采购活动的行为。	供应商需在使用投标(响应)客户端编制响应文件时，按要求填写《投标（响应）函》完成承诺并进行电子签章。
8	不属于为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商。	供应商需在使用投标(响应)客户端编制响应文件时，按要求填写《投标（响应）函》完成承诺并进行电子签章。

9、供应商特殊资格要求

序号	资格要求名称	资格要求详细说明
1	供应商具有公安部颁发的《网络安全等级测评与检测评估机构服务认证证书》。	供应商提供公安部颁发的《网络安全等级测评与检测评估机构服务认证证书》原件或扫描件。

10、分包的评审条款

评审项编号	一级评审项	二级评审项	详细要求	分值	客观评审项
1	详细评审	报价	以本次最低有效响应报价为基准价，响应报价得分=(基准价 / 响应报价×30)。 注：1.对小型和微型企业产品（服务）的价格给予10%的扣除，用扣除后的价格参与评审（如供应商均为小、微型企业，则不必再扣除）。 2.监狱企业、残疾人福利企业等同小、微企业。	30.0	是
2	详细评审	项目实施方案	供应商根据本项目实际测评对象情况提供：①项目实施方案、②项目管理方案、③测评风险控制方案、④项目实施时间计划、⑤项目人员配制方案、⑥应急预案、⑦质量保证方案等七个方面的内容，能最大限度保证项目售后服务的得21分，每有一项与本项目实际情况不符、缺项、不符合逻辑等任意一种情形的扣3分，直至本项分值扣完为止，不提供不得分。	21.0	否
3	详细评审	履约能力	1.供应商具有中国网络安全审查技术与认证中心颁发的信息安全（CCRC）风险评估二级及以上服务资质证书、ISO27001Foundation信息安全管理体系认证证书，每提供一个证书得5分，最多得10分。 2.拟派本项目的项目负责人具有信息安全等级测评师（高级）证书、信息系统项目管理师证书（高级），每提供一个证书得3分，最多得6分。 3.拟派本项目的测评质量负责人具有信息安全等级测评师（中级及以上）证书、COBIT Foundation信息系统审计认证证书、重要信息系统保护人员CIIP-A（可信计算）证书、信息安全保障人员证书（CISAW）、DSA数据安全评估师证书、计算机技术与软件专业技术人员资格证书（信息安全工程师），每提供一个证书得2分，最多得12分。 4.拟派本项目的技术测评人员应具有信息安全等级测评师（中级及以上）证书、CCSS-M网络安全服务能力评价证书（安全管理能力认证）、软件测评工程师证书、注册密码安全专业人员（NSATP-CSP）证书，每提供一种证书得2分，最多得8分。 5.拟派本项目的管理测评人员具有CISP-PTE注册渗透测试工程师证书、ITILFoundation管理认证证书，每提供一种证书得2分，最多得4分。 （须提供证书复印件并加盖公章，原件备查；以上人员需提供 “参选文件递交截止时间”前近3个月依法缴纳社保证明材料并加盖公章）注：供应商提供的具备相应证书的人员中标后必须到本项目现场提供服务。	40.0	是

评审项编号	一级评审项	二级评审项	详细要求	分值	客观评审项
4	详细评审	经验	供应商近3年（至采购截止时间）具有等级保护测评项目服务经验（以合同签订时间为准）。每一个有效经验得3分，最多得9分。 注：供应商须在响应文件中提供近3年主要业绩清单，同时在响应文件中提供主要业绩的服务合同复印件（含合同首尾页、合同金额页、盖章页、服务内容等）作为证明材料。未提供业绩证明材料或不满足要求的业绩不得分，业绩个数以合同个数为准。	9.0	是

11、合同管理安排

1）合同类型：买卖合同

2）合同定价方式：固定总价

3）合同履行期限：自合同签订之日起800日

4）合同履约地点：筠连县人民医院、筠连县中医医院、筠连县妇幼保健院指定地点。

5）支付方式：分期付款

6）履约保证金及缴纳形式：

中标/成交供应商是否需要缴纳履约保证金：否

7）质量保证金及缴纳形式：

中标/成交供应商是否需要缴纳质量保证金：否

8）付款进度安排：

1、 付款条件说明： 成交供应商第一年完成初测，出具整改建议书。 ，达到付款条件起 15 日内 ，支付合同总金额的 16.67 % ；

2、 付款条件说明： 成交供应商第一年整改完成后，采购人收到成交供应商出具的纸质版盖章的《信息系统安全等级保护测评报告》安全等级三级并通过公安部门审核。 ，达到付款条件起 30 日内 ，支付合同总金额的 16.67 % ；

3、 付款条件说明： 成交供应商第二年完成初测，出具整改建议书。 ，达到付款条件起 15 日内 ，支付合同总金额的 16.67 % ；

4、 付款条件说明： 成交供应商第二年整改完成后，采购人收到成交供应商出具的纸质版盖章的《信息系统安全等级保护测评报告》安全等级三级并通过公安部门审核。 ，达到付款条件起 30 日内 ，支付合同总金额的 16.67 % ；

5、 付款条件说明： 成交供应商第三年完成初测，出具整改建议书。 ，达到付款条件起 15 日内 ，支付合同总金额的 16.67 % ；

6、 付款条件说明： 成交供应商第三年整改完成后，采购人收到成交供应商出具的纸质版盖章的《信息系统安全等级保护测评报告》安全等级三级并通过公安部门审核。 ，达到付款条件起 30 日内 ，支付合同总金额的 16.65 % ；

9）验收交付标准和方法：验收要求：至服务期（三年）满15个工作日前，成交供应商提供每次测评的产品信息系统报告及相应的过程文档，制定验收计划及验收方案等交采购人审查，双方无异议，共同商定验收人员并实施验收工作。 验收标准：合同期满后，由采购人组织专业人员、监督人员会同成交供应商参照《财政部关于进一步加强政府采购需求论证和履约

验收管理的指导意见》（财库〔2016〕205号）的要求，按照采购文件、响应文件内容、合同内容进行验收。验收结果不合格的，不予支付未支付款项，并报告本项目同级财政部门按照政府采购法律法规及《四川省政府采购当事人诚信管理办法》等有关规定给予行政处罚或者以失信行为记入诚信档案。

10）质量保修范围和保修期：无

11）知识产权归属和处理方式：无

12）成本补偿和风险分担约定：无

13）违约责任与解决争议的方法：1．甲方违约责任及违约金支付：（1）甲方未按合同约定付款的违约责任：（2）甲方的其他违约责任：2．乙方违约责任及违约金支付：（1）乙方提供不合格服务的违约责任：（2）乙方逾期交付的违约责任：（3）乙方的其他违约责任：

14）合同其他条款：1．本合同经双方法定（授权）代表人签字（或盖章）并盖单位公章后生效，同时须送筠连县财政局备案。2．合同执行中涉及采购资金和采购内容修改或补充的，须经筠连县财政局审批，签订书面补充协议并报政府采购监督管理部门备案，方可作为主合同不可分割的一部分。3．本合同一式 六 份，甲方、乙方各执 二 份，送筠连县财政局、采购代理机构备案各一份。

12、履约验收方案

1）验收组织方式：自行验收

2）是否邀请本项目的其他供应商：否

3）是否邀请专家：否

4）是否邀请服务对象：是

5）是否邀请第三方检测机构：否

6）履约验收程序：分段/分期验收

7）履约验收时间：

1、 验收条件说明： 供应商第一年完成初测，出具整改建议书。 ，达到验收条件起 15 日内，验收合同总金额的 16.67 %；

2、 验收条件说明： 供应商第一年整改完成后，采购人收到成交供应商出具的纸质版盖章的《信息系统安全等级保护测评报告》安全等级三级并通过公安部门审核。 ，达到验收条件起 30 日内，验收合同总金额的 16.67 %；

3、 验收条件说明： 供应商第一年完成初测，出具整改建议书。 ，达到验收条件起 15 日内，验收合同总金额的 16.67 %；

4、 验收条件说明： 供应商第二年整改完成后，采购人收到成交供应商出具的纸质版盖章的《信息系统安全等级保护测评报告》安全等级三级并通过公安部门审核。 ，达到验收条件起 30 日内，验收合同总金额的 16.67 %；

5、 验收条件说明： 供应商第三年完成初测，出具整改建议书。 ，达到验收条件起 15 日内，验收合同总金额的 16.67 %；

6、 验收条件说明： 供应商第三年整改完成后，采购人收到成交供应商出具的纸质版盖章的《信息系统安全等

级保护测评报告》安全等级三级并通过公安部门审核。，达到验收条件起 30 日内，验收合同总金额的 16.65 %；

8）验收组织的其他事项：无

9）技术履约验收内容：按采购文件及合同。

10）商务履约验收内容：按采购文件、响应文件、及合同。

11）履约验收标准：按国家有关规定以及采购文件的质量要求和技术指标、供应商的响应文件及承诺与本合同约定标准进行验收；采购人与供应商双方如对质量要求和技术指标的约定标准有相互抵触或异议的事项，由采购人在采购文件及响应文件中按质量要求和技术指标比较优胜的原则确定该项的约定标准进行验收。

12）履约验收其他事项：交付时间：分别于2024年、2025年、2026年按照采购文件要求提供三次测评服务，除2024年之外，2025年、2026年必须在每年的10月30日之前完成整体测试工作，提交完整的测试报告并通过公安部门审核，同时每年在项目具备整体测试条件后30个工作日内完成整体测试工作，提交完整的测试报告，以上时间不包含客户整改时间，但需指导客户完成整改。 整改期限：客户整改时间，自收到成交供应商出具的测评报告后2个月内。 其它要求：成交供应商，签订合同时，必须向采购人提交保密承诺书。

五、风险控制措施和替代方案

该采购项目按照《政府采购需求管理办法》第二十五条规定，本项目是否需要组织风险判断、提出处置措施和替代方案：否