汇川区卫生信息数据中心网络安全等级二级保护服务采购项目

需求公示

一、资格条件：

（一）满足《中华人民共和国政府采购法》第二十二条规定，提供政府采购 法实施条例第十七条规定资料。

（一） 满足《中华人民共和国政府采购法》第二十二条规定，提供政府采购 法实施条例第十七条规定资料。

（1）具有独立承担民事责任的能力：提供法人或其他组织的营业执照等证明文件，或自然人身份证明；

（2） 具有良好的商业信誉和健全的财务会计制度：提供 2020 年度或者 2021 年度的财务报告复印件或近期财务报表复印件或银行出具的资信证明复印件

（3）具有履行合同所必需的设备和专业技术能力：提供承诺函（格式文件详见响应文件范本）；

（4）具有依法缴纳税收和社会保障资金的良好记录：税收：2021 年至今任意 3 个月依法缴纳税收的相关证明材料(如税务局出具的书面证明或网银缴费凭证或完税凭证票据等）；社保 ：提供 2021 年至今任意 3 个月依法缴纳社会保险费的相关证明材料(如社保局出具的书面证明或网银缴费凭证或社保花名册或社保缴纳凭证票据等）

（5）参加本次政府采购活动前三年内，在经营活动中没有重大违法记录：提供在经营活动中没有重大违法记录的书面声明

（6）参加本次政府采购活动前三年内无失信惩戒记录：投标供应商信用信息：对列入被失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单且还在执行期的供应商，拒绝其参加政府采购活动。信用记录查询渠道为“信用中国”和中国政府采购网（政府采购严重违法失信行为信息记录)，查询时间为购买文件之日至开标前一天的任意时间，供应商须提供查询记录截图并加盖公章，作为信用查询记录和证据编入文件。

（7）特殊资格条件：/

（二）落实政府采购政策需满足的资格要求：

1. 对小型和微型企业产品的价格给予6%的扣除，用扣除后的价格参与评审（须提供小微企业声明函，严格按照财库〔2011〕181号《政府采购促进中小企业发 展暂行办法》执行。提供的声明函必须真实，如有虚假，将依法承担相应责任）；

2.监狱企业视同小型、微型企业（提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件复印件加盖报价供应商鲜公章）；

3.残疾人福利性单位视同小型、微型企业。（供应商须严格按照财库〔2017〕141号《三部门联合发布关于促进残疾人就业政府采购政策的通知》的要求提供《残疾人福利性单位声明函》，并对声明的真实性负责）。

二、技术参数

A包：等级保护测评技术服务

等级保护测评	1、本次开展网络安全等级保护测评的信息系统包括：汇川区人口健康信息基础平台、汇川区卫生和计划生育局人口健康信息基础平台。 2、针对采购人建设的信息系统和办公网络，采取渗透测试、安全基线配置核查和病毒木马专项检查等方式，开展一次全面的网络安全风险排查工作，明确资产的重要性、脆弱点、安全威胁等内容，系统地分析网络与信息系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，以便利用有限的资源有针对性地进行安全保护和建设，提出有针对性的抵御威胁的防护对策和整改措施。 3、针对采购人建设的信息系统和办公网络，采取扫描工具以本地扫描的方式对评估范围内的系统和网络进行安全扫描，从内网和外网两个角度来查找网络结构、网络设备、服务器主机、数据和用户帐号/口令等安全对象目标存在的安全风险、漏洞和威胁，提供漏洞扫描报告。 4、完成服务所需工具、软件由投标人自行准备。

B包：等级保护硬件设备

新一代防火墙	1、实配双电源，千兆电口数≥8个，千兆光口数≥2个，接口扩展槽位≥2个，提供设备正面图片；吞吐量≥20Gbps，并发连接数≥280万，每秒新建连接数≥3万；支持SSLVPN功能；三年原厂维保服务； 2、为便于运维，硬件面板应支持专门的一键重启按键，必要时可在不登录设备的情况下一键重启设备； 3、访问控制策略：支持基于源/目的IP，源/目的端口，源/目的

	区域，用户（组），应用/服务类型的细化控制方式； 4、支持 IPv4 / v6 NAT 地址转换，支持源目的地址转换，目的地址转换和双向地址转换，支持针对源 IP 或者目的 IP 进行连接数控制； 5、支持对被保护对象的流量进行分析，通过对流量日志的统计整理，智能生成包过滤策略，提高运维人员工作效率。提供生产厂家确认的、相应的功能证明材料（包括但不限于测试报告、官网和功能截图等）； 6、支持 SYN Flood、ICMP Flood、UDP Flood、ARP Flood 攻击防护，支持 IP 地址扫描，端口扫描防护，支持 ARP 欺骗防护功能、支持 IP 协议异常报文检测和 TCP 协议异常报文检测； 7、支持通过命令行的方式对设备内部的数据流进行分析，可快速定位造成故障的防火墙内部功能模块，便于进行故障排查。提供生产厂家确认的、相应的功能证明材料（包括但不限于测试报告、官网和功能截图等） 8、入侵防护漏洞规则特征库数量在 5000 条以上，入侵防护漏洞特征具备中文相关介绍，包括但不限于漏洞描述，漏洞名称，危险等级，影响系统，对应 CVE 编号，支持对 HTTP，FTP，SMTP，POP3 协议进行病毒文件检测，支持杀毒白名单功能，可以根据 URL 或者 IP 进行排除不检测病毒； 9、支持对安全策略进行冗余分析。提供生产厂家确认的、相应的功能证明材料（包括但不限于测试报告、官网和功能截图等）； 10、支持针对不同策略、不同流量修改 TCP，UDP 和 ICMP 协议的连接超时时间 11、双机支持 A/S，A/A 方式部署，支持配置同步，会话同步和用户状态同步； 12、支持多虚一部署，可将两台物理设备虚拟化成一台逻辑上的设备，再将一台逻辑上的设备虚拟化成多个虚拟防火墙。提供生产厂家确认的、相应的功能证明材料（包括但不限于测试报告、官网和功能截图等）； 13、支持自动和手动备份，至少能够保存 10 个的文件，支持配置回滚。提供生产厂家确认的、相应的功能证明材料（包括但不限于测试报告、官网和功能截图等）； 14、支持 NTP 协议，可作为 NTP Server，也可作为 Client 设备。提供生产厂家确认的、相应的功能证明材料（包括但不限于测试报告、官网和功能截图等）；
数据库 审计系统	1、至少 6 个千兆电口；至少 1T 存储空间，审计能力至少 1200Mbps，SQL 处理数 1000 条/秒；含应用识别库；三年原厂维保服务； 2、数据库实例授权数量无限制，同时审计端口数不少于 6 个，并且无授权限制。 3、支持双操作系统，当常用系统出现故障可以使用备用系统恢复。 4、支持审计系统与管理系统一体化，不需要安装额外的管理软件，不需要单独的管理设备，无需在被审计系统上安装任何代理。 5、★支持审计 Oracle、SQL Server、My SQL、DB2、Sybase、Informix、PostgreSQL、Kingbase、Cache、Gbase、Dameng、Teradata、Oscar、MongoDB 等各类主流数据库系统。提供生产厂家确认的、相应的功能证明材料（包括但不限于测试报告、官网和功能截图等）

	6、支持对访问数据库的源地址、目的地址、SQL 操作响应时间、数据库操作成功、失败的审计，支持数据库账号登陆成功、失败的审计。 7、支持 SQL 操作审计，可审计数据库操作类、表、视图、索引、触发器、域、Schema、事物等。 8、支持以数据库客户端软件名称、数据库名、数据库表名、数据库字段名作为过滤响应条件（非正则表达式方式）的数据库审计策略。 9、★支持数据库审计事件与 WEB 业务系统事件的关联功能，可将审计到的数据库事件，与 web 服务器、客户端 IP 地址等信息关联起来。提供生产厂家确认的、相应的功能证明材料（包括但不限于测试报告、官网和功能截图等） 10、★支持自定义报表，可以根据客户需求定制更多有实际意义的报表。
安全运维审计系统（堡垒主机）	1、至少 6 个千兆电口,至少 200 个主机/设备许可；三年原厂维保服务； 2、采用专用硬件架构与安全操作系统，硬件设备可以机架安装。 3、产品采用模块化设计，可以通过扩展卡来增减业务接口，而非软件运维安全审计系统。 4、采用物理旁路部署，不改变现有网络结构，支持双机部署，保证系统发生故障时的可用性。 5、★支持混合云资源的管理，即公有云及局域网资源，支持主机、服务器、网络设备、安全设备、数据库等的资产管理，满足公有云、云资源池、数据中心多种运维场景。提供生产厂家确认的、相应的功能证明材料（包括但不限于测试报告、官网和功能截图等） 6、支持资源分类和资源系统类型管理：内置常见资源分类和资源系统类型，可自定义添加资源分类、资源系统类型和资源服务类型。 7、★公有云设备支持一键更新发现功能。提供生产厂家确认的、相应的功能证明材料（包括但不限于测试报告、官网和功能截图等） 8、支持会话、指令、剪切板上下行、文件上传下载的约束行为，支持对用户/IP/mac 地址/登录时间进行控制。 9、支持会话请求远程协助，且协同会话保持实时同步。 10、支持 SecureCRT、XShell、WinSCP 等客户端直接连接堡垒机进行代理运维目标资产。 11、★图像审计采用 OCR 图像识别技术，通过加载训练过的运维图片集合，可以识别图形操作中的程序标题、快捷方式标题、窗口内容中的文本信息。提供生产厂家确认的、相应的功能证明材料（包括但不限于测试报告、官网和功能截图等） 12、支持将本机日志、告警日志通过 SYSLOG、邮箱等进行外发和告警。
日志审计	1、至少 6 个千兆电口+至少 2 个千兆光口,冗余电源,至少 2 个扩展槽位,至少 200 日志源授权，综合采集处理均值至少 1000EPS；三年原厂维保服务； 2、支持 Syslog、SNMP Trap、Netflow、JDBC、WMI、FTP、SFTP、SCP、文件等方式进行数据采集；支持通过 Agent 采集日志数据 3、数据存储能力：压缩加密存储，压缩比不低于 10:1；日志存储不低于 10000 条/M。提供生产厂家确认的、相应的功能证明材料（包

	括但不限于测试报告、官网和功能截图等） 4、★支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等日志对象的日志数据采集。提供生产厂家确认的、相应的功能证明材料（包括但不限于测试报告、官网和功能截图等） 5、支持独立展示每个被采集源最近 24 小时的日志数量趋势，便于掌握设备的安全事件情况，支持独立展示每个设备日志的最新采集时间，便于了解设备日志的采集状态；。提供生产厂家确认的、相应的功能证明材料（包括但不限于测试报告、官网和功能截图等） 6、系统支持智能报表创建，每添加一个日志源，系统自动分析日志源类型进行相应报表创建，无需人工干预，报表和资产一一对应； 7、支持安全告警概况、安全告警趋势以及实时安全事件的统一展示，实时告警可根据级别、规则类型等进行分类； 8、★支持对日志流量非常大但是日志重要程度低的 syslog 类型日志源进行限制接收速率，降低对系统资源的占用，保障重要日志的收集。提供生产厂家确认的、相应的功能证明材料（包括但不限于测试报告、官网和功能截图等） 9、支持日志转发给第三方系统平台，支持设置多个日志转发 IP 地址，支持转发格式化日志或仅转发原始日志； 10、★支持对文本类型日志源进行限速采集，匀速采集日志，防止对系统资源产生突发冲击。提供生产厂家确认的、相应的功能证明材料（包括但不限于测试报告、官网和功能截图等） 11、支持自定义统计报表报告，支持 PDF、Word、Execl、Html 等方式导出报表，支持实时报表、计划报表；
EDR	1、至少 100 个 Windows PC 客户端防病毒功能授权,含 3 年升级许可；至少 12 个服务器端防病毒的病毒查杀支持多引擎的协同工作对病毒、木马、恶意软件、引导区病毒、BIOS 病毒等进行查杀，提供主动防御系统防护等功能。客户端系统默认支持 Windows XP/VISTA/WIN7/WIN8/WIN10。默认包含 3 年病毒库升级服务；1 个 Windows PC 客户端防病毒功能授权,含 3 年升级服务。防病毒的病毒查杀支持多引擎的协同工作对病毒、木马、恶意软件、引导区病毒、BIOS 病毒等进行查杀，提供主动防御系统防护等功能。客户端系统默认支持 Windows XP/VISTA/WIN7/WIN8/WIN10。含管理端，三年原厂维保服务。 2、客户端安装后至多占用 50M 硬盘资源，病毒库 3M 大小，日常内存占用不到 30M，有效节省 PC/Server 资源。提供生产厂家确认的、相应的功能证明材料（包括但不限于测试报告、官网和功能截图等） 3、支持全网威胁统计分析管理控制台可直观的展示病毒趋势统计、终端信息、病毒类型排行、病毒排行、终端危险排行等统计情况。并随时对网络中病毒发生的情况进行查询统计，能按时间、按 IP 地址、机器名、按病毒名称、病毒类型进行展示； 4、★对系统关键位置进行防护，阻止无文本攻击、流氓、广告程序对系统的恶意篡改等行为。从系统文件保护、病毒免疫、进程保护、注册表保护、危险动作拦截、执行防护等多个维度对系统进行防护。提供生产厂家确认的、相应的功能证明材料（包括但不限于测试报告、官网和功能截图等） 5、支持客户端防删功能，能够防止客户端在未经管理员允许情况

	下强行卸载。提供生产厂家确认的、相应的功能证明材料（包括但不限于测试报告、官网和功能截图等） 6、报表内容必须包括御类型分析、病毒类型分析、病毒排行、终端杀毒排行、病毒趋势统计、黑客拦截、对外攻击分析。支持威胁 Top10、Top20、Top30 排行； 7、★控制台支持恶意网站拦截、浏览器保护、恶意行为、文件保护、下载保护、黑客拦截、系统加固、U 盘防护、邮件监控、白名单等策略下发。提供生产厂家确认的、相应的功能证明材料（包括但不限于测试报告、官网和功能截图等） 8、管理控制台支持预制策略功能，保障新安装客户端自动应用组策略； 9、支持对移动存储设备采用标签式注册管理，可以区分内外部介质使用，定义禁用、启用只读、启用（只读_运行）和启用读写、启用（读写_运行）五种操作，按照文件类型审计在移动存储介质上文件操作记录，并可设置例外 USB 设备。 10、支持病毒自动隔离功能，对于暂时无法清除的被感染文件或者可疑文件，防病毒软件的客户端能自动将其隔离到本地隔离区；
服务器	1、CPU Intel（R）Xeon（R） CPU E5-2620v4 及以上 2、内存 DDR4 64 GB 及 以上 3、硬盘 SATA 2TB 及以上 4、网卡 4GE 千兆网卡及以上
路由器	1、端口：1 个 10/100/1000M RJ45 WAN 口，4 个 10/100/1000M RJ45 LAN 口，1 个 Console 端口 2、处理器：双核 MIPS 64 位网络专用处理器，主频 1GHz 内存：DDRIII 512MB 3、FLASH：32MB 4、典型带机量：500 台左右
机房物理环境改造	机房防火门、门禁及消防等物理环境按照等保要求进行改造

三、商务要求

1.服务期限及项目地点

2.服务期限：

A 包：等级保护测评技术服务：3 个月

B 包：等级保护硬件设备：3 年

3.项目地点：遵义市汇川区卫生健康局

4.验收标准、规范：符合国家现行有关行业验收规范标准

5.付款方式：

A 包：等级保护测评技术服务：测评完成，验收合格后五年内付清

B 包：等级保护硬件设备：验收合格使用三年后支付，五年内付清

6.磋商有效期：60 日历天

四、评审办法

一、开标

1.递交响应文件截止时间后，由采购人对供应商身份进行验证。供应商需提供以下有效身份证明文件：1.有效的统一社会信用代码的营业执照（复印件加盖鲜章）；2.法人代表授权书原件（若法人参与磋商则不需提供）、法人或被授权人身份证原件。

2.由招标人或供应商自主推荐代表检查已通过资质审查的供应商的响应文件密封情况，并当场宣布检查情况。

3.密封情况检查结束后，由招标人当众拆封响应文件，按签到顺序宣读供应商名称、递交磋商响应文件的情况，以及代理机构认为有必要宣读的其他内容。初始磋商报价不在开标阶段开启。

4.如供应商对宣读的内容有异议的，应在获得开标会主持人同意后当场提出。如确实属于招标人宣读错了的，经现场核实后，当场予以更正。

5.没有启封和读出的响应文件将原封退回给供应商。

二、磋商小组

招标人根据本项目的特点，依照《中华人民共和国政府采购法》及其实施条例、《政府采购竞争性磋商采购方式管理暂行办法》的有关规定组建磋商小组，其成员由采购人代表和在专家库中随机抽取的有关技术、经济等方面的专家共3

人组成，其中评审专家人数2人。磋商小组负责本项目的竞争性磋商工作和评审工作。

三、磋商

1.磋商原则。磋商小组成员应当按照客观、公正、审慎的原则，根据磋商文件规定的评审程序、评审方法和评审标准进行独立评审。磋商小组所有成员应当集中与单一供应商分别进行磋商。

2.竞争性磋商文件内容的变更。磋商过程中，磋商小组获得采购人同意后，可以根据磋商文件和磋商情况实质性变动采购需求中的技术、服务要求以及合同草案条款，但不得变动磋商文件中的其他内容，并将变更的内容书面通知所有参加磋商的供应商。磋商过程中，磋商小组发现竞争性磋商文件内容有严重的倾向性、或某一产品唯一性、或歧视性的，可要求采购人认可调整，并将变更的内容书面通知所有参加磋商的供应商。但任何形式的变更须以符合公平、公正原则和有利于项目的顺利实施为前提，且变更后不影响产品的性能、质量。

3.技术服务响应文件的变更。磋商过程中，供应商可以根据磋商情况变更其响应文件，并将变更内容形成书面材料送磋商小组。变更内容应作为响应文件的一部分。供应商书面材料应当由供应商代表签字确认，否则无效。

4.确定成交人。经磋商确定最终采购需求和提交报价的供应商后，由磋商小组采用综合评分法对提交报价的供应商的响应文件和报价进行综合评分。磋商小组应当根据综合评分情况，按照评审得分由高到低顺序推荐2-3名成交候选供应商，并编写评审报告。

四、评标程序

评分工作由磋商代理人负责组织，具体评标事务由采购人依法组建专家磋商小组负责。

磋商小组成员到位后，推举其中一位评审专家担任评审组长，并由评审组长牵头领导该项目评审工作。磋商小组按以下程序独立履行评审职责：

1、资格性检查。依据法律法规和磋商文件的规定，对响应文件中的资格证明、磋商保证金等进行审查，以确定供应商是否具备投标资格。

2、符合性检查。依据磋商文件的规定，从响应文件的有效性、完整性和对磋商文件的响应程度进行审查，以确定是否对磋商文件的实质性要求作出响应。

评审内容	评审因素	评审标准
资格评审标准	营业执照（多证合一）	具备有效的（多证合一）营业执照。
	具有独立承担民事责任的能力	提供具有统一社会信用代码的营业执照
	具有良好的商业信誉和健全的财务会计制度	提供2020年度或者2021年度的财务报告复印件或近期财务报表复印件或银行出具的资信证明复印件
	具有履行合同所必需的设备和专业技术能力	具有项目实施能力，提供所需设备及相关技术人员证书或提供承诺函
	有依法缴纳税收和社会保障资金的良好记录	税收：2021 年至今任意 3 个月依法缴纳税收的相关证明材料（如税务局出具的书面证明或网银缴费凭证或完税凭证票据等）；社保 ：提供 2021 年至今任意 3 个月依法缴纳社会保险费的相关证明材料（如社保局出具的书面证明或网银缴费凭证或社保花名册或社保缴纳凭证票据等）
	参加本次政府采购活动前三年内，在经营活动中没有重大违法记录	提供在经营活动中没有重大违法记录的书面声明（格式自拟）

	参加本次政府采购活动前三年内无失信惩戒记录	投标供应商信用信息：对列入被失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单且还在执行期的供应商，拒绝其参加政府采购活动。信用记录查询渠道为“信用中国”和中国政府采购网（政府采购严重违法失信行为信息记录)，查询时间为购买文件之日至开标前一天的任意时间，供应商须提供查询记录截图并加盖公章，作为信用查询记录和证据编入文件。
	法定代表人身份证明及法定代表人身份证或法定代表人授权委托书及被委托人身份证	符合招标文件规定
符合性检查	投标供应商名称	与三证合一的营业执照上的名称一致，不一致的应有工商行政管理部门出具的变更证明
	报价函签字盖章	符合磋商文件要求
	投标文件份数、密封、签署	符合磋商文件要求
	磋商报价有效性	只能有一个磋商报价，响应文件未提供选择性报价或有两个以上（含两个）磋商报价，且未超过采购预算（拦标价）
	服务期限	满足磋商文件规定的服务期限
	是否有不符合法律法规规定及磋商文件规定的其他条件	是否符合要求

3、澄清有关问题。对响应文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容,磋商小组可以书面形式(应当由磋商小组成员签字）要求供应商作出必要澄清、说明或者纠正。供应商的澄清、说明或者补正应当采用书面形式，由其授权的代表签字，并不得超出响应文件的范围或者改变响应文

件的实质性内容。

4、比较与评价。按磋商文件中规定的评分方法和标准，对资格性检查和符合性检查合格的响应文件进行商务和技术评估，综合比较与评价。

磋商小组各成员应当独立对每个有效供应商的标书进行评价、打分，然后由评审组长组织磋商小组成员对各评委打分情况进行核查及复核。

复核后，招标代理机构汇总每个供应商每项评分因素的得分。

5、推荐中标候选人名单。按评审后得分由高到低顺序排列推荐综合得分排名第一的供应商为第一中标候选人;得分相同的,按投标报价由低到高顺序排列;得分且投标报价相同的，按技术指标优劣顺序排列。

五、评分标准

评分形式（采用以下具体步骤）

第一步：资格及符合性审查

由本项目磋商小组综合审查供应商资质情况,是否符合磋商文件的基本资质要求，符合者将作为有效标，并进入第二步评议。不符合，其投标作为无效标，不能进入第二步评议。

第二步：确定成交供应商（按评分细则对供应商给相应的评分，并计算其总得分，按各项评标因素权重计算各有效供应商的最终得分）

（一）评分细则及各项评标因素分值

评分办法

A包：等级保护测评技术服务评分标准

分值		评分标准
商务评分标准（33分）	业绩情况 （10分）	供应商提供近三年经营业绩(2019年1月至投标截止时间止，合同或中标通知书日期为准)的销售业绩进行评价。每提供 1项业绩得2分，最高得10分。 注:需提供采购合同或中标通知书复印件，不提供不得分。
	安全产品制造商实力 （8分）	依据供应商具备有效期内的以下证书进行评分，每提供一项资质得2分，满分8分： （1）ISO9001 质量管理体系认证证书 （2）ISO27001 信息安全管理体系认证证书 （3）ISO14001 环境管理体系认证证书 （4）国家信息安全漏洞库（CNNVD）技术支持单位等级证书 (提供相关证明材料复印件并加盖公章）
	项目经理 （5分）	项目经理为中级及以上测评师且具备CISP资质的得5分。 注：需提供身份证复印件、证书复印件、投标人为其缴纳2021年的社保证明，不提供不得分。
	项目团队成员 （10分）	项目团队成员 1.提供高级测评师1名得2分，提供中级测评师1名得1分，提供初级测评师1名得0.5分，满分得5分。 2.提供CISP证书得0.5分，满分1.5分；提供专业级风险管理资质CISAW证书得0.5分，满分1.5分；满分得5分 。 注：需提供人员的资质证书复印件及供应商为其缴纳2021年的社保证明，不提供不得分。
技术评分标准（52分）	服务响应情况 （8分）	对各供应商的响应情况进行评议， 完全响应磋商文件技术服务要求的得8分：有一项不满足扣2分，扣完为止。

	服务方案 （19 分）	一、1.服务方案整体编制科学合理、重点突出，具体实现方式科学合理，完全满足采购人实际需求，风险把控具体完整，得 15-11 分。 2.服务方案整体编制合理，有侧重点，基本满足采购人实际需求；风险把控、基本合理，得 10-5 分。 3.服务方案编制粗糙、杂乱、未突出重点，针对性差，无法满足采购人实际需求，得 4-1 分；不提供方案不得分。 二、供应商在贵州省内设有售后服务机构的得 4 分。（提供售后服务机构房屋租赁合同或营业执照及售后服务团队名单及相关人员身份证明作为佐证材料，不提供不得分）
	项目实施方案 （5 分）	1.项目实施整体设计方案和具体实现方式科学合理，可行性强得 5 分； 2.项目实施整体设计方案和具体实现方式基本科学合理，可行性一般得 3 分。 3.项目实施整体设计方案和具体实现方式不够科学合理，可行性差得 1 分。 不提供不得分。
	保密措施 （5 分）	1.项目信息的保密措施全面、科学、合理得 5 分； 2.项目信息的保密措施基本全面、科学、合理得 3 分； 3.项目信息的保密措施不够全面、科学、合理性差得 1 分 不提供不得分。
	进度保障 （5 分）	1.项目实施进度计划科学合理以及对项目实施质量的保障程度高得 5 分； 2.项目实施进度计划基本科学合理以及对项目实施质量的保障程度一般得 3 分； 3.项目实施进度计划不够科学合理以及对项目实施质量的保障程度差得 1 分； 不提供不得分。
	售后服务 （5 分）	根据供应商提供的售后服务方案及承诺的具体性，详细程度、可行性、售后服务技术能力及售后服务人员的综合能力等因数进行综合评分 1.售后服务方案完善且全面性、合理性、及时性和可行性等得 5 分； 2.售后服务方案基本完善合理得 3 分； 3.售后服务方案不完善不合理得 1 分； 不提供不得分

	自研测评工具 （5 分）	测评机构使用自主知识产权测评服务工具，需提供相应的软件著作权证书，每提供一个证书得 1 分，不提供不得分，最高 5 分。 测评工具包括 1.“物理安全检查记录分析系统” 2.“Windows 系统安全配置检查系统” 3.“网络安全分析及处理系统” 4.“安全管理制度查询及分析系统” 5.“网络设备日志搜集与分析管理系统软件” (提供相关证明材料复印件并加盖公章)
价格得分 （15 分）	投标报价得分计算公式	报价得分＝(评标基准价/报价)×15 注：1、评标基准价指满足磋商文件要求且报价最低的报价；得分取两位小数点，第三位四舍五入； 备注：（报价低于预算价格 80%以下的，供应商须在投标文件中附成本分析报告，阐明项目成本构成内容，提供成本控制的具体方案，并能证明成本节约的可行性，否则报价分计零分。）

序号	评分因素及权重	分值	评分标准
B 包：等级保护硬件设备评分标准			
一、价格分（30 分）			
1	投标报价	30 分	报价得分＝(评标基准价/报价)×30 注：1、评标基准价指满足磋商文件要求且报价最低的报价；得分取两位小数点，第三位四舍五入； 备注：（报价低于预算价格 80%以下的，投标单位须在投标文件中附成本分析报告，阐明项目成本构成内容，提供成本控制的具体方案，并能证明成本节约的可行性，否则报价分计零分。）
二、技术分（40 分）			

1	技术要求	25 分	采购清单中所投产品的技术指标完全满足招标文件要求的得 25 分。带★的参数为重要技术参数，每负偏离一项扣 2 分，其他参数不能满足招标文件要求的，有 1 项不满足扣 0.5 分，直至扣减到 0 分为止。 **备注：1、参数中注明提供截图证明而未提供的，也视为负偏离；2、如一项参数含多项指标，该参数中只要有一项指标不满足，也视为负偏离；3、提供所投产品制造商盖公章的参数确认函原件）**
2	技术方案	15 分	需求理解:根据对需求背景、建设目标、建设任务及各项需求是否认识到位、理解充分，并提出有针对性的整体解决思路的程度进行评分： 1、情况了解最全面，详细描述了服务背景、系统现状，服务目标和需求描述 全面，部署架构合理，方案功能完善、提出针对性的解决思路，方案整体完整度和可行性高得 10-7 分。 2、情况了解一般，简单描述了服务背景、系统现状，服务目标和需求描述不够全面，方案功能基本满足、方案整体完整度和可行性一般得 6-4 分。 3、情况了解较差，没有描述服务背景、系统现状，服务目标和需求描述粗略，方案功能勉强满足、方案整体完整度和可行性较差不了解得 3-1 分。 4、供应商在贵州省内设有售后服务机构的得 5 分。（提供售后服务机构房屋租赁合同或营业执照及售后服务团队名单及相关人员身份证明作为佐证材料，不提供不得分）
三、商务分（30）			

1	产品制造商综合实力	21 分	**1、制造商研发实力：** 投标产品（运维安全审计系统、数据库审计系统、日志审计系统、终端杀毒系统）厂商均获得国测信息安全服务资质-安全工程类三级、具备信息安全等级保护安全建设服务机构能力评估合格证书、具有国家信息安全测评信息安全服务资质证书（证书颁发机构：中国信息安全测评中心）-风险评估类二级及以上；以上 3 项全部提供得6分，提供2项得3分，提1项得1分。不提供不得分。（提供相关证明材料复印件并加盖公章） **2、产品制造制造商领域专业度：** （1）所投（运维安全审计系统、数据库审计系统、日志审计系统、终端杀毒系统）产品的生产厂商具备软件成熟度模型 CMMI5 认证得 4 分，CMMI4 得 2 分，CMMI3 得 1 分，其他情况不得分，不提供不得分。（需提供相关证明资料） （2）所投（运维安全审计系统、数据库审计系统、日志审计系统、终端杀毒系统）产品制造商为国家信息安全漏洞库（CNNVD）一级技术支撑单位得 4 分，二级技术支撑单位得 2 分，三级技术支撑单位得 1 分（需提供相关证明资料），不提供不得分 （3）所投（运维安全审计系统、数据库审计系统、日志审计系统、终端杀毒系统）产品制造商具有国家互联网应急中心 （CNCERT）网络安全应急服务支撑单位（APT监测分析）证书得3分。 （4）所投（运维安全审计系统、数据库审计系统、日志审计系统、终端杀毒系统）产品制造商2021年度在CNVD（国家信息安全漏洞共享平台）支撑单位工作贡献≥12000得4分，支撑单位工作贡献≥5000、≤11999得2分，支撑单位工作贡献≤4999得1分。 **（需提供以上对应证明材料并加盖制造商公章，否则本项不得分）；**
2	售后服务	6 分	1、根据供应商提供的售后服务方案及承诺的具体性，详细程度、可行性、售后服务技术能力、日常维护方案、故障应急处理方案、备品备件储备情况及售后服务人员的综合能力等因数进行综合评分 （1）售后服务方案完善且全面性、合理性、及时性和可行性等得 5 分； （2）售后服务方案基本完善合理得 3 分； （3）售后服务方案不完善不合理得 1 分； 不提供不得分。 2、投标人本次提供的设备硬件及软件均享受 3 年运维（包括远程运维与现场运维），且保证每年至少 1 次上门巡检，得 1 分。（提供相关承诺）

3	业绩	3 分	供应商提供近三年经营业绩(2019 年 1 月至投标截止时间止，合同或中标通知书日期为准)的销售业绩进行评价。每提供 1 项业绩得 1 分，最高得 3 分。 注:需提供采购合同或中标通知书复印件，不提供不得分。

（二）排序原则

按评审得分由高到低顺序排序。得分相同的，按技术指标得分由高到低排列，技术指标得分排列相同的，按投标报价由低到高顺序排列。

（三）中标原则

由磋商小组根据计算各有效供应商的最终得分确定成交供应商。

六、无效投标条款

磋商小组评审时，供应商或其响应文件出现下列情况之一者，应为无效投标：

（一）供应商未按磋商文件规定提交足额磋商保证金的；

（二）供应商未通过资格性检查或响应文件未通过符合性检查的；

（三）供应商超出营业范围投标的；

（四）法定代表人为同一个人的两个及两个以上法人，母公司、全资子公司及其控股公司，在同一磋商中同时投标的；

（五）响应文件未按照磋商文件响应文件格式中所规定签字、盖章的；

（六）响应文件出现多个投标方案或投标报价的；

（七）响应文件含有违反国家法律、法规的内容，或附有磋商人不能接受的条件的

（八）投标有效期、服务期等商务条款不能满足磋商文件要求的。

七、废标条款

磋商小组评审时出现以下情况之一的，应予废标：

（一）符合专业条件的或对采购文件作实质响应的供应商不足三家的；

（二）出现影响采购公正的违法、违规行为的；

（三）供应商报价均超过了采购预算，采购人不能支付的；

（四）因重大变故，采购任务取消的。

（五）法律法规规定的其他情形

废标后，除采购任务取消情形外，应当重新组织采购。