**招标文件**

**项目名称：** 工控网络安全建设

**计划令号：** GJ2023042-GQ

**招标单位**： 贵州航天林泉电机有限公司

**第一部分投标邀请**

**贵州航天林泉电机有限公司**（以下称“招标人”）对**工控网络安全建设**项目进行招标。招标情况如下：

1. 招标货物名称：工控网络安全建设
2. 数量：1
3. 主要技术规格：见本招标文件第二部分
4. 交货地点：招标人指定
5. 商务材料：营业执照、纳税证明、相关资质证明、业绩证明材料、交货周期、售后服务等
6. 投标截止时间：2024年2月2日下午2：00时（北京时间），逾期收

到或不符合规定的投标文件恕不接受

1. 开标时间、地点：投标截止后一周于贵州航天林泉电机有限公司会议室
2. 设备付款方式

本次招标对中标价的设备款付款方式原则上为招标方预付款0%，设备到位安装调试合格后付款60%，三个月运行良好后付款30%，设备质保期一年满后10日内付10%的余款。

1. 企业名称及地址

企业名称：贵州航天林泉电机有限公司

单位地址：贵州省贵阳市观山湖区长岭南路89号林泉科技园区

10、投标书**一正二副**用快递投寄或其他方式传递到我公司，务必在标书密封条外写明项目名称！以免影响开标前的资料整理！供应商不到现场参加开标。

 11、联系方式：

单位名称：贵州航天林泉电机有限公司

通信地址：贵州省贵阳市观山湖区长岭南路89号林泉科技园区

联系人：龙孟伟

电话：18085598229

 招标机构：贵州航天林泉电机有限公司

2023年1月26日

**第二部分 技术规格及要求**

1. **工控安全设计思路**

在保证系统可用性前提下，对工业控制系统进行防护，实现“垂直分层，水平分区。边界控制，内部监测”。

“垂直分层、水平分区”即对工业控制系统垂直方向化分为三层：现场设备层、现场控制层、监督控制层。水平分区指各工业控制系统之间应该根据不同业务特点从网络上实现逻辑隔离，处于不同的安全区。

“边界控制，内部监测”即对系统边界即各操作站、工业控制系统连接处、无线网络等要进行边界防护和准入控制等。对工业控制系统内部要监测网络流量数据以发现入侵、业务异常、访问关系异常和流量异常等问题。

系统面临的主要安全威胁来自于黑客攻击、恶意代码（病毒蠕虫）、越权访问（非授权接入、移动介质、弱口令、操作系统漏洞、误操作和业务异常等），因此，工控安全设计方案应体着重体现以下几个方面的内容：

（1）针对林泉电机现有网络结构，按照“垂直分层”、“水平分区”原则，根据不同业务属性，制定网络整改实施方案，使之具备办公网与工控网隔离基础条件（林泉电机现有网络拓扑图不对外提供，需现场调研）；

（2）边界访问控制和系统访问控制策略；

（3）总体安全监控平台，通过平台集中展示整个网络中的安全信息和攻击威胁；

（4）文件敏感字检测、外联外设管控；

（5）进程白名单防护、外设管控；

（6）操作站操作系统安全；

（7）入侵检测及防御。

1. **新增建设清单**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 设备名称 | 数量 | 单位 | 单价 | 备注 |
| 1 | 第二代防火墙 | 1 | 台 |  |  |
| 2 | 工业防火墙 | 1 | 台 |  |  |
| 3 | 工业安全集中管理平台 | 1 | 台 |  | 日志收集、主机安全卫士控制台 |
| 4 | 工业主机安全卫士 | 1 | 套 |  | 120个授权点 |
| 5 | 工控安全监测与审计系统 | 1 | 套 |  |  |
| 6 | 终端安全管理系统 | 1 | 台 |  | 1100个终端授权点，含敏感信息检测和外设管控等 |
| 7 | 网络基础能力建设 | 1 | 套 | —— | 此项为附加服务 |

1. **新增设备技术要求（性能参数）**

|  |  |  |
| --- | --- | --- |
| 序号 | 设备名称 | 性能参数 |
| 1 | 第二代防火墙 | 1、千兆业务电口数量≥10个，千兆业务光口数量≥4，万兆业务光口数量≥4个，1个Console口，管理电口≥1，冗余电源；集成访问控制、入侵防御、病毒过滤、应用过滤等功能；2、网络吞吐量≥8Gbps，最大并发连接数≥100万，每秒新建连接数≥70000；3、支持路由模式、透明（网桥）模式、混合模式、旁路模式；旁路部署支持加入多个物理接口；部署模式切换无需重启设备；4、支持双机热备，双主模式、主备模式；设备切换时，TCP会话仍能保持；5、支持基于全局或链路进行DNS透明代理，支持指定DNS或继承链路DNS配置，针对多链路支持基于优先级、权重、流量算法进行DNS负载；6、支持防ARP攻击，造成网络故障。支持ARP绑定；支持SQL注入和跨站脚本的防御，可以针对HTTP协议的非法输入进行检查，对SQL注入和跨站脚本行为进行阻断；支持对后门和木马攻击的防御；7、提供对控制策略的策略分析，可分析并展示问题策略数量以及所占百分比、问题策略详情、策略宽松度分布情况，简化运维工作；8、支持独立的Web防护模块，系统定义超过4500条WAF规则防护功能，支持常规HTTP漏洞、SQL注入、组件、CMS、WebShell和XSS等类型的Web防护；支持HTTP协议的URL、Method、Referer、User-Agent、Cookie、URL-args等字段的等于、不等于、包含、不包含、正则等多种匹配方式的访问控制；9、系统定义最大超过6000种主流应用，支持识别多种主流应用，支持应用自定义并对自定义的应用进行分组，支持根据标签选择应用，支持自定义应用的导入和导出；支持通过立即升级、定时升级、手动上传文件三种方式升级应用特征库，支持显示升级历史和升级结果；1. 防火墙具有中国网络安全审查技术与认证中心颁发的网络关键设备和网络安全专用产品安全认证证书(增强级)(含高性能，下一代互联网支持)，提供加盖原厂商公章的证书复印件；
2. 产品厂商须具有5年以上ITSS信息技术服务运行维护标准符合性证书、CCRC颁发的信息安全风险评估资质二级及以上证书，以上证书须提供加盖厂商公章的证书复印件；
3. 产品厂商具有ISO27001（业务范围须包含安全服务、安全运维、安全咨询、系统集成），提供厂商盖章复印件；

13、产品含5年质保服务。 |
| 2 | 工业防火墙 | 1、硬件平台：千兆业务电口数量≥6个，千兆业务光口≥2，1个Console口，管理电口≥1，冗余电源；2、最大吞吐量≥5Gbps，最大并发连接数（TCP）≥100万，最大新建连接数≥90000；3、支持透明、路由、混合，多种部署模式；4、支持用户自定义的安全策略，包括MAC地址、IP地址、端口的部分或全部组合；5、白名单支持≥20种工业协议深度识别及协议；6、支持对工业协议的深度分析学习，支持将分析学习到的内容快速生成白名单访问控制策略、具备对工业协议的指令/功能码、地址、数据值等的细粒度分析学习；7、支持工业场景下网络拓扑显示，连接状态，端口UP/down状态；8、支持启发式白名单自学习，支持学习进度提示功能，当学习数据超过一定时间不变化时，应提示距离上次学习到新数据已过去多长时间；9、 产品具备中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》工业控制系统专用防火墙（增强级）；提供加盖制造厂商公章的证书复印件；10、产品厂商须具有5年以上ITSS信息技术服务运行维护标准符合性证书、CCRC颁发的信息安全风险评估资质二级及以上证书，以上证书须提供加盖厂商公章的证书复印件；11、产品厂商具有ISO27001（业务范围须包含安全服务、安全运维、安全咨询、系统集成），提供厂商盖章复印件；12、产品含5年质保服务。 |
| 3 | 工业安全集中管理平台 | 1、千兆电口≥6个，硬盘容量≥2T；2、支持最大管理设备数量30台以上，主机安全卫士500个点及以上，支持对各个单元网络的安全监控和必要的日志收集；3、系统支持对包括网络设备、安全设备与系统、主机在内的多种管理对象的安全事件进行集中管理；4、支持设备自动发现，自动发现设备支持模式包含：支持CDP思科发现协议、LLDP链路发现协议、OSPF路由邻居协议、交换机端口转发协议、交换机STP生成树协议、ARP路由补充发现，支持SNMP设备管理；5、支持安全日志审计，全面记录工业网络中的主机安全日志、网络异常攻击监测日志、网络攻击防护日志、工业网络会话信息，同时保留攻击发生时的原始报文信息，便于安全事件的追溯和调查取证；6、运用“白环境”理念，对全网安全产品进行统一策略配置。包括网络流量“白名单”、工控协议“白名单”、主机应用“白名单”；7、支持对工业防火墙安全事件的智能分析并生成智能推荐策略；8、支持全局配置闪烁声音告警开关、邮件告警开关；9、支持对工业防火墙设备的策略管理，包括黑名单、白名单、工业协议、IP/MAC管理、基础防火墙、安全防护等；10、能检测到已联网且未安装工业主机安全卫士的终端并报警，并将异常信息应能推送到“连我”/“RTX”或者915DJ平台微信端；11、产品厂商须具有5年以上ITSS信息技术服务运行维护标准符合性证书、CCRC颁发的信息安全风险评估资质二级及以上证书，以上证书须提供加盖厂商公章的证书复印件；12、产品厂商具有ISO27001（业务范围须包含安全服务、安全运维、安全咨询、系统集成），提供厂商盖章复印件；13、产品含5年质保服务。 |
| 4 | 工业主机安全卫士 | 1. 至少支持Win2000、Win XP、WinVista、Win7、Win8、Win10、Windows2003 Server、Windows2008 Server、Windows2012 Server等，Linux系统至少支持Centos、Redhat、Ubuntu、凝思、麒麟、统信等；
2. 支持应用程序管理，对应用程序进行运行前检查，禁止白名单以外的非法应用程序运行，并产生安全事件，记录非法应用程序的运行企图，支持对隐藏应用程序的检查；3、支持流行病毒利用的常见漏洞防护，包括震网病毒利用漏洞MS08-067（CVE-2008-4250）、永恒之蓝利用漏洞MS17-010（CVE-2017-0143）、永恒之黑利用漏洞CVE-2020-0796、CAD病毒等的防护；4、支持保护进程内存空间的完整性，防止缓冲区溢出攻击；支持安全基线当前合规状态的检测展示，支持安全基线的一键批量加固，支持安全基线一键恢复原始配置；
3. 支持一键检测操作系统安全基线、服务、程序、进程、用户列表等信息，并可导出报表；6、支持对安全事件的记录功能，记录与安全相关的告警和阻断事件，内容包括时间、事件类型、响应方式和执行对象的全路径等信息；7、支持控制光驱、无线网卡、蓝牙、串口、并口的启用、禁用，注册U盘可显示U盘序列号、驱动器盘符、管控策略、注册时间、注册状态、接入状态、杀毒标志、U盘类型，并可添加备注描述信息；8、支持普通U盘、安全U盘的注册管理，注册U盘可分别配置“只读、读写、执行”属性；9、支持文件保护，文件自身及其父目录不允许被重命名，避免文件保护被绕过；10、强制访问控制主体、客体，强制访问控制例外的主体、客体，其自身及其父目录不允许被重命名，防止强制访问控制策略被绕过；

11、所有功能均可以通过服务端下发策略实现，同时异常信息应能推送到“连我”/“RTX”或者915DJ平台微信端；12、产品厂商具有ISO27001（业务范围须包含安全服务、安全运维、安全咨询、系统集成），提供厂商盖章复印件；13、产品厂商须具有工业信息安全测试评估机构能力认定证书、工业信息安全监测应急支撑单位证书，以上证书须提供加盖厂商公章的证书复印件；14、产品含5年质保服务。 |
| 5 | 工控安全检测与审计系统 | 1. 标准1U机架式，全密闭无风扇，配置千兆电口≥6个，千兆光口≥4个，1个RJ45 Console管理口；1个USB接口，冗余电源，工作温度：-10℃~60℃；
2. 整机最大吞吐率≥5Gbps，最大并发连接数≥100万，每秒新建连接数≥10000；
3. 须支持≥20种工控协议的深度解析与审计（包括但不限于Modbus TCP、BAcnet、OPCDA、DNP3、S7、IEC104、MMS、Profinet 、CIP、 OPCUA\_TCP等）；
4. 自学习工业白名单，支持设置学习时长，规则组名，生成可信任白名单规则；
5. 支持手动添加工业白名单，对modbus TCP协议的功能码、地址、值域进行审计；
6. 支持基于特征的恶意报文检测；
7. 事件实时监控，包括事件总数、未读事件数以及事件发生的高峰时段，日志，CPU、内存、网络总流量占用的实时监控；支持基于流量的审计，包含流量类别，流量大小，不同时间段的流量审计；
8. 所有功能均可以通过服务端下发策略实现，同时异常信息应能推送到“连我”/“RTX”或者915DJ平台微信端；
9. 产品厂商具有ISO27001（业务范围须包含安全服务、安全运维、安全咨询、系统集成），提供厂商盖章复印件；
10. 产品含5年质保服务。
 |
| 6 | 终端安全管理软件 | 1. 支持准入控制、桌面管理、数据防泄露、终端检测响应、外设管控等功能模块一体化管理，一个管控平台，一个客户端，平台同时支持信创终端管理。（提供系统截图证明并加盖原厂公章）；

2、终端安全管理平台支持以下需求：支持分布式部署，可将系统自身功能组件（radius、通信组件服务器、存储组件服务器、数据库等组件、审计文档服务器等）独立模块化分布式部署，分担服务器的压力，提高服务器的稳定性。支持AD/LDAP、多AD\LDAP同步、钉钉、竹云IAM、UOS域、mysql数据库同步组织架构。（提供系统截图证明并加盖原厂商公章）；3、硬件性能参数不低于以下要求：2u机架式，CPU≥ 8核，内存≥64G，硬盘2\*10T（raid1），4\*千兆网口，冗余电源。此次采购含1100个授权；1. ★支持对多层文档嵌套的泄露行为进行检查，应最少支持不低于5层压缩包的文件内容检测，能够发现任何一层文档中含有的敏感信息。（提供系统截图证明并加盖原厂商公章）注：能发现压缩包中PDF文档中所含的图片内容敏感信息，并告警；
2. ★支持对各类Office、PDF等主流文档学习生成敏感数据DNA防止重要文档泄露；支持识别常见的文件内容，包括图片、doc、docx、xls、xlsx、ppt、pptx、pdf、zip、rar、7z、txt等。（提供系统截图证明并加盖原厂商公章）；6、支持Linux下U盘禁用，macOS、Windows支持禁用U盘并审计、未注册U盘只读并审计、禁止和审计自建WiFi、禁用和审计无线网卡、WiFi白名单、蓝牙等。支持基于设备GUID、设备实例路径、显示名称、设备服务名等进行某一类设备进行管控，包括审计与禁止。支持通过PING/TCP/HTTP等方式检测终端是否与互联网连通、检测终端是否与其他网络连通（含电脑直连方式）、检测终端是否与特定网络连通。支持处置：禁用网卡、锁屏，必须管理员恢复；

7、★支持软件安装卸载审计控制，可审计用户软件安装卸载行为，可禁止用户软件安装卸载行为；支持软件安装黑白名单管理，禁止运行黑名单中的软件安装包或禁止运行白名单外的软件安装包；支持自定义已安装软件黑白名单，检测到安装了在黑名单中的软件，则执行违规处理：审计或者禁止运行；支持绿色软件黑白名单管理，黑名单内的绿色软件禁止运行或白名单外的绿色软件禁止运行；（提供系统截图证明）；8、★支持正则表达式检测内容，正则表达式包括电话号码、银行卡号、身份证号、姓名、地址、邮箱、快递单号等；支持设置最少正则命中次数；支持自定义文档的敏感级别、敏感类别，并设定自动匹配规则；可以匹配文档的页数、字数、行数、以及图片数量等，也就是按照信息量的大小去界定是否敏感，在相关的外发通道时可以引用这些规则进行敏感检查，审计信息可以看到命中文档的页数、行数、字数。（提供系统截图证明并加盖原厂商公章）；9、支持服务器设置自定义扫描时间周期并给指定终端下发策略；可设定扫描全盘、指定目录、排除指定目录。支持终端客户端进行自助扫描。支持闲时扫描：设置CPU、内存阀值，超过阀值停止扫描，当终端键盘或鼠标无操作时进行闲时扫描；10、★支持自定义检查项，对终端的注册表（路径、名称、属性）、文件（路径、名称、属性，包括文件产品名称、文件公司名称、文件描述、文件CRC校验、文件源文件名、文件内部名称、文件所属软件名、文件签名、文件MD5值、文件大小）、操作系统版本（操作系统版本、系统SP版本）、进程（路径、名称、属性，包括文件产品名称、文件公司名称、文件描述、文件CRC校验、文件源文件名、文件内部名称、文件所属软件名、文件签名、文件MD5值）、服务（运行状态、注册状态）进行检查，同时，可对以上检查条件进行任务组合检查；11、★支持防火墙（网络资源访问控制）提供自定义协议与服务端口，支持TCP、UDP、RDP、HTTP、FTP、共享；支持源或目的的双向控制，支持入站和出站的双向控制。DNS黑白名单控制。支持已安装客户端的主机与未安装客户端或客户端离线的主机进行隔离控制；（提供证明材料，并加盖原厂公章）；12、支持明文水印：在文档打印时，将水印信息一起打印到文档上，支持宏替换。支持自定义显示位置、字体、字号、水印密度、水印颜色、透明度；支持水印单行模式、对齐方式、水印位置；支持明文水印、二维码水印、图片水印、矢量水印（点阵矢量图形方式，浮现在屏幕上方；支持设置颜色、透明度、形状大小、形状间距）；支持打印指定文件类型、打印指定应用才会触发打印水印，且支持将两种及以上水印方案任意组合； 13、★支持将水印信息加载到屏幕上方，支持宏替换。支持自定义显示位置、字体、字号、水印密度、水印颜色、透明度；支持水印单行模式、对齐方式、水印位置；支持明文水印、二维码水印、图片水印、矢量水印（点阵矢量图形方式，浮现在屏幕上方；支持设置颜色、透明度、形状大小、形状间距）；支持屏幕截图附加盲水印（QQ、微信、企业微信、TIM、企业QQ、钉钉、键盘按键截屏）；支持打开敏感文件、指定进程、访问指定应用才会触发屏幕水印，且支持将两种及以上水印方案任意组合；（提供证明材料，并加盖原厂公章）；支持特定IP地址不输出水印；14、支持审计与禁止Web访问行为；支持对网站进行分类、并定期更新后导入；支持http、https的URL访问与上传控制；支持对访问的域名进行检测；支持对论坛发帖内容进行敏感内容检测；支持对网页上传附件进行审计并留档；（支持IE、Firefox、Chrome等浏览器）；15、支持管控终端上的文件操作，文件源或目的为本地硬盘、移动存储介质（U盘、移动硬盘、SD卡）、网络共享、mstsc远程桌面或其他存储设备，可以进行禁止、审计、备份等管控操作；支持对文件的读、写、复制、剪切、创建、删除、另存为、新建、重命名等动作进行监控；支持记录文件路径、文件名、文件大小；文件操作过程中进行敏感检查；对行为进行阻断；对拷贝进行加密、解密、审批、审计、上传拷贝文件副本；对操作过程进行触发式屏幕录像；自定义统一提示信息、默认提示行为内容信息、支持全局提示信息；对以上提交进行任意组合；而且可定义组合条件执行顺序；16、对检查出的异常数据应能根据严重程度提供处理建议（比如较大风险的建议直接删除、一般风险项自动剪切到指定目录），由终端用户选择删除或者自动剪切到指定目录，终端用户可以随时打开软件查询未处理的文件，并随时处理；17、应提供网络版、单机版两个版本。网络版服务端能检测到已联网且未安装安全管理软件的终端，并报警；18、所有功能均可以通过服务端下发策略实现，同时异常信息应能推送到“连我”/“RTX”或者915DJ平台微信端；19、产品含5年质保服务。 |
| 7 | 网络基础能力建设 | 1. 工控网核心交换机与办公网核心交换机之间万兆组网，工控网核心—工控网汇聚—工控网接入间千兆组网（预估需新增S7706交换机万兆板卡一块，工控核心万兆交换机一台，其余交换机6台）；
2. 园区现有生产网、办公网进行分离，确保网络不存在复用情况；
3. 对办公网络与生产网络进行重新规划设计和建设，完成办公网、生产网楼间光纤铺设，楼内综合布线；
4. 网络建设完成后对所有业务信息系统进行业务联调，及时发现、处理联调过程以及试运行期间出现的故障问题，确保园区各业务信息系统的稳定运行。
 |

**四、设备操作培训、验收等要求。**

4.1需负责对招标方操作人员进行技术培训指导，直至操作人员能够安装、调试及处理简单常见故障，培训在招标人指定地点进行。

4.2使用过程中如发现质量问题，投标人接到通知后必须迅速解决。需要派遣技术人员到现场的，在得到招标人许可后，迅速派技术人员到现场对应。

4.3招标人为进行维修而要求生产并供应的设备零部件 (以下简称「维修零部件」)，投标人应尽可能满足该要求。维修零部件的价格和数量由双方协商决定。

4.4设备质量保证期为最终交付验收合格之日算起1年或一年以上。质保期内设备免费维修，由此发生的所有相关费用（包括更换零部件等内容）由投标人承担。

4.5 设备运行效率≥80%

4.6 标准件能耗等级：不低于国家及相关行业等标准规定的二级要求。

4.7 需标明产品能耗等级，并提供相关证明或测试报告。

**五、设备交付需提供的相关资料、附件。**

验收资料纸质版及电子版各一份，资料需双方进行签署确认，具体清单如下：

1. 设备操作规程；
2. 附件清单；
3. 设备使用维护说明书（含配件的型号、规格）。

**投标书（格式）**

致：贵州航天林泉电机有限公司

根据贵方为项目招标采购货物及服务的投标邀请，签字代表（全名、职务）经正式授权并代表投标人（投标人名称、地址）提交下述正本一份和副本二份。

1. 投标书；
2. 投标价格表；
3. 投标设备技术性能指标的详细描述；
4. 商务资料；
5. 规格、技术参数偏离表；
6. 其他材料。

据此函，签字代表宣布同意如下：

1、附投标价格中规定的应提供和交付的货物投标总价为

（注明币种），即（文字表述）。

 2、我们将按招标文件的规定履行合同责任和义务。

 3、我们已详细审查全部招标文件，包括修改文件（如有的话）以及全部参考资料和有关附件。我们完全理解并同意放弃对这方面有不明及误解的权利。

4、本投标自开标日起有效期为个日历日。

5、我们同意提供按照贵方可能要求的与本投标有关的一切数据或资料，完全理解贵方不一定要接受最低价的投标或收到的任何投标。

6、与本投标有关的一切正式往来通讯请寄：

 地址： 邮编：

 电话： 传真：

 投标人代表姓名、职务（印刷体）：

 投标人名称：

 （公 章）：

 日 期：年月日

 授权代表签字：

**投标价格表（格式）**

 货币单位：

|  |  |  |
| --- | --- | --- |
| 1 | 投标货物序号 |  |
| 2 | 货物名称 |  |
| 3 | 原产地 |  |
| 4 | 数量 |  |
| 5 | 主机和标准附件单价 |  |
| 6 | 备品备件价 |  |
| 7 | 易损件价 |  |
| 8 | 专用工具价 |  |
| 9 | 技术服务价 |  |
| 10 | 安装价（单独报价） |  |
| 11 | 检验培训费 |  |
| 12 | 运输（至目的地） |  |
| 13 | 保险 |  |
| 14 | 其它 |  |
| 15 | 投标总价 |  |

投标人代表签字: 日期：

**商务、技术参数偏离表（格式）**

|  |  |  |
| --- | --- | --- |
| 招标文件条款 | 投标文件对标情况及条款号（请逐项填写） | 偏差说明（正偏离、负偏离、无偏离或其他情况叙述） |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

投标人代表签字: 日期：

**除商务和技术偏差表里列出的偏差外，投标人响应招标文件的全部要求。**