安徽全柴动力股份有限公司

工业互联网安全建设项目

招

标

书

2021 年 10 月 19 日

目　录

1. 项目简介

1.1. 项目名称

全柴动力工业互联网安全建设项目。

1.2. 建设地点

安徽省滁州市全椒县襄河镇吴敬梓路 788 号。

1.3. 项目概述

安徽全柴动力股份有限公司是一家集研发、制造、销售、服务于一体的上市企业，是国家高新技术企业，国家知识产权优势企业，国家技术创新示范企业，中国内燃机行业排头兵企业，安徽省产学研合作示范企业。具备年产 60 万台系列发动机的制造能力，是目前国内最大的四缸柴油机研发与制造企业之一。

公司建有国家级企业技术中心、院士工作站、博士后科研工作站、安徽省中小功率柴油机重点实验室，是国家高新技术企业、国家技术创新示范企业、国家知识产权优势企业。2008 年以来，公司共获授权专利 420 项，其中 39 项发明；参加 10 多项国家标准、行业标准的起草制定；近 5 年来，承担国家及省市研发项目 7 项，获得国家重点新产品奖 4 项，安徽省省级重点新产品奖 3 项，安徽省新产品证书 2 项，安徽省科技进步奖 5 项。

为贯彻落实《中华人民共和国网络安全法》、《关于深化“互联网+先进制造业”发展工业互联网的指导意见》，根据《加强工业互联网安全工作的指导意见》有关要求，开展工业互联网企业网络安全分类分级，加强工业互联网企业差异化、精细化管理，落实企业网络安全主体责任，提高网络安全防护能力和水平，促进工业互联网高质量发展，依据分类分级的指导思想及要求，为工业互联网企业企业提供安全建设技术参照依据，为强化工业互联网发展提供安全支撑。

在工业互联网发展趋势浪潮概念已逐渐深入人心，工业自动化的领军企业也逐步将发展的重点放在产业领域的联网以及自动化技术与信息技术的高度融

合上。也正是因为信息化的不断融合，越来越多的信息安全问题被引入了传统工业化系统当中，加大了工业系统遭受网络攻击的可能性，工控安全事关经济发展、社会稳定和国家安全。

工业信息安全是一个全新安全领域，具备高度的前沿性和复杂性，目前工业信息安全整体形势日趋严峻。主要表现为：一是大规模、高强度工业信息安全事件频发，工业领域成为网络攻击“重灾区”；二是工控安全漏洞层出不穷，高危漏洞占比近六成，且大量集中于装备制造、交通、能源等重要领域，严重威胁国家信息基础设施安全；三是工控系统及设备大量暴露于互联网，已经成为世界各国工业信息安全的软肋。

2. 建设要求

提升设备安全防护能力，保障终端计算机、控制设备、移动存储介质的操作及使用行为管控，防范病毒及恶意代码的感染威胁，定期针对病毒威胁检测及清除，同时加强设备的统一集中管管理功能；

提升网络安全防护能力，针对企业网络的结构划分，依据纵深防御体系建设的建设前期，对企业按照 IEC62443 标准层级进行划分，对网络链路、控制系统采取冗余机制、保证网络带宽与业务的可用性，定期开展网络架构的安全风险评估并进行整改建设，加强安全设备的自身的安全能力，完善网络设备及安全设备的用户信息完整性及认证过程，对需联网设备实行接入的行为管控，依靠边界安全网关、攻击检测、安全隔离及安全审计设备建立不同安全区域边界进行安全技术措施应用。

2.1. 对投标方提供产品的基本要求

本招标文件提出的是最低限度的技术要求，投标方应保证提供符合本招标文件和有关最新工业标准的成熟的、优质的、可靠的、完整的产品。

投标方所提供的设备规格应在投标方的设计和制造经验范围内，并且经验证明在相似的使用场合下的使用是可靠的。

2.2. 招标方的基本权利

在签订合同之后，招标方保留对本招标文件提出补充要求和修改的权力，投标方许诺予以配合。如提出修改，具体项目和条件由双方商定。

2.3. 标准执行原则

本招标文件所使用的标准如与投标方所执行的标准发生矛盾时，按较高标准执行。

2.4. 产品完整性

本文件所述项目为交钥匙工程，建设目标要求、相关设备技术要求等只是最基本的，并未包含全部内容，投标方应根据这些要求、生产工艺需求及用户订货范围提供最合理配置的设备，对所提供设备的可靠性、安全性、成熟性、合规性及完整性最终负全责。若在安装、投运过程中发现有缺件、坏件等情况，及产品非该公司最新产品，投标方负责免费及时补供，以确保设备的可靠性及达到验收标准。

3. 投标要求

3.1. 对参与投标单位分别收取投标保证金 5 万元。

3.2. 投标报价和结算均以人民币为币种，单位为元。

3.3. 投标报价和结算以填表方式进行，一切与本次招标清单不符的投标，均视为未响应标书。

4. 投标资格要求

4.1. 资质要求：

①在中华人民共和国境内注册，具有独立法人资格，能够提供本次招标服务（提供营业执照原件或含二维码的复印件）；

②注册资本：不低于 1000 万元人民币或等值外币（汇率以申请文件接收当日中国人民银行授权中国外汇交易中心公布的各国货币对人民币的中间价进行换算）；

4.2. 财务要求：

投标人须提供会计师事务所出具的 2020 年度财务审计报告（提供由审计单位盖章的审计报告复印件，原件备查）；

4.3. 业绩要求：

投标人须具有 2018 年 1 月 1 日以来承接的单项合同金额 100 万元及以上具有政府、企事业单位信息系统安全集成项目业绩合同的（以合同签订时间为准，提供合同原件或复印件，合同原件备查）；

4.4. 信誉要求：

①被相关行政主管部门禁止投标的投标人，不得参加本次投标；

②投标人之间存在下列情况之一的，不得参加同一标段的投标：

a、两个及以上公司的法定代表人为同一人；

b、集团公司与全资子公司或控股子公司的关系（包括直接控股和间接控股的情形）；

4.5. 其他要求：

（1）代理商投标时须提供拟采用设备原厂商针对本项目的授权书原件且在有效期内。

（2）是否接受联合体投标：不接受

5. 主要设备采购要求

本项目涉及内容较多，安全建设需求产品如下：负载均衡、统一安全网关（下一代防火墙+IPS）、WEB 应用防火墙、上网行为管理、堡垒主机、杀毒软件升级扩容、数据库审计系统、日志审计系统、态势感知管理平台、工业防火墙、工业安全审计系统、网络安全服务（安全巡检、安全漏洞扫描和加固、安全应急、安全运维、重大时期保障服务）。

5.1. 设备详细要求

序号	设备名称	参数	数量	单位
办公网区域安全建设				
1	负载均衡	1、标准 1U 机架设备，千兆电口≥6 个，万兆光口≥6 个（满足上述端口情况下留有）扩展槽数量≥2 个，内存大小≥8G；硬盘容量≥128G SSD； 2.产品性能：吞吐量≥8Gbps，最大并发连接数≥500 万，四层每秒新建连接数≥15 万，七层每秒新建连接数≥7 万；	1	台

		3、.支持静态路由、IPv4 策略路由、IPv6 策略路由、RIPv1/v2、OSPFv2、OSPFv3、BGP、ISIS 等路由协议； 4、支持链路负载功能，支持链路数据实时预览，能够实时展示所有链路的发送/接收流量、延时、丢包率、当前连接数、新建连接数、健康监测信息、链路状态等； 5、售后服务：为保障售后服务质量，提供原厂授权和三年售后服务承诺函,要求提供原厂工程师安装和后期维护； 6、投标人提供产品厂商售后服务承诺函，甲方有权在中标后一周之内要求中标人提供产品测试，对于测试不满足的可予以终止采购。		
2	统一安全网关（下一代防火墙）	1、标准 1U 架构，冗余电源，设备千兆电口≥6 个，≥6 个万兆光口（满足上述端口情况下留有）扩展插槽数量≥2 个； 2、产品性能：全面整合传统安全网关功能，提供深度内容安全防护，有效降低黑客入侵风险，实现功能和性能的全面提升；并发会话数≥1,200,000；每秒新建会话数≥40,000；全功能开启状态支持流量不低于 200Mbps。 3、包含病毒防护功能，用于检测并阻止恶意程序，如勒索软件、病毒，蠕虫，僵尸网络，间谍软件，网页木马，可拦截间谍软件的回拨企图，阻止间谍软件下载，阻止恶意程序通过即时通信程序进行扩散，防止访问与间谍软件或网络钓鱼有关的网站。 4、包含入侵防御功能，主动式入侵防御系统提供了 6,000+条漏洞探测及防护规则，防止漏洞利用和 SQL 注入, 命令注入, Webshell 攻击, XSS 攻击, CSRF 攻击。DDOS 防护, 阻止应用层攻击和非法获取权限。用户可根据不同操作系统，不同服务类别，漏洞发布时间以及严重性，按需选择 IPS 规则，配置更灵活，且性能更好，双向防护，既可以阻止恶意攻击，又能够防止敏感信息泄漏。 5、售后服务：为保障售后服务质量，提供原厂授权和三年售后服务承诺函,要求提供原厂工程师安装和后期维护。 6、投标人提供产品厂商售后服务承诺函，甲方有权在中标后一周之内要求中标人提供产品测试，对于测试不满足的可予以终止采购。	1	台
3	WEB 应用防火墙	1、标准 1U 架构，设备千兆电口≥6 个，≥2 个千兆光口，2 个 USB 口，单电源，应用层吞吐≥12Gbps，并发连接数≥400 万，包含三年特征库升级，不限制防护站点； 2、支持智能部署，上线 WAF 设备能够自动感知 Web 网站 IP 和端口；支持安装向导式部署，按照该部署方式可直接部署完成；支持 NAT 环境下的用户识别能力。 3、具备业务合规功能，可对业务进行恶意试探、恶意撞库、恶意登录等行为进行检测及拦截；具备网站锁功能，对网站进行锁定，可按日期、周期进行锁定时间设置； 4、具备 Web 恶意扫描防护的检测与防御能力，专利级别防护能力。 5、售后服务：为保障售后服务质量，提供原厂授权和三年售后服	1	台

		务承诺函,要求提供原厂工程师安装和后期维护。 6、投标人提供产品厂商售后服务承诺函，甲方有权在中标后一周之内要求中标人提供产品测试，对于测试不满足的可予以终止采购。		
4	上网行为管理	1、标准 1U 架构，固化千兆电口≥4 个，固化光口≥2，支持并实配冗余电源；提供三年协议库服务； 2、性能要求：吞吐量≥4Gbps，最大并发连接数≥40 万，每秒新建连接数≥8000； 带宽性能≥350M； 3、支持策略路由协议、动态路由协议，包括 RIP、OSPF、ISIS、BGP； 4、为了保证员工的工作效率，设备应支持覆盖工作无关应用，移动应用不少于 1000 种，即时消息应不低于 150 种，虚拟货币交易平台不低于 40 种； 5、支持对 Windows 百度网盘客户端的文件标题和内容审计，对 QQ、微信和百度网盘的 PC 客户端外发文件进行关键字过滤和封堵； 6、支持对微信 windows 版客户端进行聊天内容、外发文件进行文件内容等进行审计； 7、可以识别协议数量超过 5200 个，并支持自定义应用规则； 8、售后服务：为保障售后服务质量，提供原厂授权和三年售后服务承诺函,要求提供原厂工程师安装和后期维护。 8、投标人提供产品厂商售后服务承诺函，甲方有权在中标后一周之内要求中标人提供产品测试，对于测试不满足的可予以终止采购。	1	台
工业互联网分类分级安全建设				
1	堡垒主机	1、硬件外型:软硬一体化 1U 标准机架式设备；CPU： 4 核；内存：≥16G；硬盘容量：2T；接口类型：千兆 RJ45 电口*1（管理口）、千兆 RJ45 电口*6、USB 接口*2、consol 口*1；处理性能：最大字符连接≥600 个，最大图型连接≥200 个；管理点数≥200； 2、支持通过动作流配置提供广泛的应用接入支持，无论被接入的资源如何设计登录动作，通过动作流配置即可实现单点登陆和审计接入； 3、支持批量导入、导出用户信息；支持用户手动添加、删除、编辑、设定角色、单独指定登陆认证方式、设定用户有效期； 4、RDP 协议支持 windows 服务端开启安全层 SSL 加密，加密级别符合 FIPS 标准，允许运行使用网络级别身份验证的远程桌面的计算机连接。 5、针对 SSH、Telnet、Rlogin、FTP/SFTP、数据库操作进行记录及审计；记录会话时间、命令执行时间、会话协议、服务端 IP、服务器端口、客户端 IP、客户端端口、操作命令、返回信息、运维用户帐号、审批用户帐号、资源账号等信息；RDP 图形操作过程中键盘输入操作记录和鼠标点击行为记录。 6、售后服务：为保障售后服务质量，提供原厂授权和三年售后服	1	台

		务承诺函,要求提供原厂工程师安装和后期维护。 7、投标人提供产品厂商售后服务承诺函，甲方有权在中标后一周之内要求中标人提供产品测试，对于测试不满足的可予以终止采购。		
2	杀毒软件升级扩容	1、提供物理机/虚拟化服务器的安全防护。支持采集终端基础信息，包括终端名称、IP 地址（私有）、IP 地址（公网）、MAC 地址、健康状态、硬件架构、操作系统、组件等信息； 2、具有包含防病毒，主机防火墙，主机 ID/PS，虚拟补丁功能、抵御病毒、间谍软件、网络钓鱼和其它灰色软件， 3、提供集中的管理、监控、更新和部署等能力，以及可集中管理的客户端防火墙、入侵检测、病毒爆发预防服务、Web 站点信誉服务、预测机器学习、行为监控、勒索病毒防护等功能模块 4、本次升级可以对 500 终端用户，50 个服务器端（包含虚拟化主机服务器的安全防护）开放式许可，三年软件和病毒库升级服务； 5、售后服务：为保障售后服务质量，提供原厂授权和三年售后服务承诺函,要求提供原厂工程师安装和后期维护。 6、投标人提供产品厂商售后服务承诺函，甲方有权在中标后一周之内要求中标人提供产品测试，对于测试不满足的可予以终止采购。	1	套
3	数据库审计系统	1、 审计一体机，软硬一体化 2U 机架式设备，6 电口（含 1 个管理口，1 个 HA 口），1 个接口扩展槽，1 个 RJ45 串口，硬盘≥2T，支持 Oracle、SQL-Server、MySQL 等数据库的审计。支持数据库实例≥20 个； 2、数据库审计：审计 Oracle，SQLServer，MySQL、DB2、Sybase、Informix、PostgreSQL、HBase、MongoDB、DM、kingbase。 3、部署方式：支持旁路镜像、Agent 方式、混合部署和分布式部署方式支持在目标数据库安装 Agent，解决无法通过旁路镜像获取流量的场景； 4、支持数据库自动发现。设备无需添加、即插即用； 5.全局审计与自动基线建立：采用全局及数据库两级设计，便于管理； 6、支持常见的虚拟机环境日志收集。 7、售后服务：为保障售后服务质量，提供原厂授权和三年售后服务承诺函,要求提供原厂工程师安装和后期维护。 8、投标人提供产品厂商售后服务承诺函，甲方有权在中标后一周之内要求中标人提供产品测试，对于测试不满足的可予以终止采购。	1	台
4	日志审计系统	1、软硬一体化 1U 机架式设备，千兆 RJ45 电口*1（管理口）、千兆 RJ45 电口≥6、USB 接口*2、consol 口*1，另支持≥2 个扩展槽位，可扩展万兆接口。内存≥16G，硬盘≥2T， 2、处理性能：日志处理能力 3000 条/秒、日志存储能力 2.5 亿条/秒，Lic 授权数≥200 个； 3、支持 Syslog、SNMPTrap、HTTP、ODBC/JDBC、WMI、FTP、	1	台

		SFTP 协议日志收集。 4、支持使用代理（Agent）方式提取日志并收集。 5、支持目前主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等。 6、支持对 IP 对象的自动发现功能；对自动发现的设备可以转资产或删除； 7、售后服务：为保障售后服务质量，提供原厂授权和三年售后服务承诺函,要求提供原厂工程师安装和后期维护。 8、投标人提供产品厂商售后服务承诺函，甲方有权在中标后一周之内要求中标人提供产品测试，对于测试不满足的可予以终止采购；		
5	态势感知管理平台	1、平台硬件：2U，2*≥CPU（8 核），内存≥128G，系统盘≥256G SSD，硬盘≥16T,具备≥2 个扩展槽，2 个千兆电口，≥2 万兆光口。 2、探针硬件： 2U 硬件架构，双电源，≥6 电口；内存≥16G，硬盘≥4T， 3、支持多个维度的动态实时展示大屏，实时数据展示； 4、具备攻击实时监控界面，支持基于攻击者 IP、受害者 IP、攻击源端口、攻击目的端口、攻击类型、攻击名称等属性作为过滤条件进行网络攻击自定义监控； 5、支持查看基于攻击源 IP 生成的安全事件，支持以时间轴的形式展示攻击者在入侵全过程中各个入侵时间节点中的攻击目标、攻击次数、攻击类型以及入侵阶段； 6、售后服务：为保障售后服务质量，提供原厂授权和三年售后服务承诺函,要求提供原厂工程师安装和后期维护。 7、投标人提供产品厂商售后服务承诺函，以及满足以上功能的承诺函并加盖公章，甲方有权在中标后一周之内要求中标人提供产品测试，对于测试不满足的可予以终止采购；	1	台
6	工业防火墙	1、标准 1U 机架设备，固化千兆电口≥6 个，固化千兆光口≥2 个，设备含 2 对 bypass，冗余电源； 2、性能要求：吞吐量≥4Gbps，最大并发连接数≥200 万，每秒新建连接数≥3 万； 3、主要包括防火墙日志、工业白名单日志、入侵防护日志、URL 过滤日志、防病毒日志、内容过滤日志、用户管理日志、运行日志、系统日志、导入日志，可根据条件类型生成相应的报表。 4、将已抓取包进行回访测试，进行策略验证，帮助用户辨别策略正确性 5、为工业设备或者工控系统提供已知漏洞的虚拟补丁，包含但不限于：西门子漏洞、施耐德漏洞、ABB 漏洞、AB 漏洞、霍尼韦尔漏洞。 6、将一台防火墙从逻辑上划分为多个虚拟系统，每个虚拟防火墙可以被看成一台独立的防火墙设备，拥有独立的系统资源和独立的安全策略，而且能够实现防火墙的大部分功能。 7、支持工业白名单报表、支持防火墙报表、支持接口流量报表、	5	台

		支持入侵防护报表、支持 URL 过滤报表、防病毒报表、内容过滤报表，可根据条件类型生成相应的报表。 8、应具备支持 bypass 功能，当防火墙出现断电时，防火墙内部接口与外部接口直接物理连通，保持内部网络与外部网络之间的正常通信，并及时告警； 9、工控协议白名单策略：支持基于工控流量的白名单自学习，通过自动学习生成白名单列表。白名单支持针对协议的数据过滤，包括 Modbus、IEC104、S7、S7-plus、Bacnet、OPC UA、OPC DA、Ethernet IP 等相关协议。 10、售后服务：为保障售后服务质量，提供原厂授权和三年售后服务承诺函,要求提供原厂工程师安装和后期维护。 11、投标人提供产品厂商售后服务承诺函，甲方有权在中标后一周之内要求中标人提供产品测试，对于测试不满足的可予以终止采购。		
7	交换机	1、交换容量：≥336Gbps (全双工)，包转发率(整机) ：≥132Mpps ，端口：24*10/100/1000TX 以太网端口+4 个 SFP+端口，兼容思科交换机。 2、需配置 8 个 10G SFP 万兆光模块。 3、以太网功能：IRF2 静态 MAC 配置，支持端口镜像和流镜像功能，支持端口聚合(聚合组端口最大 8 个端口)，支持 10GE 口聚合支持端口隔离，支持 STP/RSTP/MSTP，支持 IEEE802.3ad(动态链路聚合)、静态端口聚合，支持 Jumbo Frame 支持 RRPP。 4、VLAN: 支持基于端口的 VLAN，支持 QinQ，支持 Voice VLAN 支持协议 VLAN，支持 MAC VLAN。 5、ARP：支持 ARP Detection 功能，支持 ARP 限速。 6、售后服务：为保障售后服务质量，提供原厂授权和三年售后服务承诺函,要求提供原厂工程师安装和后期维护。 7、投标人提供产品厂商售后服务承诺函，甲方有权在中标后一周之内要求中标人提供产品测试，对于测试不满足的可予以终止采购。	2	台
8	工业安全监测审计系统	1、硬件要求：标准机架式， 1 个 RJ45 串口，1 个 GE 管理口、4 GE 监听接口（电口），固化千兆光口≥2 个，最大检测能力≥600Mbps，整机最大吞吐率≥10Gbps，最大并发连接数≥200 万。 2、系统应可以针对工业协议进行深度解析，能针对工业网络协议的内容和数据进行细致的合规性检查，对于操作指令中包含的针对点表、寄存器、数值的异常操作进行报警，最大限度地保护控制系统的安全，并提供相关审计截图。 3、支持流量审计：支持基于时间、协议、IP 地址等组合流量审计策略。支持统计各 IP 的总流量、上下行流量及 TOP10 排名；针对 IP TOP10 排名，可查看当前 IP 使用的协议及其流量。支持资产识别，源对象，目的对象，信息体具体地址，公共地址，通讯协议识别（功能码的单点，双点特性，读写属性，线圈属性） 4、可对不同行业的规约协议进行精细识别。能自定义对象信息，实现对不同行业规约协议的通讯梳理支撑；	1	台

		5、售后服务：为保障售后服务质量，提供原厂授权和三年售后服务承诺函,要求提供原厂工程师安装和后期维护。 6、投标人提供产品厂商售后服务承诺函，甲方有权在中标后一周之内要求中标人提供产品测试，对于测试不满足的可予以终止采购。		
网络安全服务（三年）				
1	安全巡检	以环境稳定性、安全性为目标针对安全设备进行深入、严谨的日常性评估，并提供可视化报告和统计的一种服务，服务频率：1 年 4 次。	1	项
2	安全漏洞扫描和加固	对用户指定的系统和资产（含工业控制系统）进行安全漏洞扫描，并对需要加固的范围进行确认、配合用户针对安全漏洞进行安全加固、安全产品部署、信息系统安全策略优化，服务频率：1 年 4 次。	1	项
3	安全应急	当安全威胁事件发生后，迅速采取措施和行动，以最快速恢复系统的保密性、完整性和可用性，阻止和降低安全威胁事件带来的严重性影响。	1	项
4	安全运维	协助用户全面运维 IT 资产和主动安全威胁防护，包括基础设施、虚拟化、服务器、应用中间件、数据库、业务系统、网络设备、存储、硬件信息等，集成漏洞扫描、未知新型网络攻击监测。帮助企业快速、有效地建立有序的运维管理体系－－人员、流程、工具，以保障用户业务系统正常稳定运行、降低用户的 IT 运维风险，同时通过联动整合主机终端、网络和数据中心的安全日志，实现威胁发现、智能研判和自动化响应处置的流程，提高安全运维工作效率，专业勒索病毒处置团队，利用勒索病毒研究成果，制定详细的防御计划，包括技术检测和加固，数据保存和备存机制优化，部署成熟有效的杀毒软件，勒索病毒发生后第一时间处置预案。	1	项
5	重大时期保障服务	提供专业安全服务人员安全值守，通过安全检测、监控预警、防护能力建设提升安全防御能力，保障重保期间网络安全	1	项
6	安全服务团队	为了保证网络安全服务的质量，安全服务团队需是原厂资深工程师。	1	项
7	等保测评服务	通过二级等保测评。	1	项
8	工业分类分级测评服务	通过工业分类分级测评。	1	项

6. 项目建设周期及付款：

1、项目建设周期 1 个月，自合同签订之日算起。

2、合同签定后设备进场、开始安装 7 个工作日内付总价的 30%。

3、项目竣工、验收合格后 7 个工作日内付总价的 60%。

4、余款 10%为质保金，质保期 3 年，第一年服务期满后 7 个工作日内

付 3%；第二年服务期满后 7 个工作日内付 3%；第三年服务期满后 7 个工作日内付 4%。

7. 投标文件组成：

1、投标书内容应包括：

（1）工程预算书。

（2）开标一览表。

（3）投标单位的资质证书等。

（4）投标单位营业执照。

（5）法人代表证书或法人代表委托书等。

（6）案例及证明材料。

（7）2020 年度的财务报表。

（8）质保期、质量保证措施以及其它售后服务的承诺。

（9）技术方案。

（10）标函中必须明确施工队伍及负责人（附技术人员简历，实际施工时投标注明人员必须常驻现场）。

（11）电子版投标书。

2、有下列情况之一者为无效标书：

（1）投标书未密封的。

（2）投标书标袋封口上未加盖单位公章或法人代表印章的。

（3）投标书未按招标文件要求编制和投送的。

（4）在评标过程中，评标委员会若发现投标人以他人的名义投标、串通投标、以行贿手段谋取中标或以其他弄虚作假方式投标的，该投标人的投标将做废标处理。

（5）投标人资格条件不符合国家规定和招标文件要求的，或者拒不按照要求对投标文件进行澄清、说明或者补正的，评标小组可以否决其投标。

（6）评标小组将审查每一投标文件是否对招标文件提出的所有实质性要求和条件做出响应。未能在实质上响应的投标，将做废标处理。

（7）投标文件有下述情形之一的，属于重大偏差，视为未能对招标文件作出实质性响应，并按前提条件规定作废标处理：

a、投标文件没有厂商授权的。

b、投标文件没有投标人授权代表签字和加盖公章的。

c、投标文件载明的招标项目完成期限超过招标文件规定的期限。

d、明显不符合技术规范、技术标准的。

e、不按投标清单投标的或擅自修改投标内容的；

f、投标文件载明的检验标准和方法不符合招标文件的要求。

g、投标文件附有招标人不能接受的条件。

h、不符合招标文件中规定的其他实质性要求。

8. 评标：

1、评审小组由招标单位组成。评审小组根据招标文件以及有关规定，对投标单位所报送的有效投标文件从资质、案例、质量、工期、报价、方案等方面进行认真、客观、公正、科学的综合评审，选择项目中标方，招标方不保证最低价中标。

2、招标方向中标方发出中标通知后，同时通知落选的投标商其投标未被接受，并退还其投标保证金。

9. 投标费用：

投标单位应承担所有与编写和提交投标书有关的费用，不论投标结果如何，招标方在任何情况下均无义务和责任承担这些费用。恕不退回投标资料。

10. 对中标单位要求：

1、中标单位在收到中标通知后，必须在中标通知规定的时间内，准时派授权代表到指定地点与买方按中标文件规定的合同格式签订合同，否则按自

动弃权处理，并没收其投标保证金。

2、中标单位不得将标的转包或分包给其他单位或个人，不得搞挂靠和联营，否则除立即终止合同外，对造成的经济损失，皆由中标单位负责。

11. 服务要求

11.1. 质保要求

1) 网络设备均应进行工厂试验，并保证设计和结构满足本招标书要求。
2) 投标方应有确保产品和服务工作符合本招标书各项要求的措施。
3) 供方应提供有关产品检验合格证书。

11.2. 服务保证

1) 投标方应对系统的网络传输技术、工艺设计、环保设计等做出保证，保证其所供应的设备在合同规定的使用期内的各项性能指标优于最新的国家标准。
2) 投标方应保证提供的技术资料的完整统一和内容正确、准确，并能满足设备的设计、安装、调试、运行、维修的要求。
3) 在招标方选用设备恰当和遵守保管及使用规程的条件下，从投标方项目验收之日起 36 个月内，设备因制造质量不良不能正常工作时，投标方应该免费为招标方更换或修理网络设备零件部件，如因此而造成招标方生产损失的，投标方应对其予以赔偿。
4) 设备发生故障，要求原厂人员 30 分钟内响应，4 小时内到达现场，8 小时内恢复使用，如 24 小时内无法修复，提供同型号备用设备保证采购方正常使用至原设备修复，保证使用单位工作不中断。
5) 投标方每年至少进行 2 次回访，并不定期到达用户现场巡回进行用户访问，经常征求用户意见，以加强与用户的联系，不断提高产品质量水平。

11.3. 培训要求

为适应本项目的需要，提高企业员工的综合素质、企业核心竞争力及施工质量等，现根据公司的实际情况和业务需求，特制定出此培训计划。

1）人员事先培训的重要性

人员事先培训，是我公司针对将要实施的项目进行的专项培训，使员工能了

解到本次项目的施工内容，技术难点，工程的总体思路。提升人员施工能力，提高工程施工质量，为提升网络深度覆盖质量，改善用户感知，提升企业品牌效应打下夯实的基础。

2）人员培训目的

培训的基本目的是让施工人员了解本次项目的基本背景情况，了解工作的流程与制度规范，从而帮助员工更快地适应环境和工作岗位，更快地进入角色，提高工作绩效。

3）培训对象

所有参与本次项目的管理人员、技术人员、施工人员。

4）培训方式

岗前培训：指员工在项目开工前，为员工提供有关工程基本情况、操作程序和规范。由培训部门制定培训计划和方案并组织实施，主要通过集中授课、讨论、视听、工程案例分析讨论等多种培训形式展开。

5）培训时间

培训时间：项目验收合格后，安排一周时间集中培训。

6）培训内容

项目相关安全运维知识、安全设备操作保养知识。