华能沾化新能源有限公司

网络安全系统改造工程技术规范书

批准：

审核：

编制：

2022 年 8 月

一、技术标准

本工程的施工及验收应满足相关国家、地方及行业现行的标准、规范，以及在合同实施期间国家、地方及行业对相关标准或规范的修改，以及新颁布的标准和规范。这些标准和规范包括（但不限于）：

《中华人民共和国网络安全法》

《中华人民共和国密码法》

《关键信息基础设施安全保护条例》

《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T 25070-2019

《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）

《信息安全技术 网络安全等级保护定级指南》（GB / T 22240-2020）

《信息安全技术 网络安全等级保护测试评估技术指南》（GB / T 36627-2018）

《公安物联网系统信息安全等级保护要求》（GB / T 35317-2017）

《信息安全技术 公共基础设施 PKI 系统安全等级保护技术要求》（GB / T 21053-2007）

《信息安全技术 信息系统安全等级保护实施指南》（GB / T 25058-2019）

《信息安全技术 网络安全等级保护测评要求》（GB / T 28448-2019）

《信息安全技术 网络安全等级保护测评过程指南》（GB / T 28449-2018）

《信息安全技术 网络安全等级保护安全管理中心技术要求》（GB / T 36958-2018）

《信息安全技术 网络安全等级保护测评机构能力要求和评估规范》（GB / T 36959-2018）

《电力信息系统安全等级保护实施指南》（GB / T 37138-2018）

《信息安全技术信息安全风险评估规范》(GB/T20984 -2007)

《公安机关互联网安全监督检查规定》（公安部 151 号令）

《信息安全技术 工业控制系统安全控制应用指南》（GB/T 32919-2016）

《工业通信网络 网络和系统安全 系统安全要求和安全等级》（GB / T 35673-2017）

《信息安全技术工业控制系统现场测控设备通用安全功能要求》（GB / T 36470-2018）

《电力行业网络与信息安全管理办法》（国家能源局 2014）

《电力行业信息安全等级保护管理办法》（国能安全[2014]318 号）

《华能集团双网建设技术部分工作指南》（华信办函[2010]63 号）

二、项目内容

对公司内外网进行安全改造，对终端进行改造。

三、其他要求

3.1 是否允许联合体：否。

3.2 是否接受代理商：是。

3.3 中标方须按照招标方要求，负责设备的接入与调试，确保设备的技术指标满足招标方的网络分区改造需求。

四、质量保证

4.1 工期要求：中标方保证在合同签订后 7 日内供货、15 个工作日内完成设备接入与调试等工作。

4.2 开箱检查：设备开箱应由厂家与中标方共同进行。

	的危险级别、连接建立时间、连接持续时间、控制端 IP 地址和端口、受控端 IP 地址和端口等 C&C 通道信息。提供各种响应动作：阻断会话、临时阻断和抓包分析等。 可基于 IP 地址、网段、时间、VLAN、协议类型等条件设定 IPS 检测及响应方式。 支持虚拟 IPS 功能，不同的用户可以方便定制满足自身要求的检测模版。 系统应具备网络准入控制能力，通过和终端管理系统联动，拒绝不安全主机连入网络，说明网络准入控制原理和实现效果。 ★系统应支持 venuseye 威胁情报，具备软件著作权 ★威胁情报类型不少于 50 类，至少覆盖安卓恶意程序、APT 攻击、远控木马、僵尸网络、僵尸主机、挖矿、DDOS 攻击、欺诈、赌博、物联网/IOT 攻击网络、物联网/IOT 失陷主机、恶意网站、钓鱼、勒索软件、web 攻击主机、网络蠕虫等。 系统应支持威胁情报，通过通用接口获得第三方的威胁情报，提升防御能力。 系统应支持特殊环境下的攻击源真实地址还原能力。 系统应具备终端和服务器环境感知能力，通过主动扫描和扫描结果导入获得终端环境情况。 ★系统应支持事件响应模版，能够批量修改事件响应动作，包括：事件级别、事件启用开关、动作、日志合并方式、日志开关、抓包取证。 ★系统应支持多种事件响应方式，满足客户的安全要求，需包括：重置、临时阻断、丢弃报文、丢弃会话等动作。 采用先进的模式匹配及协议分析技术实现对网络报文的分析； 具备协议自动识别功能； 支持检测规则自定义功能：自定义参数不低于 100 种。 ★系统应支持常见默认事件集，便于用户使用，默认事件集至少包括：全集、中高级事件、僵尸木马蠕虫事件集、WEB 事件。 事件库应支持 CVE 和 CNNVD 兼容能力。 系统应支持 QQ 和 MSN 应用识别功能，支持黑白名单功能，阻止或允许部分帐号登录。 ★系统应支持密码穷举探测功能，提供至少 20 种密码穷举行为特征探测和阻断。 ★系统应支持弱口令检测功能，需支持至少 8 种网络协议并支持至少 7 种弱口令检测元素，文字说明支持的网络协议和定义弱口令的检测元素。 系统应提供 SQL 注入攻击、XSS 攻击的检测和防御功能，对 Web 服务系统提供保护； ★针对 SQL 注入和 XSS 攻击，设备应支持在线事件分析功能。SQL 注入至少提供攻击位置、攻击方法、解码后数据、攻击域、影响的数据库等，XSS 攻击至少提供协议字段、攻击数据、解码后数据、攻击域、编码方式等，并提供功能截图。 ★系统应针对 SQL 注入、XSS 攻击提供白名单功能。XSS 攻击白名单能够精确到检测点、属性和名称。SQL 注入白名单并支持至少 10 类和 70 个配置项目。 ★系统应支持多种防 web 扫描能力，包括爬虫、CGI 和漏洞扫描等，并支持设置至少 4 个不同级别的扫描容忍度/扫描敏感度。 系统应提供旁路部署及在线、旁路混合部署等部署方式。 系统应支持 IP 地址转换（NAT）功能，包括：源地址转换、目的地址转换、静态地址转换。 系统应支持桥组部署方式，并支持 STP 协议。 系统应支持路由模式，至少包括：静态路由、策略路由、ISP 和 OSPF 路由协议。

	★支持 DHCP 功能，包括 DHCP 服务器和 DHCP 中继功能。并可以作为客户端获得 IP 地址，满足客户自动化管理的需要。 系统应支持端口聚合/链路捆绑协议，并提供手工方式和 LACP 两种配置方式。 系统应支持完善的会话管理功能，可实时查看当前会话状态，支持根据源地址、目的地址、端口号或协议类型查询会话； 系统应支持通过授权扩展支持对 HTTP、FTP、SMTP、POP3、IMAP 协议的病毒检测和过滤功能； 系统应支持通过授权扩展支持对 HTTP、FTP、SMTP、POP3、IMAP 协议的文件屏蔽功能，防止文件的下载和传输。 系统应支持 VLAN、VoIP 数据流病毒过滤； ★系统应支持双病毒引擎，需提供包括国产厂商在内的防病毒引擎厂商合作证明。 系统应支持对文件感染型病毒、蠕虫病毒、脚本病毒、宏病毒、木马、恶意软件等过滤，病毒库数量不少于 30 万。 系统应支持 HTTP 协议和邮件协议防病毒，通过信息替换功能，用以通知用户病毒被阻断，管理员可以自行设置替换信息； 系统应支持 Web 过滤功能，至少支持黑白名单、关键字过滤、禁止 HTTP 代理外，还支持 Script、 Java Applet 等过滤，并能通过统一模版设置， 系统应支持邮件内容过滤功能，有效防止恶意邮件及信息外泄。可根据邮件 SMTP 命令、发件人、主题、附件、IP 及邮件大小进行过滤， ★系统应支持敏感信息防护功能，识别信息和文件中的关键字、身份证、手机号码、固定电话号码、银行卡、IP 地址等敏感信息，并支持文件指纹识别和白名单功能。 并说明支持的应用情况和处理方式。 系统应支持双机热备和双机主备功能，并且主备热备时需支持连接状态和配置同步。 系统应支持硬件 BYPASS。在设备故障、重启及断电的情况下可保障网络畅通，能够手动配置 BYPASS 的启停。 ★系统应支持软件 Bypass 功能，通过 CPU 和内存阈值实现软件 Bypass 的开启，提供不同的阈值计算方式（最高值/平均值、时间区间等）， ★系统应支持重点资产和应用监控功能，当资产和应用出现异常时，通过 syslog 和邮件进行告警，并可以记录日志。 系统应支持多种设备管理方式，包括 HTTPS、CONSOLE、SSH、TELNET 等； ★系统应支持 WEB 登录图像验证码功能，防止暴力破解。 系统应支持在线管理员数目限制和管理员唯一性检查功能，提高系统管理的安全性。 ★需支持动态口令卡或 Ukey 方式的双因子认证，增强配置管理的安全性 系统应支持定期修改密码功能。 ★系统应支持较强的密码安全性，提供首次登录密码修改功能，首次登录时提供强制修改和提醒修改两种方式。 ★系统应提供系统监控和趋势曲线图展示，至少支持内存占用率、CPU 占用率、总流量、每秒新建连接数、并发会话数的趋势图，可按照 1 小时、6 小时、12 小时、1-7 等时间段展示趋势曲线 ★系统应支持历史入侵事件处理功能，直接对历史事件进行分析和处理，并用于未来事件检测。并可以查询处理情况。 ★支持场景分析功能，提供进行更深入的分析能力，至少包括僵尸木马蠕虫的分布式攻击场景分析。 系统应支持本地日志及 SYSLOG 日志发送，支持向至少 3 个 syslog 服务器发送日志。 系统应支持 syslog 格式修改功能，通过对日志内容裁剪、修改次序，满

	足用户安全管理平台日志格式要求。 系统应提供 netflow 日志发送功能，满足第三方管理平台对 netflow 日志的审计需求。 系统应支持声音报警，通过设置事件级别、入侵事件级别和病毒事件进行声音报警。 系统应支持报表个性化设置，通过自定义报表生成单位、报表生成人、单位 logo 和安全摘要信息等信息，快速生成符合单位特点的报告，减少工作量。 系统应提供定期自定发送报表功能，通过邮件将 html、doc、xls、CSV 和 pdf 格式报表发送给管理员。
其他要求	★中标方须提供原厂出具的针对本项目的授权、原厂 2 年售后服务承诺函。

6.2.防毒墙系统（防病毒网关）【2 套】

指标项	技术规格要求
硬件性能	标准机架式，≥6 个千兆电口，2 路 bypass，整机吞吐率≥2Gbps，最大并发连接数≥150 万，病毒检测吞吐率≥1Gbps，企业版病毒库 2 年升级服务许可。产品包修 2 年，软件、规则库升级 2 年升级。
功能参数	必须支持透明、路由、混合、旁路 4 种工作模式，同时支持旁路模式+在线模式部署 支持 802.3ad ，可在透明、路由模式下支持多条链路带宽进行捆绑，支持 LACP 协议，支持 5 种捆绑算法（基于源地址、目的地址、源端口、目的端口等组合 HASH）. 必须支持将任意接口数据完全镜像到设备自身的其余接口，用于抓包分析 ★根据转发策略，支持 8 元组（应用、用户等）进行流量镜像 要求必须支持一对一、一对多，多对多的 NAT，且公网地址池支持轮询和源地址保持两种模式，支持夸协议 NAT 转换，NAT64 支持：IVI、嵌入式地址、地址池三种转换方式，NAT46 支持：IVI、地址方式转换方式 支持基于物理接口、vlan 接口、聚合接口的 NAT 配置策略 ★要求必须支持基于标准 SYSLOG 及二进制 NAT 的日志格式；支持二进制日志外发，支持日志服务器负载，支持 3 种方式。 必须支持所列所有 ALG 应用，包括：H.323、FTP、TFTP、RTSP、PPTP/GRE 必须支持会话控制功能，要求能够基于源、连接数做会话数限制，支持按照用户、应用、时间、接口类型、地址、服务等方式对数据进行访问控制 支持策略命中数统计功能，便于管理员维护访问控制策略， 具备对应用程序的识别和控制能力。应用程序特征库不少于 2700 种，并支持在线更新或手动更新； 支持 P2P 节点识别，支持常见的国际应用 Google Facebook Twitter 等应用 ★支持 IPv4/6 抗应用型 DOS 攻击防护，如 HTTP Flood、DNS query flood 等攻击防护；支持抗流量型攻击防护，如 syn flood、udp flood、icmp flood，tcp flood 等攻击防护 抗常见 DOS 攻击防护，jolt2、land_base、ping_of_death syn flag、tear_drop 、winnuke 、smurf、 ip spoof 等。 支持静态和动态路由，动态路由至少包括：BGP/RIP 和 OSPF 动态路由协议；静态路由协议支持基于源地址、目的地址、源接口的路由；支持 ISP 路由并内置多运营商路由表，支持 ISP 路由 必须支持基于用户、应用等 7 元组的策略路由，必须支持 IPv6 策略路由，必须支持应用引流。

	支持基于 LLB 策略负载分担，支持基于时延、丢包率有效的探测。支持基于连接、基于源 IP 的负载算法。 必须支持 HA 主主 主备模式（抢占和非抢占模式），支持备设备可远程管理、在线升级特征库。 支持 HA 口、心跳口分离，支持聚合口做心跳口。 支持 VRRP、网口联动。 支持 VRF 功能，可支持 1024 个 VRF。 ★支持集中化云向管理，可通过云平台监控设备状态、下发配置等。 支持 Vmware、KVM 虚拟化平台 VM 安装，支持通用服务镜像直接安装。 支持管理黑白名单。 支持特征库、版本批量升级和离线升级，支持 USB 升级。 必须支持在线状态、应用流量、健康信息监控。 支持不少 10 个配置文件存储和恢复。 ★支持 HTTP，FTP，POP3，SMTP，IMAP 协议的病毒查杀、病毒库自动更新、虚拟脱壳、自定义查杀文件大小、查杀可疑病毒、可疑脚本、图片病毒、查杀邮件正文、附件、网页及下载文件中包含的病毒。 实时病毒连接阻断，病毒事件日志记录。 ★预定义 20 种文件类型，支持自定义扫描文件类型，支持常见的压缩格式文件扫描。 ★支持病毒防护沙箱联动功能，能够将灰文件信息同步云端进行分析，并且返回分析结果。 ★支持 200 万余种病毒的查杀，病毒库支持在线或者离线升级。 2 年售后服务，病毒库升级更新。
其他要求	中标方须提供原厂出具的针对本项目的授权、原厂 2 年售后服务承诺函。

6.3. 堡垒机系统【1 套】

指标项	技术规格要求
硬件性能	标准机架式，≥6 个千兆电口，内置 50 主机/设备操作监控许可证，2*1TB 硬盘，支持所有主流图形终端、字符终端、文件传输和数据库管理，图型支持：≥500，字符支持≥1500，支持 HTTP/HTTPS、KVM 和第三方软件（如 Radmin、Pcanywhere），最大 2000 个并发会话连接数。
功能参数	★旁路代理模式，不影响正常业务流量； B/S 架构，采用 HTTPS 方式远程安全管理，无需安装管理客户端； >=100/1000M RJ45*2 个自适应以太网口； 设备内置存储系统，硬盘不低于 2TB，采用 RAID 磁盘阵列； 内置 50 个主机/设备操作监控许可证书； ★图形并发会话数>=100，字符型并发会话数>=400 ★字符型远程操作协议：SSH(V1、V2)、TELNET、RLOGIN、AS400； ★图形化远程操作协议：RDP、VNC、X11； ★文件传输协议：FTP、SFTP； ★数据库远程操作协议：支持 ORACLE、MSSQL、Sybase、Mysql、DB2 数据库远程访问协议审计； ★支持通过应用发布的代理进行协议扩展，支持 Radmin、Pcanywhere、HTTP/HTTPS，可定制开发其它访问协议及客户端支持； ★应用发布代理支持 RemoteAPP 穿透方式，中标方供货时须提供功能截图证明，并加盖原厂公章； ★*Web 访问方式:通过系统的 Web 页面控件直接访问服务器或通过 WEB 页面调用本地工具（含数据库官方客户端）直接访问服务器； 多种类浏览器支持：IE、firefox、chrome、safari；web 访问方式支持历史访问配置参数自动记忆功能； ★web 访问方式支持直接输入目标 IP 快速连接功能；

	★通过 web 方式使用 SSH 协议支持 clone session 功能；支持直接调用 SFTP 功能；支持设定窗口颜色、保存屏幕内容、打印屏幕内容、复制粘贴等功能； 客户端访问方式：支持通过管理员常用的客户端(如 SecureCRT、PUTTY、Mstsc、PLsql、SQLplus 等)直接连接堡垒机再访问到服务器； 支持客户端(SecureCRT、putty)clone session 功能；支持 secure shell client 软件中直接调用 sftp 功能； 登录资源菜单访问：客户端访问审计系统即可显示用户能访问的主机资源菜单，用户通过字符菜单或图形菜单选择列表方式直接访问服务器； 支持多种认证方式：本地密码认证、UsbKey 认证、第三方 CA 证书认证、RSA 动态口令认证、安盟动态口令认证、RADIUS 认证、LDAP 认证、AD 域认证、短信认证以及指纹认证； 支持系统自带的 Usbkey 和 Token 令牌强身份认证模式； ★支持备注模式：运维用户访问服务器前必须先填写该次访问的维护目的等内容，否则不能进行访问操作； ★支持工单授权功能：通过运维人员申请或管理员下发工单的方式来赋予运维人员访问目标服务器的权限，且有工单生效时间限制； 支持设定会话连接单位时间内空闲无操作，连接自动断开；支持运维用户多次登录失败自动锁定账号功能及解锁机制设定； ★支持在线 ping 主机功能，即时获取该主机存活信息； 支持主机账号及协议通道验证功能，即时获知该账号及访问通道是否有效； ★支持主机登录限制，同一台服务器可以只允许一个用户登录，防止已登录用户被登出； 支持以 WEB 在线视频回放方式重现维护人员对服务器的所有操作过程，无须在客户端安装播放客户端软件； 支持关键事件自动生成消息如：二次审批、备注审批、协同操作邀请； ★支持专用消息接收客户端。
其他要求	★中标方须提供原厂出具的针对本项目的授权、原厂 2 年售后服务承诺函。

6.4. 上网行为系统【1 套】

指标项	技术规格要求
硬件性能	标准机架式设备，产品具备至少 6 个千兆电口、2 个千兆光口，内存≥4G，硬盘容量≥128G，支持至少 2 个 USB 口和 1 个 RJ45 串口 网络层吞吐量（大包）≥3Gb，应用层吞吐量≥300Mb，带宽性能≥200Mb，IPSEC VPN 加密性能（最高性能）≥50Mb，支持用户数≥1000，包转发率≥27Kpps，每秒新建连接数≥2400，最大并发连接数≥120000。
功能参数	支持网关模式：支持 NAT、路由转发、DHCP、GRE、OSPF 等功能；支持网桥模式：以透明方式串接在网络中、支持电口 bypass、必须支持多路桥接功能，最多可支持 32 组网桥模式；支持旁路模式，无需更改网络配置，实现上网行为审计，旁路支持主主、主备模式部署； 支持部署在 IPv6 环境中，设备接口及部署模式均支持 ipv6 配置，所有核心功能（上网认证、应用控制、流量控制、内容审计、日志报表等）都支持 IPv6； 可设置四类管理员，分别为系统管理员、安全管理员、审计管理员，以及多种权限的超级管理员；管理员支持分级，高级别管理员的策略配置优先生效，并可修改低级管理员的策略； 支持首页分析显示接入用户人数、终端类型；资产类型分布、新设备发现趋势、终端违规检查项排行、终端违规用户排行；带宽质量分析、实时流量排名；泄密风险、工作效率、共享上网等行为风险情况； 支持从本地导入和扫描导入，支持以 CSV 格式文件导入帐户/分组/IP/MAC/描述/密码等信息 支持 LDAP、Radius、POP3 等第三方认证；支持 ISA\lotus ldap\novel ldap\oracle、sql server、db2、mysql 等数据库等第三方认证

	支持终端分类可视：1.对网络接入的终端进行可视化管理，展示终端详细信息、异常状态等 2.支持查看终端类型，以及终端详细信息（厂商，系统，端口等）；3.支持查看终端类型分布； 支持 20 款以上主流杀毒软件的运行情况、软件版本、病毒库更新时间检查，对不满足检查要求的终端可重定向页面修复、弹窗提示、限制权限、禁止上网； 在无安装客户端时，通过流量状况检查 10 款以上主流杀毒软件的运行情况，对不满足检查要求的终端可重定向页面修复； 支持终端登录域检查、操作系统检查、进程检查、文件检查、注册表检查、补丁检查、管理员账号检查、自定义任务检查等。 设备内置海量预分类的 URL 地址库，能够针对各种 URL 类型做识别和分类，同时所有 URL 类型都支持区分“网站浏览”、“文件上传”、“其他上传”、“HTTPS”等细分行为并分别做权限控制；URL 数量在 2000 万以上，包含分类数量 150 个以上； 禁止使用代理：1.不允许使用外部 HTTP 代理；2.不允许使用外部 Sock4/5 代理；3.不允许在 HTTP, SSL 一些的标准端口上使用其他协议；（比如在 80 端口上传输非 HTTP 协议数据，在 443 端口上传输非 HTTPS 协议数据等）； 支持通过抑制 P2P 的上行流量，来减缓 P2P 的下行流量，从而解决网络出口在做流控后仍然压力较大的问题； 能够实时看到各级流控通道的状态：包括所属线路、瞬时速率、通道占用比例、用户数、保证带宽、最大带宽、优先级，启用状态等。 中标方在供货时须提供功能截图证明，并加盖原厂公章。
其他要求	★中标方须提供原厂出具的针对本项目的授权、原厂 2 年售后服务承诺函。

6.5 交换机【2 台】

指标项	技术规格要求
硬件性能及功能参数	24 个 10/100/1000Base-T 以太网端口，4 个 SFP，4 个 SFP 光模块，4 对单模光纤跳线，无风扇自然散热，静音，交换容量 336Gbs/3.36Tbps 内置 AC 电源，包转发率 51/126Mpps，原厂 2 年包修服务

6.6 交换机【2 台】

指标项	技术规格要求
硬件性能及功能参数	48 个 10/100/1000Base-T 以太网端口，4 个万兆 SFP，传输速率：10/100/1000Mbps，背板带宽 432Gbps/4.32Tbps，包转发率 144/166Mpps，端口数量 52 个，支持 4K 个 VLAN，支持 Guest VLAN、Voice VLAN，支持 GVRP 协议，支持 MUX VLAN 功能，支持基于 MAC/协议/IP 子网/策略/端口的 VLAN，持 1:1 和 N:1 VLAN Mapping，支持对端口速率限制，支持报文重定向，每端口支持 8 个队列，支持基于端口的流量监管，支持双速三色 CAR 功能，支持 WRR、DRR、SP、WRR+SP、DRR+SP 队列调度算法，支持报文的 802.1p 和 DSCP 优先级重新标记，支持基于队列限速和端口整形的功能功能，支持 PIM DM，PIM SM，PIM SSM，支持 IGMP v1/v2/v3 Snooping，支持可控组播，支持 VLAN 内组播转发和组播多 VLAN 复制，支持捆绑端口的组播负载分担，支持基于端口的组播流量统计，支持 MLD v1/v2snooping（Multicast Listener Discovery snooping），网络管理 支持智能堆叠 iStack，支持虚拟电缆检测(Virtual Cable Test)，支持 Telnet 远程配置、维护，支持 SNMPv1/v2c/v3，支持 RMON，支持 eSight 网管系统、支持 WEB 网管特性，支持 HTTPS，支持 LLDP/LLDP-MED，支持系统日志、分级告警，支持 802.3az 能效以太网 EEE，支持 sFlow，安全管理 用户分级管理和口令保护，支持端口隔离、端口安全、Sticky MAC，支持 MFF，支持防止 DOS，ARP 攻击功能，ICMP 防攻击，支持黑洞 MAC 地址，支持 MAC 地址学习数目限制，支持 IEEE 802.1X 认证，支持 AAA 认证，支持 Radius、HWTACACS 等多种方式，支持 SSH V2.0，支持 HTTPS，支持 CPU 保护功能，支持黑名单和白名单，支持 DHCP Relay、DHCP Server、DHCP Snooping，支持 DHCPv6 Relay、DHCPv6 Server、DHCPv6 Snooping，支持用户认证点和策略执行点分离，原厂

	2年包修服务

6.7 数码复印机【1台】

指标项	技术规格要求
硬件性能及功能参数	标配输稿器+内置装订器+双纸盒+工作台 。A3彩色激光数码复印机，复印/打印方式 激光静电转印方式，感光材料 OPC，显影系统 干式双组分显影 定影系统 高级彩色快速定影技术，内存标配 3.5GB，SSD 固态硬盘 256GB，预热时间 主机电源打开时 10秒以内或更少，睡眠模式恢复时 10秒以内或更少快速启动 4秒或更少，最大原稿尺寸 A3，首页输出时间，(A4，BW/CL)，6.1/8.4s 或更少，灰度等级 256级，分辨率复印 600dpi x 600dpi，打印 1,200dpi x 600dpi,1,200dpi x 1,200dpi (half-speed) 复印倍率 固定倍率 25%，50%，61%，70%，81%，86%，100%(1:1)，115%，122%，141%，200%，400%，手动缩放 25% - 400%（以1%为单位），连续输出速度 iR-ADV DX C3826 26ppm，连续复印张数 1 - 999张，供纸量（80g/m2） 标准双纸盒 550张 x 2+100张（多功能托盘），选配 550张 x 2(with Cassette Feeding Unit-AW1)，纸张厚度 纸盒1&2 52 to 256 gsm，纸张类型 纸盒 1 A4，A5，A5R，A6R，B5，16K，ISO-C5，自定义：105.0 x 148.0 mm to 297.0 x 215.9 mm，纸盒2 A3，A4，A4R，A5，A5R，A6R，B4，B5，B5R，8K，16K，16KR，COM10 No.10，Monarch，DL，自定义：105.0 x 148.0 mm to 304.8 x 457.2 mm。电源 220-240V 50/60Hz 5A，原厂2年包修服务。主要组件：双面自动扫描输稿器-BA1（选配），原稿输送方式 自动文档输稿器，原稿尺寸 A3，A4，A4R，A5，A5R，B4，B5，B5R，B6，8K，16K，自定义尺寸：139.7 x 128 mm to 297.0 x 431.8 mm，原稿扫描速度 单面：70/70 (300 x 300 dpi，send)，51/51 (600 x 600 dpi，copy)，双面：35/35 (300 x 300 dpi，send)，25.5/25.5 (600 x 600 dpi，copy)，扫描分辨率（dpi） 600x 600，原稿托盘容量 100页（80gsm），双面同步扫描输稿器-C1（选配），原稿输送方式 自动文档输稿器，原稿尺寸 A3，A4，A4R，A5，A5R，A6R，B4，B5，B5R，B6R，8K，16K，自定义尺寸：69.9 x 139.7 mm to 304.8 x 431.8 mm，原稿扫描速度 单面：135/135 (300 x 300 dpi，send)，80/80 (600 x 600 dpi，copy)，双面：270/270 (300 x 300 dpi，send)，160/90 (600 x 600 dpi，copy)，

	扫描分辨率（dpi） 600x 600，原稿托盘容量 200 页（80gsm）。

6.8 服务器【3 台】

指标项	技术规格要求
硬件性能及功能参数	2U,机架式,CPU Intel Xeon Silver, CPU 线程数 20 线程,CPU 频率 2.2GHz4210,主板芯片组 Intel C621,智能加速主频 3.2GHz,标配 CPU 数量 2 颗,制程工艺 14nm,三级缓存 13.75MB,CPU 核心 10 核,扩展槽 最大支持 6 个标准 PCIe,内存类型 DDR4,内存容量 64GB,内部硬盘架数前置支持 12 块 3.5 英寸硬盘或 25 块 2.5 英寸硬盘，后置 2 块 M.2 硬盘或 2 块 2.5 英寸 SATA 硬盘，标配 2TSATA*6,1G 缓存 RAID 卡，热插拔盘位 12 个热插拔硬盘槽位，磁盘控制器 RS0820P(2G 缓存),/1000M*2/双电源/导轨，系统管理 主板集成 BMC 管理芯片，标配 KVM 功能，提供 1 个独立的 1Gb 网络 RJ45 型管理端口，网口速率支持 10/100/1000M 自适应切换；支持外插自研网卡提供 NCSI 功能，显示芯片 AST2500 BMC 芯片，标准接口 1 个前置 USB3.0+1 个前置 USB 3.0（支持 USB2.0 和外插 LCD 液晶管理模块），2 个后置 USB 3.0 2 个 VGA（1 个前置，1 个后置） 1 个后置千兆管理网络接口，网络控制器主板通过 PHY 集成 2 个高性能千兆网,windows sever 2019 ， 其中一台服务器部署补丁分发平台。原厂 2 年包修服务。

6.9 视频会议主机【1 套】

硬件性能	技术规格要求
功能参数	★视频输入接口 1xHT-RX3xHDMI， ★视频输出接口 3xHDMI， ★音频输入接口 1xHD-AI（2 级）1x 卡农头 1xHDMI（音频输入）2xRCA， ★音频输出接口 4xRCA3xHDMI（音频输出）， ★网络接口 2xUSB 2.0 A 口 2x10/100/1000M LAN1xPOE 网口 2xRJ45 串口 带宽要求 IP：64kbps-8Mbps 其他特点 音频协议：G.711A/G.711U/G.722/G.722.1C/G.729/Opus/AAC-LD 视频协议：H.263/H.263+/H.264 HP/H.264 BP/H.264SVC/H.265 辅流协议：H.239/BFCP ★活动双流：4K30+4K30，1080P60+1080P60（4K15） ★数据会议：1080P 60 4K30 音频特性：快速回声消除（AEC），自动噪声抑制（ANS），自动增益控制（AGC），语音清脆化（VoiceClear），语音增强（AudioEnhancer），唇音同步 安全性：网络适应性 超强纠错（SEC），丢包重传（ARQ），视频前向纠错（FEC） 安全性管理信令 H.235/TLS 加密,媒体 SRTP 加密会议接入加密,会议控制加密,管理员加密 SSH/HTTPS 传输加密，双流加密 其他接口：1xWIFI(内置)，1x 蓝牙(内置) 工作频率：50Hz-60Hz ★麦克风：2 个 麦克风参数：拾音距离 6 米 拾音范围：360° ★麦克风接口：HDAI ★含控制 touch1 个 摄像头性能参数： ★摄像头：2 个 ★视像分辨率 4K25/30、1080p50/60、1080p25/30 ★镜头变焦：12 倍光学 ★输出接口：1×HDMI 接口 1×USB 接口 1×HT-TX 接口 2×RS232 串口

6.10微机【20台】

指标项	技术规格要求

功能参数	处理器：I7-10700，内存：≥8G，硬盘：1TB+256G，系统版本：win10 专业版，有线网卡：千兆网卡，不含显示器，2 年包修。

6.11 笔记本【2台】

指标项	技术规格要求
功能参数	处理器：i7-8565u，内存≥16GB，硬盘：512GB 固态硬盘，尺寸：/13.3 英寸，显卡：集成显卡，摄像头：红外摄像头，电源：48WH，系统版本：win10 操作系统 ，FHD，指纹，2 年保修。

6.12 机柜梳理【1项】

指标项	技术规格要求
工作内容	根据边界安全清晰，弱电强电分离走线，整齐美观，运维方便等原则，对 6 个网络机柜与 6 个服务器机柜内设备及走线重新优化布局，线路梳理，标签标识，包含提供相应附材。

6.13机架式光纤收发器【2项】

指标项	技术规格要求
基本要求	标准机架式，14 个插槽，满配单模、单芯（7 发、7 收）光纤收发器。

6.14第二接入网（第二套调度数据网）的安全改造接入【1项】

指标项	技术规格要求
基本要求	根据省调要求，实施第二接入网（第二套调度数据网）的改造接入，项目内容包含调度数据网的路由器、交换机、纵向加密等设备配置与接入。

加“★”项为必须满足项，必须提供证明材料，否则按无效标处理。

七、供应商职责

7.1供应商进场前，针对采购方提出的报审资料不合格项，供应商应在规定时间内予以补充完善，直至满足要求为止

7.2负责整个项目的安全、质量及进度；

7.3供应商委派的技术人员必须提供供应商方出具的正式委派单（或其他证明材料），且具有相应的工作经验及技术能力，对现场设备较为熟悉。

7.4 负责对对孔洞进行封堵。

7.4合同要求的工作内容全部完工后，供应商按完工有关规定，向采购方代表提供采购方代表签字完工报告；

7.5在本项目施工范围期间，供应商现场食宿自理，供应商人员交通由供应商自行解决，所配备车辆应满足现场道路交通条件；

7.6开工前，供应商必须进行全面的安全技术交底，并结合工程实际制定保证安全的技术、安全措施，使全体施工人员均掌握工程特点及所有安全措施及安全注意事项。

7.7供应商接受采购方的安全监督、管理和指导。

7.8供应商承包的项目，必须自行组织施工，严禁转包及未经采购方批准的分包。

八、验收

8.1项目验收

（1）供应商应对所有正式交付件的综合质量审查负责，指定各交付件的相关责任人，明确相关职责；

（2）供应商应提交验收流程、验收方法和验收依据；

8.2项目文档

（1）供应商提供的资料应使用国际单位制（SI），语言为中文；

（2）资料的组织结构清晰、逻辑性强。资料内容要正确、准确、一致、清晰完整。如所供资料不能达到要求时，供应商应免费给予补充；

（3）供应商资料的提交应及时充分，满足项目进度要求；

（4）对于其它没有列入合同技术资料清单，却是项目所必需的文件和资料，一经发现，供应商应及时免费提供；

（5）供应商完成项目后应提供网络拓扑图、安装调试报告、培训资料。

九、质保

质保期为合同完工时签订验收证书之日起1年，出现任何质量问题，供应商应在采购方通知之时起48小时自负费用进行修复，每延迟一日，按照工期延误的相关约定承担违约责任。

十、工程清单

序号	工程名称	工程内容	数量	备注
1	内网改造工程	防病毒网关1套，堡垒机1套，服务器3台，24口以太网交换机2台，48口以太网交换机2台，视频会议主机1台，数码复印机1台，内网微机20台，光纤收发器池2只。对现有1台WEB应用防火墙WAF、1台IPS、1台防火墙二年特征库升级、软件升级、产品维保。具体要求详见工程技术要求。	1项	
2	外网改造工程	交换机1台，入侵防御系统1套，防病毒网关1套，上网行为管理系统1套，笔记本2台。具体要求详见工程技术要求。	1项	
3	第二接入网（第二套调度数据网）的安全改造接入	根据省调要求，实施第二接入网（第二套调度数据网）的改造接入，项目内容包含调度数据网的路由器、交换机、纵向加密。	1项	
4	机柜内设备线缆规范化安全梳理	根据边界安全清晰，弱电强电分离走线，整齐美观，运维方便等原则，对6个网络机柜与6个服务器机柜内设备及走线重新优化布局，线路梳理，标签标识，包含提供相应附材。	1项	