服务器集群虚拟化、网络安全建设和运维服务技术要求

重庆长征重工有限责任公司

2023-6-8

目录

1 项目概况

1.1 项目范围

序号	项目	项目名称	数量（台/套）	规格型号	承包方式	交货期	交货地点
1	项目一	服务器集群虚拟化和运维服务	1 套	详见第 2.2 章节“项目一（服务器集群虚拟化和运维服务）”	交钥匙工程，投标方总承包，负责项目的设计、建设和售后，设备的制造、包装、运输、就位、安装、调试、培训和运维等工作。	合同签约生效后**2个月**	重庆长征重工有限责任公司
2	项目二	网络安全建设	1 套	详见第 2.3 章节“项目二（网络安全建设）”	交钥匙工程，投标方总承包，负责项目的设计、建设和售后，设备的制造、包装、运输、就位、安装、调试、培训和运维等工作。	合同签约生效后**2个月**	重庆长征重工有限责任公司

1.2 概述

1.2.1 存在问题

（1）整体网络结构问题

网络架构较为混乱，不便于扩容和维护管理：园区网在建设初期，设备和光纤/电缆随意布放，缺乏统一的网络分层规划管理，网络拓扑相对混乱，不便于对网络性能瓶颈进行正确评估和有效扩容，给日常网络管理也带来很大难度。

网络可靠性规划不合理，影响企业生产和经营管理、造成投资浪费：由于缺乏有效的园区网规划，对于网络可靠性考虑不够，网络中既存在单点故障导致网络可靠性低、影响企业生产和经营管理行为；同时也存在网络过度冗余、造成投资浪费的现象。

（2）服务器及系统应用问题

目前我公司应用系统仍然是采用直接部署在单台物理服务器上运行方式，存在资源利用率低下、业务连续性差、稳定性低、能耗高、灵活性（扩展性）差等诸多问题。当一台业务系统服务器出现硬件故障的时候，会影响整个公司的这个业务系统运转。

（3）数据备份

缺乏一套稳定、高效的备份系统来满足数据中心所有业务系统的数据保护需求,以及应对各种数据丢失风险或数据安全问题的挑战。目前采用的数据备份手段为，系统软件数据库为实时备份；整体数据外部备份为一个月人工进行手动备份方式，存在效率低下而无法保证两次备份时间窗口之间因系统或业务崩溃而造成的数据丢失风险和问题。

（4）数据传输问题

业务数据传输、数据交换等没有根据业务和用途划分有效、识别区域，全在核心交换机上发生数据交换，并缺乏对全网数据流量直观、清晰、可视化的统一管理手段。

（5）网络安全问题

系统性不强，安全防护仅限于网络安全，关于系统、应用和数据的安全存在较大的风险；

计算机应用系统对网络的依赖性增强。计算机网络规模不断扩大，网络结构日益复杂。计算机网络和计算机应用系统的正常运行对网络安全提出了更高的要求。

园区网对于内部和外部用户缺乏有效的身份认证手段、用户可随意接入网络，网络层面的安全保证和防御措施也不到位，造成园区网的脆弱和易攻击。对终端安全、防病毒、防入侵等等完整的防护措施是缺失的。

（6）互联网连接问题

原有的网络安全产品在功能和性能上都不能适应新的形势，存在一定的网络安全隐患，产品亟待升级。对于企业用户访问外网进行安全行为审计等；企业多出口链路场景下的负载均衡、灵活选路需求。传统园区网建设缺乏有效满足这些增值业务需求的统一解决方案考虑，解决这些业务存在园区网络分散建设、重复投资的问题。在招标方移动端系统上线之后，其应用服务器及数据服务器必定是部署在招标方厂区内，如何保证其在互联网上的数据安全。

信息系统不仅需要安全可靠的计算机网络，也需要做好系统、应用、数据各方面的安全防护。为此，要加强安全防护的整体布局，扩大安全防护的覆盖面，增加新的安全防护手段。

（7）管理维护困难

缺乏简单有效的网络管理系统，企业 IT 网络运维部门面临很大压力：当前，园区网 IT 运维部门面临很大的网络运维压力，来自于园区网内外部的安全事件频发、网络可靠性低引发的网络业务中断现象，网络故障诊断、分析定位过程对于 IT 运维人员的技术能力和经验水平要求较高，缺乏简单有效/低成本的图形化

网管工具、进行实时网络拓扑显示、状态监控和各种故障事件预警/告警展示。另外，IT 运维部门也需要实施统计园区网各路径的流量信息，便于对网络带宽进行管理和规划，给后续网络扩容提供参考。

1.2.2 需求说明

公司目前正在运行和后续建设上线的 OA、ERP、PLM、能源管理等系统，以及数十台交换机和服务器等设备组成的园区网络。

根据公司目前存在的信息化问题，并组合实际情况，对现有的服务器、交换机等硬件资产需参照**信息安全等级保护 2.0 三级安全防护**为标准对公司的信息化现状进行梳理、分析;按标准进行查缺补漏等，根据信息系统存在的问题进行整改，并提供详细的解决方案。硬件平台应当满足公司信息管理基础平台应用系统运行需求，提供基本的计算、存储、网络等资源，并适度考虑未来 3~5 年业务增长带来的资源需求挑战。具体需求如下：

（1）本次需要建设完善的网络架构，并对公司联网设备进行分区分域分类管理，并通过交换机划分 VLAN 的方式进行逻辑隔离，以及一些特殊的业务系统通过物理隔离方式实现。

（2）采取服务器虚拟化的方式来解决业务应用系统统一部署和硬件资源高效利用。通过部署硬件负载均衡或软件负载均衡两种不同解决方案来应对高可用性及高并发需求的挑战。

（3）建设一套主数据中心存储和备份存储，数据备份系统要求备份服务器区全部数据（包含虚拟机、应用系统、文件、数据库），保证在主数据存储出现宕机时备份存储能保障业务继续运行。部署和建设一套 16Gbps 的光纤存储区域网络架构（FC-SAN），来满足业务系统与统一共享存储的高速访问。

（4）针对公司目前存在的网络风险建设一套完整的防护，防火墙、入侵防护系统、终端安全管理系统、网络准入系统、防病毒系统、日志审计系统、数据库集群等。

（5）针对网络管理困难问题，建设一套 NTP 时间同步服务器、IP 地址管理、DHCP、DNS 服务器、网络节点（交换机）管理、服务器管理、虚拟机管理、数据库管理等一系列管理措施。

（6）对本次的互联网网络以及灾备平台进行规划设计。

（7）针对本项目建设内容与后续运行情况，特别是涉及到招标方应用系统（包括但不限于 ERP、PLM、OA、MES、能源管理系统等）制定一套详细的运维管理方案（包括服务响应、定期巡检、技术保障、实战（网络安全、数据恢复）演练）。

（8）针对招标方人员制定详细的人员培训方案。

1.3 设计原则

（1）规范性原则

本次项目在规划、设计、建设过程中，应遵循国家相关法律、法规，严格执行国家有关规范标准。

（2）可靠性原则

为保证公司整个业务和网络 7×24 小时不中断，所选用设备和软件等应具有极高的可用性，确保业务的连续性和数据的安全性和实时性。

（3）先进性原则

本次项目在建设过程中应采用国际先进的设备与技术，满足当前信息系统和网络使用的业务需求，兼顾未来的发展扩充，一是要适应信息化快速发展和高速的数据传输需要，二是要应对网络上层出不穷的病毒、木马、漏洞攻击等网络威胁，三是适应随着信息化发展暴增的数据量，四是整个网络架构要应对公司复杂的网络需求。

（4）安全性原则

在整个项目中应该考虑服务器安全、业务系统安全、网络安全、数据安全以及保密性等，一是要注意各种防护措施，二是出现问题要能快速响应和排除。

（5）可集成性原则

在整个网络架构中，各种硬件资源、业务系统、防护措施等要有良好的集成性，不能出现业务和网络冲突、误杀进程、正常访问阻挡等问题。各类资源良好协同，营造畅通、安全、快速响应的网络环境。

（6）可扩展性原则

对在整个网络架构中的扩展性来说，一是服务器集群要能灵活增加实体服务器实现资源叠加使用，虚拟机中的业务系统也要能灵活增加。二是数据存储根据公司实际需要可扩展。三是网络节点根据需求可自定义增加和减少。四是网络中的整个防护措施要能根据不同的业务和网络节点进行扩展和分割。

（7）经济性原则

在满足招标方整个网络架构和各业务系统的使用需求下，充分利用公司现有的网络线路、服务器、交换机、软件等资源，用最小的经济代价实现最大化收益，不要出现资源浪费等情况。除目前急需建设的软硬件之外，其余部分可分阶段实施。

1.4 建设目标

（1）提供基本的计算、存储、网络硬件环境保障

硬件平台应当满足招标方信息管理基础平台及业务应用系统的运行需求，提

供基本的计算、存储、网络等硬件环境，并适度考虑业务增长带来的计算与存储需求。

（2）信息安全保障

保证本次的整体设计方案参照**信息安全等级保护 2.0 三级安全防护**设计。由招标方决定哪些内容分阶段实施。

信息系统安全包括物理安全、网络安全、数据安全、应用安全、安全制度等内容，保障招标方信息管理基础平台的安全、平稳运行和数据信息的安全管理与应用。

（3）高效运行

服务器集群与存储之间采用≥16Gb 的光纤网络连接，业务网络采用≥万兆网络连接。

信息平台应面向全公司业务操作用户，对 OA、ERP、MES、财务等相关业务系统提供安全、稳定、高效运行服务。总体性能原则上要求普通功能系统响应时间应小于 3s，高并发响应时间小于 5s；OA 类功能系统响应时间应小于 2s，高并发下应小于 3s。

（4）稳定持续运行

整体规划信息管理基础平台将采用服务器虚拟化作为核心技术，也直接关系到公司的综合业务系统是否能正常运行，必须保证 IT 系统 7×24 小时正常运行（维护时间除外），保证 99.9%的可用度。

（5）数据备份及数据恢复

①等级指标

要建设容灾系统，就需要相应的指标，作为衡量和选择容灾系统解决方案的参数。根据灾备建设国家标准 GB/T 20988-2007 《信息系统灾难恢复规范》，灾备系统建设可分六级。

根据招标方信息管理基础平台建设要求，应当按照国标要求**≥第五等级**的标准来规划建设。

②恢复时间目标（RTO）和恢复点目标（RPO）目标

信息系统灾难恢复能力等级与恢复时间目标（RTO）和恢复点目标（RPO）对应关系：

恢复能力等级	恢复时间目标（RTO）	恢复点目标（RPO）
1	2 天以上	1 天至 7 天
2	24 小时以后	1 天至 7 天
3	12 小时以上	数小时至 1 天
4	数小时至 2 天	数小时至 1 天
5	数分钟至 2 天	0 至 30 分钟
6	数分钟	0

以上是规范给出的某特定行业灾难恢复能力等级与 RTO、RPO 之间关系的示

例。 参考上面的标准，以及投资与实际需求的最佳平衡点应达到最高的性价比要求，招标方信息管理基础平台应当以**≥第五等级**的标准来规划和建设。

（6）管理运维目标

在运维管理及各种管理系统中，对各种服务器、虚拟机、数据库、存储、交换机、终端等设备要实时监控，出现问题能**立即**定位。

增加局域网内网络设备时间同步功能，解决局域网内连接设备的时间不一致问题。

运维服务和技术支持详见本文件第 6 节“运维服务和技术支持”。

1.5 设计依据

按照招标方实际业务使用需求，集团公司以及国家和政府要求建设。

招标方目前为内部网络，暂无与外界网络通信需求。根据招标方目前有的软硬件资源和未来业务需求制定本建设方案。

1.6 引用标准

《信息系统灾难恢复规范》（GB/T 20988-2007）；

《计算机信息系统安全保护等级划分准则》（ GB17859-1999 ）；

《信息系统安全等级保护实施指南》（ GBT 25058-2010 ）；

《信息系统安全保护等级定级指南》（ GB/T22240-2008 ）；

《信息系统安全等级保护基本要求》（ GB/T22239-2008 ）；

《信息系统等级保护安全设计技术要求》（ GB/T 25070-2010 ）；

《信息安全技术 信息系统安全等级保护测评要求》；

《信息安全技术 信息系统安全等级保护测评过程指南》；

《信息安全技术 信息安全风险评估规范》（ GB/T 20984-2007 ）；

《信息安全技术 信息系统安全管理要求》（ GB/T 20269-2006 ）；

《信息安全管理体系要求》（ GB/T 22080-2008 ）；

《信息安全管理实用准则》（ GB/T 22081-2008 ）；

《信息系统通用安全技术要求》（ GB/T 20271-2006 ）。

2 项目主要内容、技术参数要求、及数量概述表

2.1 项目选型总体要求

（1）**投标方所投主要系统及设备选型最低必须为知名一线品牌优质产品，技术参数应满足或优于下述详细列表参数要求，所选品牌应选用推荐品牌或同档次品牌产品，或选用高于推荐品牌档次产品。**

（2）主要系统（虚拟化系统、备份系统、数据库、网络准入系统、终端安全管理系统、防病毒系统）和主要设备（主数据中心存储、FC 交换机、防火墙、堡垒机）应选用成熟产品并具有类似本项目的广泛成功案例**（提供不少于两个的合同复印件）**。

（3）主要系统及使用的设备、材料等必须符合国家法律法规和现行相关标准要求，并经具有资质的检验、认证机构检测或认证合格。主要参数和主要功能应按国家相关要求提供检测报告或证明材料。

（4）投标方投标中主要设备和主要系统，提供原厂授权书及售后服务承诺书（详见本章节清单），强制性认证产品必须具备 3C 认证证书，网络安全相关设备（如：防火墙、防病毒系统、终端安全管理系统、网络准入系统、堡垒机）必须严格遵守国家的强制性认证要求并取得相关证书。

（5）投标方负责所选各系统的无缝集成，整套系统设计要求具有高度的可靠性，系统整体设计和产品选型能够确保各子系统、各产品有效集成；各主要软硬件产品最终使用授权必须为正式授权，不接受临时授权或短期授权产品。

（6）主要系统及设备需求以评审通过的最终设计和实际建设需求为准；投标方须根据现场勘查和招标方实际需求，对各子系统及工程进行合理设计。**若因投标方设计问题，在建设过程中出现系统、设备或材料不足或缺失，由投标方按需免费补充。**

（7）投标方在偏离表中对本项目招标技术要求的相关系统功能要求进行一对一响应，说明“符合”“正偏离”“负偏离”的内容，作为评标依据**（其中带“★”参数为否决项，其中带“▲”参数为重点打分项）**。若本章节“技术参数要求、功能需求及数量概述表”未提及或经现场勘察后发现与现场实际情况不符的，投标方可提出质疑并提出合理的调整方案，经招标方确认后统一进行调整，各投标方可自行踏勘。

（8）投标方可根据自身条件选择对招标方的项目一（服务器集群虚拟化和运维服务）和项目二（网络安全建设）进行响应和报价，**注意报价时需将两个项目分开单独报价**。项目的中标方在签订的合同范围之内必须无条件配合招标方的集成和运维工作。

2.2 项目一（服务器集群虚拟化和运维服务）

2.2.1 软硬件设备清单

序号	设备名称及建议品牌	主要技术（性能）指标或规格要求	单位	数量	单价（元）	总价（元）
1	主数据中心存储 建议品牌：Dell EMC PowerStore、H3C CF、华为 Dorado、神州云科 Yk、联想 DM 等一线品牌	1、★控制器：“双活”（Active-Active）双控控制器工作设计，任何卷都可以从任何控制器的任何目标端口进行访问，本次配置两个控制器；整机最大可配置≥2 颗 CPU，本次配置≥2 颗 CPU，整机 CPU 核总数≥24 核（物理核心数）。控制器支持本地可升级； 2、★前端端口：支持 SAN 及 NAS 环境，且不需要增加额外的硬件组件即可支持 FC/ISCSI/NFS/SMB（CIFS)等协议。最大支持的 FC 端口≥20 个；最大支持的 10Gb iSCSI 端口≥16；本次配置≥8 个 16Gb （或 32GB）FC 端口，≥4 个 10GB（或以上）光口； 3、★控制器系统物理内存：存储控制器整机可支持物理内存总量≥192GB，非闪存卡或 SSD 扩展方式，提供缓存中数据断电保护功能，且单控制器失效不影响正常控制器的缓存功能。本次配置物理内存≥192GB； 4、★容量：最大支持裸容量≥3PB，支持增加磁盘扩展柜；支持≥7TB 和≥15TB（全闪存储）大容量的闪存盘，本次配置硬盘容量≥48T（采用 NvME SSD 硬盘），单盘容量≤4T； 5、▲可靠性：硬件全冗余，无单点故障，达到≥99.9%可用性；保证在某硬件出问题时，能够进行自动切换，不出现单点故障；支持在线更换磁盘、电源等部件； 6、▲RAID 保护方式：实配动态 RAID 技术，可单盘扩充容量，无需专用热备盘，硬盘失效后剩余硬盘可同时参与数据重构速度快； 7、支持操作系统：支持 AIX、Solaris、HP-UX、Linux、Windows、VMWare 等主流操作系统； 8、▲软件功能配置：配置全容量统包所有软件许可，包含后期扩容容量； 9、统一拷贝数据管理功能：免费提供利用存储端负载创建与数据库等应用一致性快照管理的图形化软件，应用管理员可直接进行快照日程定制化，并可在主机挂载用于数据分析，备份恢复和测试开发等用途； 10、▲在线数据重删和压缩功能：支持在线重删和压缩功能，提升闪存空间的利用率。并可支持强哈希 SHA-2 算法的高级去重功能； 11、自动精简配置功能：用户可以为应用程序提供比在存储阵列中分配给它的物理容量更多的容量；可简化并加速调配过程，提供“适时”的容量分配，并提高存储容量利用率； 12、▲存储容灾功能：支持存储间实现同步或异步容灾；提供基于数据块和文件级的远程复制功能，以实现基于存储设备的灾备数据复制及恢复；本次	台	1		

序号	设备名称及建议品牌	主要技术（性能）指标或规格要求	单位	数量	单价（元）	总价（元）
		配置同步/异步远程复制软件许可； 13、文件系统高级功能：支持 64 位并可创建≥20TB 的文件系统，可动态收缩和扩展，支持 IP 多租户逻辑分割，支持文件保护满足法规遵从 SEC 17a-4(f)规则要求； 14、性能分析软件：配置同品牌单独阵列的性能分析软件，能够获取实时的性能数据和历史性能数据； 15、▲服务：质保≥3 年，原厂商提供≥3 年 7×24 小时质保服务，并出具原厂服务承诺授权函。				
2	FC 光纤交通道换机 建议品牌：博科 G610、华为 SNS、浪潮 FS、联想 DS、H3C CN 等一线品牌	1、★24 口 32GB 机架式交换机，速率≥16Gbps，本次激活≥16 口，配置≥16 个 16Gb SFP 模块（原厂非第三方），级联功能，单电源,上架导轨； 2、管理软件：Telnet、HTTP、SNMP v1/v3（FE MIB、FC 管理 MIB）； 3、审核、系统日志、更改管理跟踪；10/100/1000M 以太网(RJ-45)、带内光纤通道；串行端口(RJ-45)；USB； 4、▲提供质保≥3 年，三年 7*24 小时服务。	台	2		
3	服务器交换机 建议品牌：华为 CloudEngine、H3C LS、锐捷 RG-S 等一线品牌	1、▲背板带宽≥25.6Tbps；包转发率≥1260Mpps；配置 2 个冗余电源； 2、▲端口：≥24 个万兆 SFP+,≥4 个 100/40GE QSFP,（含≥24 个 10GB 万兆光模块（原厂非第三方），2 根≥40G QSFP28 堆叠线） 3、网络标准：IEEE802.1d,IEEE802.1x,IEEE802.3,IEEE 802.3u,IEEE802.3x,IEEE802.3z,IEEE802.1Q,IEEE802.1p； 4、支持 VLAN 功能；支持全双工； 5、网管功能：支持网管功能，支持 FTP,TFTP,Xmodem,支持 SNMP v1/v2/v3,支持 sFlow 流量统计,支持 RMON,支持 NTP 时钟 6、▲提供质保≥3 年。	台	2		
4	备份系统	1、★为所有云、虚拟、数据库和物理工作负载提供出色可用性。通过至简设计的管理控制台，提供快速、灵活和可靠地备份、恢复并复制所有应用和数据； 2、▲即时虚机恢复:在整个主机或存储系统发生故障且许多系统处于离线状态的情况下借助（即时虚拟机恢复）技术，可以快速恢复整个平台所有受影响的系统； 3、连续性数据保护和容灾:支持异地灾备功能,将虚拟机数据定时复制到备份数据中心。支持任何虚拟化环境应用程序提供接近连续的数据保护。通过管理控制台的 UI 管理接口,提供故障移转和故障恢复功能； 4、可验证保护:可以对每个备份进行实时验证，期间会扫描恶意软件、在隔离备份的环境中启动备份进行自动测试，并最终关闭文件。操作完成后，系统将提供一份恢复验证结果报告，以供用户审核；	套	1		

序号	设备名称及建议品牌	主要技术（性能）指标或规格要求	单位	数量	单价（元）	总价（元）
		全面透视虚拟化业务：统一监控多种虚拟化环境；审计,分析预测，存储使用趋势，规划未来空间需求;简单、自动化地记录保护状态 7x24小时监控备份架构的状态和性能； 5、虚拟机数据库保护:支持在备份/复制时借助应用感知功能感知虚拟机中运行的数据库应用;支持虚拟机镜像级保护结束后，立即运行数据库事务日志备份的子 JOB，可以以每 5 分钟的间隔将日志进行备份； 6、支持磁带库作为二级备份:支持到磁盘的备份，还可以支持到物理磁带库和虚拟磁带库的备份。可提供高级磁带功能，包括并行处理、原生 GFS 保留、全局介质池等，以增强灵活性、简化管理和提供存档选项，满足企业的数据长期保留需求； 7、★防勒索病毒解决方案：使用经过测试的原生不可变存储(强化 Linux 存储库将备份存储至不可变存储，能够有效防止修改或加密，无需锁定即可获得可靠保护)来加强勒索软件防护,并及时有效检测可恢复性并防止攻击； 8、▲提供≥100TB 容量授权，备份软件必须提供虚拟机、数据库、文件及操作系统备份授权，授权数量无限制； 9、▲提供质保≥3 年。				
5	桌面虚拟化	1、▲桌面与应用虚拟化软件支持多种后台服务器虚拟化平台,要求必须支持服务器虚拟化平台； 2、软件自身支持从 web 浏览器方式访问虚拟桌面和虚拟应用； 3、支持各种主流终端(瘦客户机)设备接入访问虚拟桌面和虚拟应用； 4、支持各种广泛的外围设备的重定向,如普通打印机/发票打印机/读卡器,包括串口/并口/USB 口，并对这些端口提供良好的重定向能力； 5、终端用户可从多种网络环境下访问虚拟桌面，并且在广域网或者网络性能较差(例如:带宽不低于 50Kbps;网络延迟不大于 250ms;丢包率不大于 5%)的情况下仍可保持访问的流畅性或者最终用户体验； 6、▲必须支持虚拟桌面可利用胖客户端的本地计算能力，同时集中管理桌面的统一镜像；能够利用现有 PC 资源除了硬盘之外，内存、CPU、GPU 都调用本地的计算资源； 7、▲支持直接将应用进行虚拟化； 8、★本次提供授权点位≥20 个点位； 9、▲提供质保≥3 年。	套	1		
6	日志审计系统	1、▲对海量日志进行自动化管理，通过一个集中的平台来对日志进行收集、分析、报表、查询和归档。该软件帮助减少内部威胁、进行日志取证分析、监视特权用户以及满足各种法律法规的合规性要求，生成各种各样的报表，例如：用户活动性报表、合规性报表、历史趋势报表以及其他报表 2、▲要求采集所有网络接入的硬件设备和应用系统日志（操作系统、防火墙、交换机、数据库、ERP、OA、PLM、MES、能源管理系统等）均能接入上传到日志审计系统；				

序号	设备名称及建议品牌	主要技术（性能）指标或规格要求	单位	数量	单价（元）	总价（元）
		3、▲提供质保≥3 年。				
7	IT 运维管理系统	1、▲一款功能强大的网络监测软件。能够帮助用户来监控网络性能，实时检测网络故障，排除故障并防止停机，支持网络设备监视、物理服务器监视、虚拟化监视、分布式网络监视、硬件监视、告警和通知、自动化工作流、定制仪表板等； 2、▲能建立清晰的 IT 服务支持全局视图 ，加快 IT 解决问题和履行服务速度 提升 IT 运作效率让服务化繁为简； 3、▲自动发现服务器与网络设备； 4、▲提供质保≥3 年。				
8	NTP 网络时间服务器 建议品牌:北新时频 XDB、千星时频 TF、北斗邦泰 T600	1、▲客户端同步精度<0.5μs； 2、守时精度：内置恒温晶振，守时 24 小时，最大偏差≤10 微秒； 3、可用性指标：MTBF≥80000 小时； 4、服务器同步精度：<=1μs； 5、接口配置：至少配置≥4 个 10/100/1000M 自适应以太网接口（每个端口具备授时和管理功能），≥1 个 Console 接口，至少 1 个显示器接口，≥1 个干接点报警接口； 6、NTP 请求量：≥10000 次/秒； 7、日志记录功能：≥5000 条； 8、配置方法：支持 Console 模式、Telnet 或 SSH 进行远程管理、配置和升级； 9、支持网络协议种类：TPv1.v2.v3&v4(RFC1119&1305)SNTP(RFC2030)MD5 Authentication（RFC1321）Telnet（RFC854）NTP Unicast,Broadcast,Multicast,Autokey TIME（ RFC868)FTP （ RFC959 ） DHCP (RFC2131) HTTP/SSL/HTTPS （RFC2616） SSH/SCP(Internet Draft)SNMP v1,v2、MIB II (RFC1213)RSA 非对称加密 IPV4、IPV6、IPv4/IPv6 Hybrid； 10、▲卫星接收机：支持 GPS、北斗二代双参考源，可扩展 GLONASS 卫星参考源；命令设置可仅使用 GPS 授时、仅使用北斗授时或使用 GPS 和北斗联合授时； 11、授时模式：支持 NTP Peer Client/Server Broadcast Multicast； 12、▲管理软件： （1）提供全网时间统一监控软件，可监视卫星信息、服务器信息、客户端信息。卫星信息包括卫星时间、锁定状态、锁定颗数、经纬度、高度等信息；服务器信息包括 NTP 授时状态、同步状态、服务器时间、网络配置等信息。 （2）支持≥10000 台客户端监视，可根据需要设置告警类型、告警级别等进行选择上报。 （3）在监控软件中可直接查询、配置网络参数。 （4）具备驯服/保持、失锁/入锁状态（远程）监视功能。 13、用户界面：配置高亮 VFD 液晶，轮循显示 GPS/北斗 2 搜星状态、时间、卫星个数、经纬度、高度、各网卡 IP、系统工作状态；三色指示灯支持显示 NTP 服务是否启动、网络连接是否正常、NTP 请求是否超过 8000 次/秒及 GPS 是否锁定等信息；	台	1		

序号	设备名称及建议品牌	主要技术（性能）指标或规格要求	单位	数量	单价（元）	总价（元）
		14、▲客户端同步软件：支持 Win2000、Windows XP、Win2003、Windows7、Windows 8、Windows10、Windows Server、Linux 等系统平台，支持 SNTP1,2,3,4 等协议。支持系统托盘、开机自动运行、手动设置同步周期。软件可以显示参考时间、原始时间、接收时间、传输时间、本地时间等信息及服务层次、时延、偏差等； 15、▲提供质保≥3 年。				

2.2.2 配件扩容改造、辅料清单

序号	设备名称	适配型号	主要技术（性能）指标或规格要求	单位	数量	单价（元）	总价（元）
1	处理器	联想 SR650	英特尔® 至强® 金牌 6138、20 核心处理器 27.5MB 高速缓存，2.0 GHz	颗	8		
2	内存扩容	联想 SR650	DDR4-2666 32G	张	96		
3	内存扩容	戴尔 R740	DDR4-2400 32G	张	12		
4	扩展卡	联想 SR650	x16/x8/x8 PCIe G4 Riser 1/2 Option Kit	张	4		
5	扩展卡	戴尔 R740	扩展卡/RISER 卡/PCI 插槽/提升卡 riser 卡 R740riser2+3 共 2 个 X16/3 个 X8	张	2		
6	扩展卡	华为 2288H V5	扩展卡/RISER 卡/PCI 插槽/	张	1		
7	HBA 卡	QLE2690	HUA-SP-FC 单端口-16Gb/s-PCIE 3.0 x8	张	14		
8	存储硬盘	联想 DE2000H	4XB7A14113 B4BZ Lenovo ThinkSystem DE Series 1.8TB 10K 2.5″ HDD 2U24	块	24		
9	电源	戴尔 R740	750W 铂金电源	块	2		
10	万兆网卡	戴尔 R740	Intel X710-DA2 PCIe 10Gb 2-Port SFP+ Ethernet Adapter	张	2		
11	万兆网卡	联想 SR650	ThinkSystem LOM 10Gb 4-Port SFP+ Ethernet Adapter	张	4		
12	堆叠板卡	华为 S7706	VSTSA 集群卡	张	4		
13	堆叠线	华为 S7706	10G 堆叠线	根	8		
14	光纤跳线		1、16Gbps LC-LC 光纤跳线 2、万兆光纤跳线（连接头不定）	批	1		
15	其他		超六类屏蔽网线、超六类万兆水晶头（全金属、镀金接口）、线缆魔术贴、绑扎带等等	批	1		

2.2.3 实施与技术服务

序号	名称	主要内容与要求	单位	数量	单价（元）	总价（元）
1	整体规划设计	1、参照网络安全等级保护 2.0 三级标准设计整体的网络架构（**由招标方决定分步实施内容**）。	项	1		
2	网络规划设计	1、对现有网络环境进行全面调研、形成现有网络调研环境拓扑及网络情况汇总表（需求分析报告），并按照新的网络进行规划设计、将网络按照核心服务区、生产业务区、办公区、互联网接入区进行划分；并通过相应技术手段进行安全隔离，并按照网络结构进行组网设计、IP 地址规划和改造； 2、新增核心网络区：部署核心层汇聚交换机，用于部署该区域对应的核心交换网络用于承载核心区域业务系统； 3、新增生产区域管理网：新增一套管理网用于管理和查询，并在该网络中部署相应的安全设备(建立安全管理中心)来提高管理安全和方便管理以及相关扩展业务； 4、新增互联网区域(规划)：部署隔离安全设备，用于互联网区域与核心数据交换的安全防护。	项	1		
3	项目实施安装	1、本项目内包含的服务器、主数据中心存储、虚拟化系统、网络设备、网络安全设备、扩容配件的采购、安装和调试。 2、对新建机柜的合理规划。满足现有设备搬迁运行需求并考虑较长时期内业务发展需求，结合搬迁按设备类型、热量排放、网络分区、应用分类等规划设备部署； 3、根据最新的系统架构及网络拓扑的重新部署。根据招标方对新机房的网络规划和安全规划要求，本次迁移工作需要对整个网络，安全，计算，存储和应用做比较大的调整和部署，迁移对各个网络区域的划分进行重新部署，对各个业务系统的访问和调用需要重新实施部署，安全策略需要根据迁移中利旧设备和新增设备的搭配使用重新规划和部署。	项	1		

序号	名称	主要内容与要求	单位	数量	单价（元）	总价（元）
4	数据迁移	1、现状详细梳理。对现有信息系统的现状进行详细整理，梳理清楚现有机房内设备状况、设备和应用之间的对应关系、设备连接关系、信息点状况、信息系统架构、应用关联关系、应用服务要求等基础信息，形成当前 IT 系统的详细勘察报告（需求分析报告），为本次数据迁移策略的制定以及后期系统的维护提供重要的基础信息； 2、业务平稳迁移。通过风险分析、应用关联分析、 业务影响分析，制定安全有效的整体搬迁策略，减少业务影响，减少业务中断次数与时间，规避搬迁风险，保障业务连续性；制定充分、细致的搬迁实施方案，提供与搭建应急环境，进行充分详细的准备工作，根据搬迁策略，将业务系统顺利迁移到新的服务器集群中； 3、数据总量 20T（包含全部应用系统（OA、ERP、财务、能源管理、档案管理、测试系统等）、数据库、文件等） 4、在数据迁移之前需要做好备份，保证数据安全完整； 5、搬迁周期可控。在可控的范围内尽量缩短新系统并行周期，充分分析业务、存储、网络等各种关联分几批有计划搬迁，数据迁移时间定在周末时段，系统停止运行不得超过 12 小时。	项	1		
5	培训	1、本项目中包 1 包含的全部软硬件设备的安装部署、调试、使用和维护； 2、本项目内涉及的各种专业技术的培训（如：虚拟化技术、主流操作系统、主流数据库技术、网络技术（路由和交换机）、网络安全技术、软件部署架构技术等（nginx、nPart、keepalived、docker、k8s、Apache、Tomcat、IIS 等））； 3、其他要求见本文件第 9.1 节“培训要求”。	项	1		
6	运维技术服务	1、详见本文件第 6 节“运维服务和技术支持”； 2、提供一年免费项目整体质保和技术服务，另外增加两年付费运维技术服务。 3、负责对项目二中包含的设备进行集	年	2		

序号	名称	主要内容与要求	单位	数量	单价（元）	总价（元）
		成、互联等工作。 4、当出现技术争议时，由招标方组织技术商讨会确认，并签署备忘录。				

2.3 项目二（网络安全建设）

2.3.1 软硬件设备清单

序号	设备名称	主要技术（性能）指标或规格要求	单位	数量	单价（元）	总价（元）
1	下一代防火墙 建议品牌：清华永新SG、天融信NGFW、H3C SecPath、山石网科、绿盟NX、深信服AF、启明星辰USG、奇安信、华为等一线品牌	1、★具备≥4个10GE SFP+插槽，具备≥16个1GE RJ45接口以及≥8个1GE SFP插槽（包含对应光模块），配置冗余双AC电源（提供产品彩页复印件并加盖原厂公章）； 2、★防火墙吞吐量≥27Gbps，包转发率≥16Mpps，防火墙转发时延（64字节）≤5us（提供产品彩页复印件并加盖原厂公章）； 3、▲并发会话数≥300万，新建会话≥28万/秒； 4、★IPS吞吐量≥5Gbps，NGFW吞吐量≥3.5Gbps，威胁防护吞吐量≥3Gbps，本次开启IPS安全防护功能（提供产品彩页复印件并加盖原厂公章）； 5、★支持并开通≥3年防病毒、入侵防护、应用控制、云沙箱订阅服务，支持并开通的虚拟防火墙数量≥10个（提供原厂售后服务承诺函并加盖原厂公章）； 6、▲SSL VPN吞吐量≥2Gbps，IPSEC VPN吞吐量≥13Gbps，支持并开通≥200个SSL VPN隧道模式并发能力； 7、支持L3路由/L2透明模式部署，支持旁路监听模式部署； 8、支持主-备、主-主、集群的冗余部署方案，双机热备要能支持多种组网形式，确保可靠性，并且数据接口和心跳线支持冗余； 9、支持服务器的负载均衡； 10、支持15000种以上的入侵检测特征数目，支持特征码检测和行为检测，并支持分级启用； 11、支持SQL注入、XSS防护； 12、支持对HTTP的方法（GET、POST、PUT、HEAD等）做限制策略； 13、▲支持Dos & DDoS防攻击检测和阻止，支持抵御SCTP Flood、SYN Flood、UDP Flood、ICMP Flood、ICMP sweep等攻击类型，动作支持记录、阻断两种模式，支持对攻击IP进行隔离； 14、支持HTTP、FTP、IMAP、POP3、SMTP、HTTPS、IMAPS、POP3S、SMTPS、MAPI协议病毒过滤，支持深达10级以上的文件压缩；可以限制过滤文件的大小，对超大文件采取“通过”或“阻止”动作； 15、支持对SSL加密流量的内容检测和安全过滤； 16、▲支持Modbus、Profinet、S7、OPC等多种工业协议识别和防护，可在防火墙策略中调用以执行	台	1		

序号	设备名称	主要技术（性能）指标或规格要求	单位	数量	单价（元）	总价（元）
		放行、检测、阻断等动作，实现工控环境的可视化与控制； 17、支持防数据泄漏功能，能对 HTTP、FTP、SMTP、POP3 等协议中的敏感内容进行过滤和阻断；支持指纹识别、水印过滤功能； 18、支持 Web、Telnet、SSH 方式对设备进行远程管理； 19、设备内置抓包功能，可针对接口抓包，并保存为 Wireshark 可直接打开的格式文件； 20、▲产品资质证明：（1）具有公安部安全产品销售许可证、（2）具有中国信息安全认证中心颁发的信息安全产品证书、（3）具有中国国家版权局颁发的防火墙系统的软件著作权证、（4）具有中国国家版权局颁发的病毒防护系统的软件著作权证、（5）具有中国国家版权局颁发的入侵防御系统的软件著作权证，（以上证明材料提供复印件并加盖投标产品厂商公章）； 21、▲提供质保≥3 年，提供原厂授权和原厂售后服务承诺函。				
2	堡垒机（运维安全审计系统） 建议品牌：思福迪、行云管家、齐治、天融信、启明星辰、JumperServer、启明星辰、帕拉迪、绿盟科技堡垒机等一线品牌	1、▲系统架构 （1）产品架构：软硬件一体化产品，采用标准机架式硬件结构； （2）部署方式：旁路代理模式，不影响正常业务流量； （3）高可用性：支持双机热备部署； （4）管理结构：B/S 架构，采用 HTTPS 方式远程安全管理，无需安装管理客户端； （5）网络接口：≥100/1000M RJ45*4 个自适应以太网口； （6）数据存储：设备内置存储系统，存储空间≥1TB SSD 硬盘； 2、性能要求：并发会话数 图形并发会话数≥150;字符型并发会话数≥350 3、功能要求 （1）支持协议：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，可自定义其它访问协议及客户端支持；支持应用发布方式 HTTP 越权访问提示及阻断功能； （2）支持在 web 页面上进行连接测试（PING、TRACEROUTE、TELNET）； 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(如 SecureCRT、putty)会话复制功能；支持 SSH 软件中直接调用 sftp 功能； （3）支持多种认证方式：支持多种认证方式：本地密码认证、UsbKey 认证、TOTP 令牌认证、第三方 CA 证书认证、邮件认证、RADIUS 认证、LDAP 认证、AD 域认证；支持认证方式全局设定、单一用户认证方式设定，支持多种认证方式组合；	套	1		

序号	设备名称	主要技术（性能）指标或规格要求	单位	数量	单价（元）	总价（元）
		（4）访问控制及异常告警：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；支持审计限制策略：限定管理员针对指定的运维用户的运维记录进行审计； （5）用户管理功能：支持添加、删除、修改以及启用、停用运维用户； 支持用户多角色划分功能，如系统管理员、配置管理员、审计管理员、密码管理员、审计审计员、运维用户等，对各类角色可组合进行细粒度的权限管理； 支持用户安全策略功能，如密码锁定次数、密码有效期、密码复杂度、用户有效期、用户登录时间限制、用户登录 IP 范围等； 支持用户授权快速绑定及集成、移交功能，可以将用户的群组属性和权限交接给其它用户 （6）主机管理功能：支持主机/主机组的多级架构管理，可以复制、剪切、粘贴、移除主机/主机组，实现主机/主机组架构的灵活调整，支持系统类型管理：内置常见系统类型，可自定义添加目标设备的系统类型及内容，包括显示图标、该系统拥有的协议及默认端口等内容；支持添加主机页面在线 ping 主机功能，即时获取该主机存活信息； （7）▲主机 SSH 运维支持密钥托管功能；支持自动更改 SSH 密钥功能 （8）▲操作行为记录：支持对运维操作会话的在线监控、实时阻断、会话回放、起止时间、来源用户、来源 IP、目标设备、协议、命令记录、操作内容（如对文件的上传、下载、删除、修改等操作等）的详细行为日志。支持对 RDP 标题窗口、键盘输入的记录和搜索定位支持全字段搜索审计日志，只需通过关键信息快速搜索定位，支持日志关联分析，可直接关联到日志同个会话中的所有操作日志； （9）会话过程回放：支持倍速/低速播放、拖动、暂停、停止、重新播放等播放控制操作； （10）▲密码管理：改密类型支持 Windows、Linux、Unix、AIX、Cisco、HUAWEI、H3C、Ruijie 等； 支持按设备、数据库、系统帐号、计划执行时间、改密周期、密码策略、改密结果发送等生成详细的改密计划，到期自动执行；支持使用 agent 方式修改主机密码； （11）实时监控：支持实时监控近期发生的所有会话信息，显示会话状态（连接中、退出、阻断）；支持对会话进行同步监控，执行会话回放、监控和阻断操作；支持记录审计系统自身的管理操作，保障审计系统自身安全； （12）历史查询及审计报表：支持单一条件快速查询、查询结果二次过滤以及多重条件组合高级查询功能；内置丰富的报表统计模板，且支持 PDF、doc、html 导出。 （13）协同操作：支持双人协同操作功能；支持自定义运维协议代理端口号、支持启停运维协议服务；支持系统硬件、系统服务进程、数据库、应用代理进程状态实时在线监控；支持页面管理硬盘并进行更换；支持邮件、短信、Syslog、FTP、SNMP 等输出接口配置支持系统告警日志发送；				

序号	设备名称	主要技术（性能）指标或规格要求	单位	数量	单价（元）	总价（元）
		4、▲产品资质要求：《计算机软件著作权登记证书》，国家公安部计算机信息系统安全专用产品销售许可证、IT 产品信息安全认证证书 5、▲系统先进性：提供产品相关专利或者国家级认证证书作为加分项目； 6、★可管理对象数量（授权）：内置≥50 个主机/设备操作监控许可； 7、▲产品授权及服务：提供针对本项目的原厂授权函，提供≥原厂三年 7*24 小时的售后服务承诺，提供三年原厂保修及原厂免费现场服务，产品的安装、培训由原厂工程师完成实施；在设备维保期内，厂家提供对系统软件的免费升级服务，保证系统软件为最新版本。				
3	网络准入系统 建议品牌：画方科技、北信源、盈高、联软、中孚信息、奇安信等一线品牌	1、★硬件配置：1U 机架式设备,CPU≥2.0GHz,内存≥16G,硬盘≥1T,≥6 网口(千兆电口),扩展≥2 个万兆光口，配置冗余双电源；每秒事务数（TPS）：≥5000（次/秒）；最大吞吐量：≥1.5Gbps；最大并发连接数≥5000（条）； 2、▲系统部署：需采用纯旁路部署，禁止通过修改交换机端口 VLAN ID、策略路由与镜像抓包功能实现准入控制，以防造成交换机负载过高，影响正常终端的网络通信与数据交换； 3、▲终端发现及类型识别： （1）支持自动发现入网终端的 MAC 地址、IP 地址、网卡厂商、TCP 服务端口、接入 VLAN、接入交换机端口等信息。 （2）支持自动识别终端类型，如办公机、交换机、路由器、打印机等，生成终端类型统计报表。 4、▲阻断控制： （1）支持在不安装客户端代理的情况下，实现 HUB 和非网管交换机环境下非法终端与合法终端的通信隔离与阻断，并支持通过浏览器提供 portal 引导提示。 （2）支持基于终端的部门/终端类型/操作系统/标签和接入 VLAN 配置不同的准入策略，管理员可查看符合每条准入策略的终端。 5、▲认证策略：支持通过多种入网认证方式。至少包括用户名密码认证、MAC 地址认证、手机验证码登录、图形密码认证登录等，支持与外部认证平台联动，如：企业微信、AD/LDAP、Radius 服务器等。 6、注册策略：支持新终端入网注册策略，注册需支持基于 vlan 段设置是否启用。可采用准入客户端、浏览器 Portal 页面方式进行终端注册。支持管理员自定义注册内容，至少包括注册项内容、注册条目、前后顺序、标题、提示语句、是否必填等，对于关键注册项，如用户名、部门等支持选择模式和输入模式切换， 7、客户端策略： （1）客户端应兼容 Windows 系列的 32/64 位操作系统； （2）▲准入系统管理端应支持在同一准入策略中分别对 windows 操作系统和国产化操作系统自定义设置规范检查内容。支持健康合规检查策略，采用动态检测技术，需支持多种检查机制，至少支持	套	1		

序号	设备名称	主要技术（性能）指标或规格要求	单位	数量	单价（元）	总价（元）
		入网检查、定时检查、周期检查机制，针对接入内部网络的计算机终端实行多种安全检查策略，支持分组策略下发控制，拦截不安全终端接入网络；（提供产品功能截图证明） （3）▲准入客户端支持对电脑上必须存在或禁止存在的内容进行检查（包括：软件/进程/服务/文件/注册表/TCP 端口/UDP 端口等），对检查不合规的项，可提供修复路径或修复文件。（需提供产品功能截图证明） 8、▲网络策略： （1）支持 IP 冲突发现功能，能够定位冲突 IP 的 MAC 地址，能够对绑定的 IP/MAC 进行保护，对违规使用绑定 IP 的终端进行阻断。 （2）支持在不安装客户端或插件的情况下，对目标终端进行 MAC 地址仿冒（MAC 克隆）检查。支持对非法设备同时仿冒合法设备的 IP 地址、MAC 地址、TCP 端口等信息的行为进行发现和阻断。 （3）能够发现内网私接的 HUB、不可网管交换机等，能够及时产生告警并阻断接入设备入网。可自动发现网中网行为，如小路由、随身 WiFi、免费 WIFI、代理上网等行为。 9、交换机管理： （1）支持与网络交换机联动，自动生成网络拓扑和交换机面板图，可基于端口颜色区分显示端口开关状态/连接状态/接入终端数目/告警终端等，管理员可直接在面板图上对端口进行开关操作和端口绑定策略。 （2）支持将 IP/MAC 绑定和 MAC/PORT 绑定策略同步到交换机配置上。 10、▲IP 地址管理： （1）支持 Trunk 管理多 VLAN 的 IP 分配功能，无需配置交换机 DHCP RELAY 即可实现为所有 VLAN 分配 IP 地址；可自定义 DHCP option 功能；能够基于部门、标签、终端类型、操作系统下发固定的 IP 地址段，以兼容未来不同网络环境。 （2）支持 IP 地址网格视图管理，能够通过图示直观的查看各网段中在线、离线、从未使用的状态，能够通过颜色区分保留 IP 地址、可用 IP 地址、绑定 IP、告警 IP 等。 11、入网报告： （1）支持记录终端所有网络接入日志，包括上线、下线、IP 变更、IP 冲突、接入端口变更、主机检查结果、用户认证、新终端入网、违反入网策略、被阻断、解除阻断等。 （2）支持管理员自定义每个入网事件的告警等级和处理动作，如是否记录、是否告警、是否需要管理员人工确认。 12、系统管理： （1）系统应具备自我防护能力。支持设置 SSH 黑白名单、管理页面登陆黑白名单、防 DDOS 攻击、防 SYN-FLOOD 攻击、客户端通信加密等，支持在准入服务器上虚拟密罐服务进行可疑行为监测并记录异常访问日志，管理员可自定义虚拟服务端口、访问频率、告警阈值等。 （2）提供强制入网终端收看培训视频的功能。 13、▲产品资质：原厂商必须提供《计算机信息系				

序号	设备名称	主要技术（性能）指标或规格要求	单位	数量	单价（元）	总价（元）
		统安全专用产品销售许可证》、《涉密信息系统产品检测证书》、《计算机软件著作权登记证书》（需提供有效证书复印件，并加盖原厂商公章） 14、★授权许可：提供≥700 点授权许可，支持废弃设备授权回收。（支持交换机、打印机、打印服务器、扫描仪、扫码枪等哑终端放行策略，不占用授权点位数； 15、▲提供质保≥3 年，提供原厂授权和原厂售后服务承诺函				
4	终端安全管理系统 建议品牌：北信源、联软、溢信科技、启明星辰、网御星云、奇安信、天融信等一线品牌	1、★资产管理： （1）系统自动采集终端的软、硬件信息，在 WEB 平台可查到系统的软硬件属性及更换情况。 （2）自动收集硬件的信息包括：硬盘型号、硬盘序列号、硬盘容量、显卡类型、内存大小、CPU 类型、CPU 主频、主板序列号等硬件设别的信息。 （3）支持收集软件信息包含操作系统、操作系统序列号、安装软件信息、服务等信息，页面可直观展示所安装软件列表还有运行程序列表。 （4）通过注册客户端时选择的组织架构，可以实现终端资产与持有人进行绑定。 （5）硬件资产可以自动关联持有人的姓名、电话、组织架构、IP、MAC 等重要信息，方便对硬件信息的实名管理和查询。 （6）管理平台可以根据终端的设备类型、设备用途等信息进行统计，方便对硬件资产的各种报表统计和导出。 2、▲共享文件夹管理策略： （1）可采集共享目录 （2）支持关闭 windows 默认共享 （3）可监控共享文件夹 （4）可对监控共享文件夹加白名单 3、▲补丁管理： （1）支持补丁分发，软件分发支持 Windows 操作系统安全补丁、IE 浏览器和 Windows 应用程序相关补丁等，及时修复终端操作系统及相关应用程序安全漏洞。 （2）支持 Windows 操作系统补丁，支持的 Windows 操作系统版本包括：Win2000、WinXP、Win2003、WinVista、Win7、Win2008、Win2008R2、Win8、Win8.1、Win2012、Win2012R2，Windows 系统补丁包括 Windows 操作系统的 Service Pack 或安全更新。 （3）支持在线扩展 Windows 应用程序补丁支持。 （4）补丁分发策略支持多种分发，策略包括：补丁自动分发策略（包含自动下载静默安装）、自定义安装补丁策略（可按实际需要安装相应的补丁）、自定义卸载补丁策略（用户可按实际需要卸载相应的补丁）。 （5）支持强制补丁，能够强制终端必须安装指定的补丁。 4、进程异常监控策略： （1）支持未响应窗口监控 （2）支持进程意外结束监控 （3）支持服务意外停止监控 （4）进程意外处置方式：上报审计、终端告警。	套	1		

序号	设备名称	主要技术（性能）指标或规格要求	单位	数量	单价（元）	总价（元）
		5、★移动存储介质管理： （1）支持管理员对入网的移动存储介质进行注册，可以对已注册的移动介质进行管理，包括授权、启用、停用、删除、取消注册、导出注册列表等。 （2）同时支持终端程序及服务页面程序对 U 盘进行注册管理，无需审批方便快捷。 （3）可单独下发标签授权，方便用户管理（多个 U 盘可以注册为同一种标签）。 （4）支持 U 盘与终端进行点对点的授权，可以灵活控制单个 U 盘在不同终端上拥有不同的使用权限。 （5）支持移动存储介质权限设为普通设备与加密设备，可设置是否允许网外使用，可设置是否使用密码访问。 6、修改网络配置：可点对点远程修改终端的 IP 地址、子网掩码、默认网关、DNS 地址 7、设备使用策略：支持监控打印机、摄像头、麦克风使用情况；支持多人围观检查。 8、软件分发： （1）支持任意格式文件的分发。并支持软件安装包的自动分发和安装，支持软件后台静默安装。 （2）软件分发支持选择指定安装包程序，指定分发软件保存路径，可以设定安装参数，并可以设置执行软件安装的指标项和软件安装完成的检测指标项。 执行软件安装条件包括：注册表、本地文件版本判断。软件安装完成检测指标包括：注册表、进程、本地文件版本判断。 （3）支持任何普通格式的文件自动分发，可以将文件自动分发到指定终端的指定目录下。 9、▲外设使用控制 （1）能够识别外设类型，并根据策略配置进行管控，审计外设控制记录。 （2）受控外设包括：软驱、光驱、USB 移动存储、USB 非移动存储、鼠标/键盘、手机、本地打印机、网络打印机、串口、并口、1394 接口、红外、蓝牙、PCMCIA、冗余硬盘、无线网卡、普通网卡、磁带机、图像设备等。 （3）支持针对指定设备进行例外放行。 10、终端端口管理：可查看点对点终端的进程 ID、进程名、协议类型、本地地址和远程地址；支持远程结束端口。 11、★网络非法外联控制： （1）能快速发现和控制网络中的非法外联行为，阻断终端通过多网卡、WIFI、3G 网卡、手机等多种方式网络非法外联访问，杜绝网络非法外联行为发生。 （2）能够识别和管理终端物理网卡（包括有线和无线网卡），也能够识别终端代理上网。 （3）能够禁用可能被用于连接网络非法外联设备的外设接口，至少能够禁用 Modem、红外、COM、无线网卡、蓝牙和 USB 接口。 （4）支持多种探测外联模式，更能全面发现违规外联的行为。 12、▲生产制造商资质：产品制造商具有中国网络安全审查技术与认证中心颁发的《信息安全服务资质认证证书》（软件安全开发服务(二级或一级)）；				

序号	设备名称	主要技术（性能）指标或规格要求	单位	数量	单价（元）	总价（元）
		产品制造商同时具备、ISO9001、ISO27001 证书； 13、★提供 API 接口（能与第三方系统对接实现组织结构和人员同步，以及数据库中的数据招标方要能进行提取）； 14、★本次提供授权点位≥700（支持废离线（废弃）设备授权自动回收），支持扫码枪、iPad、打印机、打印服务器、扫描仪等哑终端的注册放行（不占用授权点位数）； 15、▲提供质保≥3 年，提供原厂售后服务承诺函。				
5	防病毒系统 建议品牌：瑞星、火绒、金山、360 等一线品牌	1、▲体系架构系统部署： （1）要求系统支持中/英文界面，系统部署采用 C/S 架构，管理采用 B/S 架构，管理员只需通过浏览器登录控制中心，即可对系统进行管理 （2）要求支持 Windows XP、Windows 7、Windows 8、Windows 8.1、Windows 10、Windows Server 2003、Windows Server 2008、Windows Server 2012、Windows Server 2016、Windows Server 2019、Linux、Unix （3）要求客户端安装方式支持 Web 安装、AD 域环境批量静默安装、共享安装 （4）要求客户端安装后占用≤200M 硬盘空间，病毒库大小≤200M，日常使用内存占用≤100M，有效节省电脑资源。 （5）要求中心支持容灾备份功能，当主中心计算机遭受如宕机、断电、硬件/软件故障等意外情况或人为操作错误导致主中心计算机无法正常使用时，备用中心将自动顶替宕机的主中心且同步数据。 （6）要求中心支持级联部署及管理，可实时查看下级终端威胁及在线情况，上级可对下级灵活分配授权，上级可登陆下级中心直接进行管理，同时可实现分级管理中心能够通过一级管理中心升级病毒库和客户端版本以及补丁升级数据 （7）功能可按照模块进行授权，可选择功能授权模块包括:中心定制、远程桌面、U 盘管理、终端动态认证、硬件管理、多级中心、API 接口、备用中心;可根据需求自定义功能模块。 2、▲中心基础设置： （1）要求支持展示全网终端安全概览； （2）要求支持定制防护策略以及策略细粒度配置：包括病毒防御（文件实时监控、恶意行为监控、U 盘保护、下载保护、邮件监控、Web 扫描）；系统防御（系统加固、应用加固、软件安装拦截、浏览器保护、摄像头防护）；网络防御（网络入侵拦截、对外攻击拦截、恶意网站拦截、Web 服务保护、爆破攻击防护、僵尸网络防护、远程登录防护）；访问控制（IP 协议控制、IP 黑名单、联网控制、网站内容控制、程序执行控制、设备控制）以及安全工具可根据不同分组需求定制不同的策略 （3）要求中心支持任务通知，可在任务完成时、硬件变更时、终端安全服务异常时、子中心连入时、子中心脱离时接收通知 （4）要求中心具备事件日志模块； （5）要求中心配备安全工具及管理工具：域部署工具、离线升级工具、中心迁移工具、移动存储注	套	1		

序号	设备名称	主要技术（性能）指标或规格要求	单位	数量	单价（元）	总价（元）
		册工具安全 U 盘程序、专杀工具； （6）要求中心支持全局信任区可通过信任文件路径、信任文件校验和方法添加信任文件以及添加信任网址。 3、▲中心管理： （1）要求可按照不同分组创建管理员且管理权限可按模块划分，支持管理员接收邮件预警； （2）要求支持中心无操作自动登出设置，防止管理后台闲置时自动退出，避免频繁登录； （3）要求中心具有登陆二次验证功能，开启该功能后，通过登录中心时进行二次验证的方式，阻止中心遭遇密码泄露、弱口令暴破、撞库等黑客破解行为带来的危害，达到保护控制中心的目的； （4）要求管理员可设置高危操作动态认证，下发远程桌面任务、添加信任文件或进行文件分发时需要管理员进行二次动态认证后才可执行高危操作； （5）要求支持中心地址屏蔽来自搜索引擎的页面访问，当中心架设在公网时防止他人恶意访问； （6）要求支持远程桌面任务应答时间配置，可设置超时处理方式，拒绝或接受； （7）要求支持可对终端添加多个中心地址,当终端接入网络环境时,中心可对终端实施管控。 4、终端运维管控：要求中心支持对终端下发快速查杀、全盘查杀、自定查杀任务，可推送终端升级、发送通知、同步防护策略、垃圾清理、关机、重启等任务。中心支持将终端禁网，实现上网行为管控。支持将终端隔离区内文件恢复。支持将终端拉黑，避免占用授权点数。 5、▲漏洞扫描补丁修复： （1）要求支持漏洞集中修复、统一修复高危漏洞、统一修复所有漏洞，并展示以修复补丁和未修复补丁的信息； （2）要求支持补丁文件管理，缓存在中心本地的补丁，可进行下载； （3）要求支持热补丁机制，利用产品自身防御功能，防护其他软件以及系统出现的漏洞，阻止对计算机造成损害与入侵。 6、▲反病毒引擎： （1）要求具有反病毒底层技术，反病毒引擎为本地反病毒引擎，不依赖云（联网时的病毒查杀能力与断网时的病毒查杀能力一致）。具有轻量级的病毒库，却有较强的病毒查杀能力； （2）要求反病毒引擎具备全文哈希、分段哈希、局部敏感哈希、关键数据特征等扫描技术，可提取恶意代码中关键代码或数据片段来标识恶意代码； （3）要求反病毒引擎具有虚拟沙盒技术，能对待扫描的 PE 样本应用通用脱壳和动态行为扫描技术，用较少的记录，长期、有效地检出家族性样本。且虚拟沙盒接近真实 CPU 的执行效率和高还原度的操作系统环境仿真且具有很强的抗干扰能力； （4）要求反病毒引擎具有基于虚拟沙盒的动态行为分析，可以跟踪和记录运行在其中程序的行为，通过行为记录，可以通过启发式分析算法对程序的恶意性进行评估； （5）要求反病毒引擎具有代码级修复能力，对寄生类恶意代码拥有完善的解决方案。				

序号	设备名称	主要技术（性能）指标或规格要求	单位	数量	单价（元）	总价（元）
		7、▲恶意威胁防范： （1）要求支持零信任恶意行为分析模型，监控并分析程序执行过程并对评估得到的恶意行为即时阻断； （2）要求支持基于 HTTP 协议的数据流量检测，可检测恶意代码并追溯恶意代码来源； （3）要求支持无需沙箱即可针对包括但不限于 Web 服务器、数据库软件、Office 软件、编辑软件、浏览器、设计软件等软件进行加固，防止前述软件漏洞被攻击者(人或程序)利用进而进行渗透攻击； （4）要求支持 Web 服务保护，保护 Web 服务，阻止黑客针对高危 Web 服务进行漏洞渗透攻击，包括 Apache、Nginx、IIS、PHPStudy、Tomcat 等的高危漏洞； （5）要求支持对引导区、系统进程、启动项、服务、驱动、系统组件、系统关键位置、网络驱动器等位置进行病毒查杀； （6）要求支持勒索病毒诱捕，可在根目录生成 txt、pem、sql、xlsx、mdb、jpg、rtf、xls、doc、docx 等格式的诱捕文件，当出现勒索行为，对其进行捕获并进行隔离； （7）要求具有阻止黑客通过桌面爆破植入勒索病毒防护能力，可针对弱口令弊端、暴力猜密码等一切基于 RDP 协议的爆破进行有效阻止； （8）要求支持病毒库更新周期为一天一更新，紧急或重大事故出现可及时升级； （9）要求支持≥十万多种家族类型病毒，亿级别以上样本数量。 8、▲防病毒： （1）要求支持恶意行为监控，通过监控程序运行过程中是否存在恶意操作来判断程序是否安全，从而可以作为传统特征查杀的补充，极大提升电脑反病毒能力； （2）要求支持 U 盘保护，U 盘接入电脑时自动扫描根目录下文件、自动扫描被病毒修改的项目，保护电脑不被感染； （3）要求支持下载保护，对互联网、即时通讯软件或网盘等下载的文件进行扫描； （4）要求支持 Web 扫描，应用程序与网站服务器进行通讯时，Web 扫描功能会检测网站服务器返回的数据，并及时阻止其中的恶意代码。 9、系统防护： （1）要求支持系统加固，针对病毒会利用或修改的系统脆弱点，设置相应的防护规则，有效保护系统关键文件不被篡改、破坏或恶意创建，防止特定注册表项目不被恶意篡改，监控针对系统的敏感行为，拦截高风险动作，阻止特定命令行被恶意利用的行为，保护系统关键进程不被攻击利用，针对病毒特殊行为进行免疫等； （2）要求支持应用加固，通过对容易被恶意代码攻击的软件进行行为限制，防止这些软件被恶意代码利用； （3）要求支持浏览器防护，保护浏览器的主页不被病毒锁定，也可自行设置主页地址。 10、访问控制： （1）要求支持联网控制，自定义阻止某程序联网，				

序号	设备名称	主要技术（性能）指标或规格要求	单位	数量	单价（元）	总价（元）
		自行管控电脑中所有程序是否联网。可通过文件sha1、文件路径方式配置。 （2）要求支持网站内容控制，自定义限制计算机访问指定网址，达到屏蔽该网站的目的。 （3）要求支持程序执行控制，自定义限制终端使用某软件；可通过文件 sha1、文件路径方式配置。 （4）要求具有 U 盘信任功能，当终端开启访问控制-设备控制-U 盘设备时，可以通过在中心的“信任设备”功能来添加需要信任的移动存储设备，以允许该设备在任意终端使用； （5）要求支持对 U 盘注册的同时进行加密，即使 U 盘丢失，也可保护数据，防止数据泄露。 11、★更新迭代： （1）要求支持内网环境中心使用离线增量包更新病毒库与组件版本； （2）要求支持断网内网环境使用离线升级工具进行病毒库、版本组件、补丁数据的更新升级； （3）要求支持客户端主动升级及平台即时/定时推送升级任务； （4）提供≥3 年免费病毒库升级（离线）。 12、▲产品资质证明：（1）《计算机信息系统安全专用产品销售许可证》、（2）《计算机软件著作权登记证书》、（3）国家计算机病毒应急处理中心实验室认证 13、★提供授权点位≥700 点，持离线终端可设置过期时间，过期终端超时后将自动从中心删除（回收断网设备、废弃设备授权数量）； 14、▲提供质保≥3 年，包含≥3 年内的软件升级和病毒库更新服务，原厂授权和提供原厂售后服务承诺函				

2.3.2 实施与技术服务

序号	名称	主要内容与要求	单位	数量	单价（元）	总价（元）
1	项目实施安装、调试	1、项目二内包含网络安全设备的采购、安装和调试。 2、在本次规划的网络安全区中部署设备。	项	1	/	/
2	培训	1、项目二包含的全部软硬件设备的安装部署、调试、使用和维护； 2、项目二内涉及的各种专业技术的培训（如：网络安全技术、网络连接技术）； 3、其他要求见本文件第 9.1 节“培训要求”。	项	1	/	/
3	质保与运维服务	1、项目二中标方在签订的合同范围之内必须无条件配合招标方的设备安装、调试、集成和运维工作。 2、当出现技术争议时，由招标方组织技术商讨会确认，并签署备忘录。	项	1	/	/

3 IT 基础架构规划

3.1 整体网络拓扑图

（整体网络拓扑图由技术部门在投标单位进行现场需求调研时给出，投标单位需要准守招标方相关保密规定，不得泄露本项目招投标相关内容）

图 1 网络拓扑图

本次项目建设方案的覆盖范围有：服务器虚拟化区，数据库区，数据备份区，高效传输层中的 FC 交换机及其他通信线路，数据层中的共享统一存储和备份存储、网络安全区（部分）、防火墙（部分），以及运维技术服务。

3.2IP 地址规划

投标方向招标方提供详细的 IP 地址规划建设方案。

- IP 地址规划的重要性：

IP 地址的合理规划是网络设计的重要环节，企业网络必须对 IP 地址进行统一规划并得到有效实施。IP 地址规划的好坏，会影响到网络路由协议算法的效率、性能、扩展及网络的管理，也必将直接影响到网络应用的进一步发展。

❖ IP 地址规划总体要求

IP 地址空间的分配，要与网络拓扑层次结构相适应。既要有效地利用地址空间，又要体现出网络的可扩展性、灵活性和层次性，同时能满足路由协议的要求，以便于网络中的路由聚类，减少路由器中路由表的长度，减少对路由器 CPU、内存的消耗，提高路由算法的效率，加快路由变化的收敛速度，同时还有考虑到网络地址的可管理性。

IP 地址规划将遵循以下总体要求来分配：

（1）唯一性

一个 IP 网络中不能有两个主机采用相同的 IP 地址；

（2）可管理性

地址分配应简单且易于管理，以降低网络扩展的复杂性，简化路由表；

（3）连续性

连续地址在层次结构网络中易于进行路径叠合，缩减路由表，提高路由计算的效率；IP 地址的分配必须采用 VLSM 技术，保证 IP 地址的利用率；采用 CIDR 技术，可减小路由器路由表的大小，加快路由器路由的收敛速度，也可以减小网络中广播的路由信息的大小。

IP 地址分配尽量分配连续的 IP 地址空间；相同的业务和功能尽量分配连续的 IP 地址空间，有利于路由聚合以及安全控制；

（4）可扩展性

地址分配在每一层次上都要留有一定余量，以便在网络扩展时能保证地址叠合所需的连续性；IP 地址分配处理要考虑到连续外，又要能做到具有可扩充性，并为将来的网络扩展预留一定的地址空间；充分利用无类别域间路由（CIDR）技术和变长子网掩码（VLSM）技术，合理高效地利用 IP 地址，同时，对所有各种主机、服务器和网络设备，必须分配足够的地址，划分独立的网段，以便能够实现严格的安全策略控制。

（5）灵活性

地址分配应具有灵活性，以满足多种路由策略的优化，充分利用地址空间；

（6）层次性

IP 地址的划分采用层次化的方法，和层次化的网络设计相应，在地址划分上我们也采用层次化的分配思想。

（7）节约性

根据服务器、主机的数量及业务发展估计，IP 地址规划尽可能使用较小的子网，既节约了 IP 地址，同时可减少子网内网络风暴，提高网络性能。

4.详细设计方案

4.1 总体方案

项目总体设计方案参照本文件第 3.1 节“整体网络拓扑图”的基础上进行建设，投标方需在此网络拓扑图的基础上完善详细设计方案。本项目中建设内容主要分为以下几个部分：

（1）服务器集群与虚拟化建设

按照本次招标要求，对招标方现存的 4 台联想服务器进行扩容改造，安装部署虚拟化环境，承载招标方的各种业务系统。实现资源再利用，以及各种硬件资源的合理分配使用。

（2）数据存储和数据备份建设

按照本次项目建设内容，新购一台全新主数据中心存储作为主业务数据存储，对招标方现有的一台存储进行扩容改造，实现数据备份功能。要求实现部分容灾备份功能。

使用 FC 交换机搭建一套可靠的存储网络，与业务网络进行区分隔离，实现数据的高效传输和利用。

（3）数据库集群建设

本次利用招标方两台物理机实现数据库集群搭建，连接招标方各种需要的应用系统（ERP、OA、PLM 等），实现数据统一管理。

（4）网络安全建设

本次新建防火墙、网络准入系统、终端安全管理系统、防病毒软件、堡垒机、日志审计系统，实现对招标方现有局域网安全的有效管理和监控。

（5）网络运维管理建设

投标方按照本文件第 3.2 节要求规划网络 IP 地址，并按照方案建设。对招标方现有的服务器、虚拟机、数据库、存储、网络安全设备（防火墙、防病毒系统等）、网络设备（交换机、路由器等），有可视化的管理运维平台。

（6）容灾中心与互联网专网建设

在整体网络拓扑图中，互联网与容灾平台建设暂定，中标方需要在后续运维期间协助招标方完成互联网与容灾平台的设计与建设。

4.2 服务器集群与虚拟化

投标方向招标方提供详细的服务器集群虚拟化建设方案。

（1）服务器虚拟化

为了实现公司的业务系统连续、稳定、可靠运行，本次方案设计采用服务器虚拟化技术，通过在计算、存储、网络、可用性、安全和自动化等方面提供的一整套应用和基础架构服务实现了一个完整、高效，安全的虚拟化平台。而服务器虚拟化与运维管理解决方案可以使用户了解整个虚拟化环境的运营状况，实现性能提升，同时优化容量，确保关键应用的稳定健康运行。借助运维管理解决方案，用户可以使用单一控制台来优化容量和监控工作负载性能，例如：用户能够回收未使用的容量、将虚拟机调整至适度规模、改善利用率并提高整合率，从而充分利用虚拟化平台。

（2）数据备份服务器

部署一台服务器装载数据备份软件。

（3）存储

部署一台全闪共享存储与一台备份存储。

（4）光纤交换机（高效传输）

新购 2 台光纤交换机互连各种服务器与存储，组成一套存储网络。

4.3 数据存储和数据备份

投标方向招标方提供详细的数据存储和数据备份建设方案。

4.3.1 数据存储

提供文件存储、块存储、对象存储。

4.3.2 数据备份

按照数据安全、以及系统持续运行的要求，系统应当稳定、可靠运行。然而，计算机应用系统不可避免会遭受到各式各样的故障或运行风险，这些故障或运行风险包括物理故障、逻辑故障、数据丢失等。例如：数据库停机、服务器崩溃、逻辑坏块等等，因为我们必须需要通过有效地技术手段来保障信息化系统在面临这些风险或故障威胁时，尽可能减少或避免停机而带来的损失。本次项目规划、设计方案将采用备份系统。为招标方提供了针对虚拟化平台超可用数据管理平台，在确保任何应用程序、任何云基础架构中的数据随时可用，业务保证持续运行的前提下，还可帮助用户将数据管理方式从基于策略转变为基于行为，提升数据的“智能化”水平，实现数据的自我治理。

支持异地灾备功能，将虚拟机数据定时复制到备份数据中心。支持任何虚拟化环境应用程序提供接近连续的数据保护。通过备份软件上的管理控制台的UI管理接口,提供故障移转和故障恢复功能。

在容灾复制任务进行时，复制软件能够自动感知到应用程序，为在线运行的

应用程序进行复制优化，确保数据一致性的情况下实现虚拟机的在线复制。这是按照虚拟机为单位的颗粒度复制。

另外，虚拟机的复制考虑到带宽限制的因素，首次数据的传输可以去通过备份将数据离线方式存放到异地的数据中心，该功能预先通过离线的方式传输了大量原始数据，因此在后续的传输过程中可以仅传输少量的增量数据，变化的数据，以实现带宽和时间的节省。

整个复制过程可以说是虚拟化平台上的应用级复制，因此并不存在硬件上的限制条件，对环境也没有特殊的要求，只要在源端和目标端都拥有虚拟化平台即可完成数据的传输，实现复制效果。这个不依赖底层存储是否具备复制功能，不依赖底层存储是否相同平台，不依赖存储架构，也不依赖虚拟化平台的复杂度。

在虚拟机层面，容灾复制要求在开始前执行创建一个虚拟机快照，确保数据以及应用的一致性，因此，要求虚拟机能够被创建快照，所有无法创建快照的虚拟机将无法执行这个复制，这是容灾复制的一个限制条件。

设置增量备份和全量备份策略。

4.3.3 存储网络

使用 FC 交换机搭建一套可靠的存储网络，与业务网络进行区分隔离，实现数据的高效传输和利用。

4.4 数据库集群

投标方向招标方提供详细的数据库集群建设方案。

本次利用招标方两台物理机实现数据库集群搭建，实现数据库应用系统的高可用和冗余。

连接招标方各种需要的应用系统（ERP、OA、PLM、MES 系统等），实现数据统一管理。利用数据库本身的特性和安全（实例、用户、权限）功能实现不同应用系统之间的数据隔离和数据安全。

4.5 网络安全

4.5.1 方案总体架构

投标方向招标方提供详细的网络安全建设方案。

依据本方案的设计依据和标准，基于网络安全法和信息安全等级保护的要求，结合安全模型在整体的安全策略的控制和指导下，在综合运用防火墙、身份认证和加密等防护工具的同时，利用防病毒系统、入侵防御、日志审计等系统了解和评估系统的安全状态，并通过备份容灾方式来保证系统在受到破坏后的迅速恢复。

（1）安全策略

安全策略的制定要结合现有的信息系统实际情况制定，安全策略要明确被保护的主体和原因，明确安全工作的具体职责，提供解决出现的问题的基准。安全策略要在一段时期内固定不变。

（2）安全防护

1）物理安全的目的是保护中心机房以及供电设备、服务器、网络安全设备和通信链路等免受自然灾害、人为破坏等攻击；同时能验证用户的身份和使用权限，防止用户越权操作；确保中心机房有一个良好的电磁兼容环境；建立完备的机房安全管理制度，妥善保管备份磁带和文档资料；

2) 网络安全访问控制，防火墙是保证网络安全的重要屏障，可以实现不同安全级别的网络安全隔离，保证内部网络的边界安全。通过制定和实施相应的安全策略保证不同安全级别之间的网络不发生越级通信。防火墙在任何情况下都不应该被旁路。

3) 网关病毒过滤，目前绝大部分的病毒威胁来源于网络，尤其是电子邮件和网页浏览，因此部署一个有效的安全网关防护系统来解决边界病毒、垃圾邮件和非法内容是非常必要的。例如防毒墙、或是配置防毒模块的安全网关，终端的安全防护以网络版的杀毒软件为主，并配以终端安全管理软件，以防止非法外联。

（3）安全检测

1) 入侵检测系统通过扫描网络数据流的特征字段或者探测系统的异常行为，来发现安全攻击的存在。一旦发现攻击可以根据预定的措施自动反应，例如暂时封掉发起该扫描的 IP 地址，同时记录下网络攻击的相关日志以进行追查和溯源。

2) 安全审计收集审计跟踪的信息，通过列举被记录的安全事件的类别，例如明显违反或成功操作的完成等日志信息，能适应各种不同的需要，同时对潜在的侵犯安全的攻击行为起到威慑作用。

3) 安全扫描采用非破坏性的办法来检验系统是否存在被攻击导致崩溃的漏洞。网络安全扫描技术与防火墙、安全监控系统互相配合能够为网络提供很高的安全性。

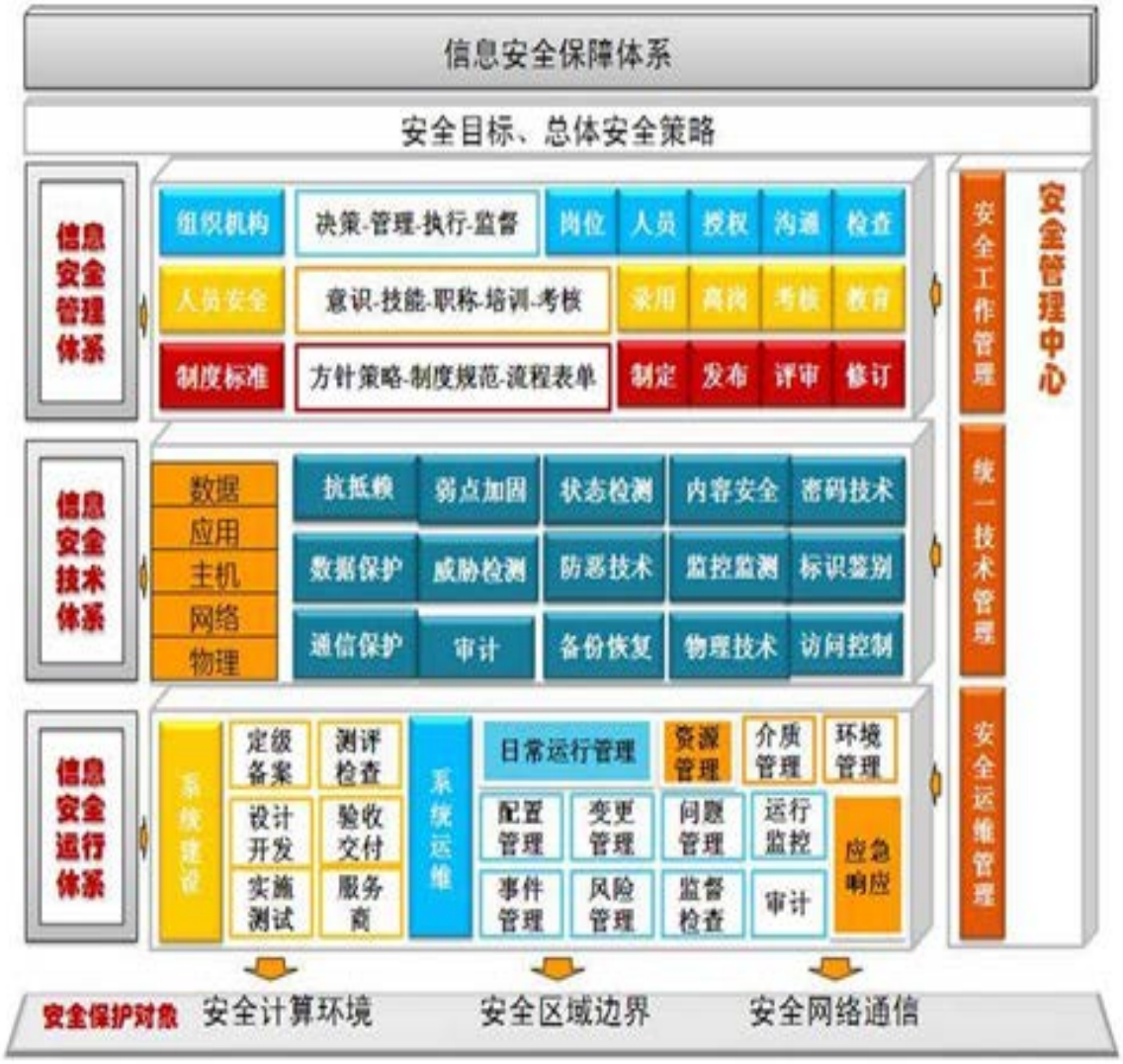
（4）安全响应

安全产品的复杂性和多样性导致很多时候安全产品本身并不能解决网络中出现的所有涉及安全的问题。这就需要安全产品生产商定期提供网络安全风险分析和产品的特征库的更新服务，发现异常并及时处理，以便发生攻击事件时，在最短的时间内提供技术支持和应急预案。

4.5.2 信息安全技术详细设计

目前生产业务管理系统主要包括应用服务器、数据库服务器、OA 服务器、测试服务器和一些交换机、路由器等网络安全设备；具备了信息系统的基本要素，终端用户数 600 余个，分布在园区各车间内，各业务系统的边界并未部署防火墙来进行安全隔离和区分。

本系统主要承载本单位生产信息管理业务，是针对此业务的单一信息系统。生产业务管理系统采用 B/S、C/S 结构设计，各客户端进行数据的采集和检索，服务器端进行数据的加工、存储和传输等。系统整体安全架构如下图：



安全防护解决方案

（初步网络安全拓扑图由技术部门在投标单位进行现场需求调研时给出，投标单位需要准守招标方相关保密规定，不得泄露本项目招投标相关内容）

生产业务管理系统整体分为 5 个区域，分别为核心交换区、安全管理区、服务器区、内网区和终端区，各区域之间通过防火墙实现安全隔离与防护。

1) 核心交换区通过堆叠技术将 2 台物理交换机合并。

2) 终端区由接入交换机组成。接入交换机负责网络内部的数据交换以及数据的快速转发。

3) 安全管理区由下一代防火墙、入侵防御系统、入侵检测系统、网络准入设备、全网流量可视化监控、日志审计系统、运维审计系统、WAF 应用防火墙、数据库审计防火墙、漏洞扫描系统等组成。

4) 服务器区由多台物理服务器组成虚拟化环境，为业务系统提供硬件支持。为了保障虚拟机业务系统的安全，虚拟化服务器应部署东西向虚拟化安全防火墙。

（1）安全域划分方案

安全域建设是基于网络和系统进行安全建设的部署依据；安全域和域边界防护使纵深防护能够有效地实施；安全域边界是灾难发生时的抑制点，防止影响的扩散。根据之前对生产管理系统的分析，一般分为以下几个功能区域，终端域：由所有办公终端组成；服务器域：由生产管理系统的服务器，杀毒服务器和系统备份服务器等组成；安全管理域：由安全管理平台的服务器和安全设备组成，实现对系统的管理。

（2）边界安全方案

安全域划分的主要目的是保证域边界的安全防护。在终端域与服务器域的边界部署防火墙，可以采用透明模式接入两个安全域之间。防火墙采用透明模式的

工作方式无须改变原有网络结构，对网络性能和系统体系结构影响较小；防火墙规则上只开放生产业务管理系统需要的网络端口和地址，可以有效地保护网络。

（3）信息系统防病毒方案

信息系统的终端和服务端需要部署网络版防病毒系统。

（4）网络准入解决方案

部署一套网络准入系统，对公司入网设备进行管理放行。

（5）终端安全管理解决方案

部署一套终端安全管理系统，实现对招标方局域网内设备的有效管理。

安全监测解决方案

安全监测解决方案包括入侵检测方案、漏洞扫描方案、安全审计方案三个方面：

1）入侵检测方案

在网络中部署入侵防御系统对入侵和滥用行为进行检测和审计。通过在网络中部署入侵防御系统，可以提供有效的安全保障。可以检测和发现针对系统的网络攻击行为，对这些攻击行为可以采取记录、报警和主动阻断等动作，以便事后分析和行为追踪。定义禁止访问网站，限制内部人员对不良网站的访问。可以提供强大的网络行为审计能力，让网络安全管理员跟踪用户和应用程序等对网络的使用情况，帮助他们改进网络规划。对入侵防御系统的使用和使用人员的管理一定要有专门的制度。

2）漏洞扫描解决方案

漏洞扫描可以动态地了解网络设备、主机和应用的安全弱点、通过修补这些安全弱点来尽量减少攻击的可能性。它能实现对目标网络稳定的周期性扫描，保证整体网络防护；具有跨过路由器和防火墙进行直接安全分析的能力，能对目标网络实现扫描，扫描对象可以是基于 TCP/IP 协议的网络上的各种服务器或是主机，防火墙、路由器以及 WEB 站点和数据库进行扫描，它帮助系统管理员集中了解系统中存在的安全漏洞，并提供相应的网络安全漏洞解决方案。

漏洞扫描系统采用硬件机架式无限 IP 的系统，部署在安全管理区，旁路接入核心交换机即可。

3）安全审计设计方案

网络安全审计系统采用旁路侦听技术，是主机审计的有力补充。网络审计可以审计任何经由特定网络中间设备的主机的网络信息，基于对网络协议的分析与统计，从网络层对整个网络进行审计与保护。

4.6 网络运维管理

投标方向招标方提供详细的网络运维管理建设方案。

部署一套网络管理运维软件。按照最终确定的 IP 地址规划方案，来进行招

标方的基础网络架构搭建工作。包括但不限于局域网内交换机的配置，服务器的配置等工作。

数据库可视化运维。

部署一台 NTP 时间同步服务器，保证招标方局域网类联网设备和软件系统的时间准确性。

4.7 灾备中心（暂定）

中标方需要在后续运维服务期间协助招标方完成灾备中心的设计与建设。

地震、洪水、火灾非人为灾害也会对数据中心造成全面的破坏，供电问题也会导致数据中心停止运转，从而引发系统停机。为应对这些不可预估的风险，计划在异地搭建应用级容灾系统，以保障公司各种信息化系统的业务的正常运行。

招标方信息管理基础平台发生灾难时,通过手工切换灾备系统能够在15分钟内接管生产中心各业务应用系统。生产系统与灾备系统正常情况下互为备份。需要进行远程容灾的应用系统包括 OA 系统、财务系统、MES、ERP 等系统。灾备中心拟部署在厂区内。

4.8 互联网专网建设方案

投标方针对招标方实际情况提供详细的互联网专线建设规划设计方案（本次项目不实施）。

广域网互联拟采用 SVPN 或者零信任架构规划和设计。

5 实施服务要求

5.1 实施团队要求

投标方应确定由固定人员组成的项目实施团队，**并提交团队人员名单**。项目实施的相关人员一经确定，在项目实施过程中未经招标方允许不得更换，如果出现此情况，招标方除有权要求中标方退还预付款外，还有权追索中标方合同款5%的违约金。如果导致合同不能按期履约，招标方有权按退货索赔程序处理，并要求中标方承担相应的法律责任；如为确保项目实施进度，根据情况需要可以增加高级别的项目实施相关人员。（项目二不作强制性实施团队要求）

以下为中标方实施团队基本资格要求：

（1）项目总监

资质：现任中标方单位的领导职务，具有丰富的服务器集群、网络架构、应用系统架构建设项目经验。核心素质要求具备优秀的沟通、分析和解决问题的能

力。

职责：从总体上把握项目方向、协调管理、阶段性检查和指导，对项目的质量、进度、团队、商务等方面具有决策或者建议权，与招标方领导层沟通项目整体状况。

（2）技术专家

资质：现任中标方单位的核心技术专家，具有丰富的信息技术知识和服务器集群和网络架构建设、应用系统架构建设项目经验。核心素质要求具备优秀的沟通、分析和解决问题的能力。

职责：负责在项目执行过程中就项目阶段成果进行评估及验收，对项目中出现的重大技术问题进行分析与指导。

（3）项目经理

资质：现任中标方单位的项目管理核心人员，具有 3 年以上服务器集群、数据库集群、网络架构建设、应用系统架构建设项目实施经验，精通主流数据库、主流操作系统、网络相关技术；**组织团队实施 2 个以上类似本次项目（服务器集群、网络架构、应用系统架构）实施案例及经验（提供相应的证书及案例资料）**。核心素质要求具备优秀的沟通、分析和解决问题的能力。

职责：作为项目负责人，向项目总监汇报，贯彻上级领导的精神，全面负责项目实施有关的所有问题，包括项目进度、质量、资源配置以及商务协调等，负责问题收集、讨论并跟进问题处理情况、问题总结，并负责监控项目实施落地全流程。

（4）实施工程师

资质：现任中标方单位的项目骨干人员，具有服务器集群虚拟化、数据库集群、网络安全、应用软件架构部署建设等专业知识；具有 3 年以上项目实施经验；具有良好的沟通协调能力。

职责：负责项目实施过程中的需求调研过程的管理与沟通，协调用户和第三方系统开发商积极参与项目管理、测试和验收过程；主导硬件和系统部署、主持技术难点攻关，最终保证系统的功能齐备、性能可靠、运行稳定；负责用户培训，指导用户使用系统和处理常见问题。

5.2 实施过程要求

（1）项目组织管理

投标方和招标方均应详细说明实施本项目拟采用的团队组织方法和具体项目组织机构，保证在此项目实施期间有足够的人力投入和技术支撑，以保证项目质量。要求以计划为核心管理实施任务，以例会和阶段性汇报为核心控制项目进度，执行严格、规范的变更管理流程，针对项目任务和问题及时报告、快速决策执行。

（2）项目进度计划

投标方依据招标方总体计划安排制定详细的项目进度计划，明确规定项目工

作分解结构、具体任务内容、时间节点、交付物及数量、执行人、完成计划所需的资源，标识出项目重要里程碑节点，并依据项目进度计划有序推进项目各阶段实施工作。

（3）项目质量控制

投标方必须按照项目质量管理和质量保证体系，提出具体措施，确保项目质量。项目实施过程中对问题进行登记、跟踪、通告，保持与用户沟通，严格控制，保障项目实施质量。

（4）项目沟通管理

投标方必须在投标文件中详细明确说明项目沟通计划，确保投标方与用户之间、投标方内部、不同项目投标方之间信息沟通顺畅。决策层根据项目进展按需要随时沟通，项目管理层定期和不定期沟通协调，执行层的阶段性汇报、组织项目例会、最终验收会等，并做好会议纪要。实施过程中如实际内容、规格、数量等情况发生变化，由招标方和中标方协商处理。

（5）项目风险管理

投标方应充分认识到项目风险管理的重要性，在投标文件中必须分析识别项目中的各类风险因素，并提出相应的对策。必须通过制定详细实施计划、明确双方工作界面、保障人员稳定等措施，严格控制项目风险。

*5.3 项目交付文件

中标方在项目建设实施过程中将提供相关的文档（含纸质文件和电子文件各1 份），所有产品均要求技术资料完整，有光盘资料的必须提供完整光盘资料，自带软件的要求以光盘（或 U 盘）形式提供，项目二不用提供下列第（1）（2）项文件及第（3）项部分无关文件。项目交付文件清单如下：

（1）需求分析报告

（2）项目整体设计方案

（3）项目实施方案（实施方案含风险分析及措施）和相关图纸（总体架构图、网络拓扑图、总体工程图（机柜内布置图）等）

（4）各软硬件系统上线方案和实施计划表（时间表）

（5）项目实施过程问题记录表

（6）用户试运行意见和问题记录表、软硬件试运行报告

（7）系统安装配置手册、运维操作手册

（8）项目所含设备、软件等的操作指导书、用户操作手册（使用说明书）

（9）常见问题处理手册

（10）可部署和运行的系统代码、安装程序

（11）项目所含设备、软件、材料等的产品检测证书、检测报告及合格证

（12）项目所含关键设备的备件及易损件清单

（13）培训方案和培训记录表

（14）运维技术服务方案和记录（检查报告、运维记录等）

（15）软硬件调试记录、测试报告、竣工方案及竣工图等

（16）项目初步验收和最终验收报告

6 运维服务和技术支持

6.1 运维对象清单

序号	对象名称	运维内容和要求	备注
1	服务器和虚拟化系统	1、服务器硬件安装、调试、维护； 2、虚拟化系统安装、调试、维护、优化、运营维护期内的免费升级； 3、在服务器端，按照招标方需求对操作系统的安装、调试、维护、优化（不限数量）。	
2	数据库	1、主流数据库（Oracle、MySQL、SQLServer等）集群部署安装（双活）； 2、招标方的全部应用系统（ERP、PLM、OA、MES、财务、能源管理、档案管理、网盘系统等）数据库优化； 3、招标方的全部应用系统（ERP、PLM、OA、MES、财务、能源管理、档案管理、网盘系统等）数据迁移（保证数据的安全性和完整性）（招标方如有需要）。	
3	主数据中心存储和备份系统	1、设备和软件系统的安装、调试、维护； 2、存储的分配设置和优化； 3、定期的备份恢复演练、容灾演练。	
4	网络链路和通信（交换机、路由器、网关等）	1、局域网网络地址规划、分配和优化； 2、网络设备调试、网络调试。	
5	网络安全	1、网络调试； 2、网络安全产品（防火墙、防病毒软件、网络准入系统、终端安全管理系统、堡垒机、日志审计系统等）的策略配置和调整； 3、系统集成（如：防火墙的其他安全管理软件的联动配置、应用系统与日志审计系统的联动配置）； 4、定期网络安全演练。	
6	应用系统（包括但不限于：OA、ERP、	1、应用系统架构和部署技术支持服务； 2、应用系统优化技术支持服务；	

序号	对象名称	运维内容和要求	备注
	PLM、MES、能源管理、档案管理系统等）	3、由于招标方应用环境发生变更，其中不涉及软件专门修改的，需要中标方协作的技术支持服务； 4、由于网络或硬件造成的数据错误、丢失，系统不能正常运行； 5、由于后台数据非软件原因造成的错误、丢失，系统不能正常运行； 6、招标方应用软件系统自身应用的问题； 7、应用系统数据迁移和恢复（确保数据安全完整）。 8、各种中间件维护以及软件部署架构技术支持（包括但不限于 nginx、nPart、keepalived、docker、k8s、Apache、Tomcat、IIS 等）	
7	其他	招标方应用需求发生变更，双方确认为超过运维的范围的需求，中标方须积极配合招标方并提供服务，但双方需另外签订合同以确认服务项目及其费用金额： 1、本招标内容之外的二次开发技术支持（如 API 接口、数据库接口等）； 2、招标方在建设方案协议范围外要求中标方提供与第三方软件之间的前台数据接口。	

6.2 技术支持要求

（1）投标方必须具有良好的技术人员储备，包括但不限于网络工程师、数据库工程师、信息安全工程师，系统架构师等并取得相关证书。

（2）投标方人员提供相应的软件架构技术：如 K8S、POD、Docker、Nginx 等技术支持。

（3）在运维服务期间，针对招标方现有的网络架构（包含内部局域网络、安防监控网络、工控网络等全部子网）、网络安全措施、应用系统部署方式和架构提出针对性建议和解决方案。（如：后期扩展升级计划方案、网络架构变更建议、互联网解决方案、应用软件部署方式调整等）。

（4）针对招标方互联网线路和灾备中心提出针对性的建设方案和建议。

（5）在运维服务期间、当招标方系统部署安装应用系统或者迁移应用系统时提供技术支持（包括但不限于数据库技术、操作系统技术、软件部署架构技术等）。

（6）投标方在第 8 节“售后服务及质保要求”的要求之上，制定相应的运维技术服务方案。

7 开箱检验、安装、调试和项目验收要求

7.1 开箱检验

（1）软件系统部署之前，相关系统功能模块清单、实施方案，应由招标方评审通过并签署确认。

（2）硬件到货后，中标方和招标方共同到场开箱验货，查看货物是否完整、无损坏，品牌、型号或规格、技术参数、配置、数量是否符合要求，合格证、检测报告等资料是否齐全，上电自检是否正常。

7.2 安装、调试

（1）合同中提供的所有软硬件设备全部应由中标方负责完成安装，安装过程应作安装详细记录。一切在安装过程中造成的软硬件设备损坏、损失，责任均在中标方。

（2）合同中提供的所有软硬件设备全部应由中标方完成现场调试。在安装、调试、验收期间，中标方的工程师负责对合同项下的货物进行操作、调试及执行必要的维护。在此期间所造成的设备损坏、损失，责任均在中标方。

7.3 项目验收要求

7.3.1 文档验收

依据本文件第 5.3 节“项目交付文件”检查交付的文档资料是否齐全，文档质量是否符合要求、是否完成签署，系统源代码和安装文件是否齐全、准确。包 1（服务器集群虚拟化和运维服务）和包 2（网络安全建设）根据实际情况进行统一验收或者单独验收。

7.3.2 软件验收

（1）到货验收：软件系统部署之前，相关系统功能模块清单、实施方案，应由招标方评审通过并签署确认。评审方式为：招标方按合同及招标文件的要求组织技术人员根据招标方实际需求的合理性、可行性进行评审，并签署验收结论。

（2）初步验收：应用系统试运行之前须对软件功能和性能进行初步验收。验收方式为：招标方按合同及招标文件的要求组织用户对软件进行功能和性能进行测试及初步验收，中标方针对测试出的问题及时整改，并签署验收报告。

（3）最终验收：软件系统试运行完成后进行最终软硬件整体验收。验收方

式为：按招标文件、合同的要求，试运行期间招标方组织用户使用，通过试运行发现和处理系统存在的问题；试运行（一个月）完成后由招标方组织有关专家针对功能和性能情况进行验收评审，并签署验收报告。

7.3.3 硬件验收

（1）到货验收：硬件到货后对硬件进行到货验收。验收方式为：中标方和招标方共同到场开箱验货，查看货物是否完整、无损坏，品牌、型号或规格、技术参数、配置、数量是否符合要求，合格证、检测报告等资料是否齐全，上电自检是否正常，并签署验收结论。

（2）初步验收：硬件安装调试完成后，进行初步验收。验收方式为：招标方按照相关技术要求组织技术人员检查功能及性能是否满足要求，并签署验收报告。

（3）最终验收：硬件安装调试上线运行完成后，进行最终软硬件整体验收。验收方式为：按招标文件、合同的要求，试运行期间招标方组织用户使用，通过试运行发现和处理系统存在的问题；试运行（一个月）完成后由招标方组织有关专家针对功能和性能情况进行验收评审，并签署验收报告。

7.3.4 验收失败

在最终验收失败的情况下，中标方工程师应以书面的形式向招标方说明验收失败的原因，排除故障后重新开始测试验收。如果测试验收失败次数超过三次或测试验收时间超过合同规定的有关期限，招标方有权拒绝验收，有权退货，并按中标方违约处理。招标方除有权要求中标方退还预付款外，还有权追索中标方合同款 10%的违约金。如果导致合同不能按期履约，招标方有权按退货索赔程序处理，并要求中标方承担相应的法律责任。

当招标方认为验收失败而拒绝验收后，中标方工程师可与招标方验收人员共同签署验收失败的备忘录，明确、详细地写明验收失败的原因、存在的问题、招标方的要求以及解决方式、措施和期限。

7.3.5 验收成功

在招标方确认本项目（包 1 或者包 2）中全部软硬件系统安装部署完成之后，整体试运行 1 个月；如无问题由招标方确认最终验收成功，招标方应与中标方工程师共同签署验收报告，若有未尽事宜可写入备忘录中，双方签字后开始生效。

在验收过程中，若发现设备有短缺、损坏或不符合合同条款和质量标准的情况，中标方将负责补齐、更换，由此引起一切费用由中标方承担。

8 售后服务及质保要求

8.1 售后服务

（1）投标方应在招标方所在地或附近地区设有常驻机构以响应招标方的技术服务要求。提供证明材料。

*（2）投标方应在维护期内应提供每周 7 x 24 小时不间断的技术支持响应。在维护期内提供 7 x24 小时小时热线电话、远程在线诊断和故障排除、现场响应以及 Email 和传真支持服务。

*（3）投标方对其提供的应用软件应提供不少于 12 个月（自完成最终验收之日完成起计算）的免费升级及保修服务的保证期。

（4）投标方的技术维护人员应具有 3 年以上维护管理经验，具备良好的沟通、协作能力。

（5）运营维护期内，投标方有责任免费提供如下技术支持服务：

1）电话咨询：投标方必须为招标方提供技术援助电话，解答招标方在系统使用中遇到的任何问题，及时提出解决问题的建议和操作方法；

2）现场响应：自收到招标方的服务请求起 12 小时内，若电话咨询服务不能解决问题，投标方应即刻指派技术人员在 24 小时以内赶赴现场进行故障处理；遇到重大技术问题，投标方应及时组织有关技术专家进行会诊，并在 24 小时内采取相应措施以确保系统的正常运行；

3）事故处理：故障解决后 48 小时内，应向招标方单位提交故障处理报告。 报告中必须说明故障种类、故障原因、故障处理方法等。

*（6）在设备的质保期内，必须由专业技术人员负责对用户的设备进行维修和更换故障部件，更换的设备或部件必须是来自设备原厂商的全新同型设备或备件，不得以其它方式替代。设备的维修时间不得超过 5 天。维修期内由中标方提供备机供招标方使用，备机抵达现场时间为 24 小时以内。

*（7）保修期和运维期限（3 年）之内提供每年不低于 2 次上门预防性主动维护服务和检测，巡检中应对系统性能、运行状况、稳定程度等进行评估，并根据招标方需求经确认后进行优化 ，维修或更换出现故障隐患的设备或部件。每次巡检结束后，需向最终用户提交巡检报告，并出具检测报告，负责提出预示发生问题的解决方案和建议，通过巡检，保证避免出现因系统故障导致生产中断的事故。（**由投标方在投标方案中制定运维巡检方案**）

（8）投标方提供对维保设备的日常升级服务，以及硬件使用和应用系统技术支持，包括人员权限、数据校正与修改等方面的使用维护，以及系统使用过程中的其他问题。

（9）中标方负责应用硬件和相关系统软件的使用性维护，包括 Bug 无条件修复、API 接口提供、一定量的需求变化等（维护期内的非合同约定范围内的新

需求，可以由中标方和招标方共同确定工作量，并根据工作量进行报价，且中标方须给予最大限度的费用优惠）。

8.2 质保要求

（1）从最终验收合格之日起，项目质保期为 12 个月(硬件设备质保期若大于 1 年，质保期按照厂家最长质保期执行；若硬件设备质保期小于 1 年，中标方需提供质保满 1 年)；

（2）1 年质保期届满，中标方提供延期 2 年的运维保障与技术服务，详细运维保障需求见本文件第 2.4 节“实施与技术服务”，在总共 3 年运维服务届满之后，招标方可根据需要，与中标方签订有偿的系统维护运维协议；

（3）质保期内，如中标方公司被兼并或收购，兼并或收购公司有责任继续对招标方履行服务；

（4）中标方保证备品备件能够满足质保期结束前正常运行及维修的需要，并提供关键设备的备件及易损件清单，便于招标方进行采购储备，确保后期维修维护。

9 其他要求及说明

9.1 培训要求

（1）培训内容包括但不限于：虚拟化技术、主流数据库（Oracle、MySQL、SQLServer 等）、主流操作系统（Windows、Linux 等）、服务器配置、网络设备配置、硬件设备使用、应用系统使用、软件部署架构技术（包括但不限于 nginx、nPart、keepalived、docker、k8s、Apache、Tomcat、IIS 等）等等。

（2）投标方应根据投标产品的实际需要，在投标文件中提出详细具体的培训方式，明确培训课程内容和目的、培训时间、培训方式、培训对象、培训效果等。采用上级试用、持续跟踪等方式，确保应有的培训效果。

（3）投标方须为招标方不同层次、不同类别的用户分别提供不同类型的培训，保证招标方所有使用人员在培训后能够独立使用各系统的所有功能模块。

（4）投标方须为招标方维护人员提供技术运维培训，确保招标方维护人员在培训后能够独立安装、部署、维护平台系统，能够处理常见软硬件问题。

9.2 知识产权承诺

（1）投标方**须承诺**在本项目中提供招标方的软件产品均为投标方自主开发的产品或投标方合法采购使用的产品，招标方的合同价格须包含购买投标方在本项目开发过程中用到的自主版权产品的使用权。

（2）投标方**须承诺**，如果投标方在软件开发过程中涉及第三方产品的知识产权，一旦出现技术、经济或法律上的纠纷，由投标方全面承担并全权解决，确保不影响招标方的使用。

9.3 保密要求

投标方应承诺在项目调研、方案设计和施工过程中严格遵守国家保密法律、法规，严格执行招标方的保密要求，**并签署保密协议**。对接触到的国家秘密事项、招标方商业秘密信息、招标方所提供的项目资料及图纸等承担保密责任，在任何情况下绝不泄密，不扩散，否则投标方承担相应的法律责任直至刑事责任。

9.4 环境安全

（1）投标方根据工程需要安全防护；负责施工现场安全保卫，所有费用都须包含在合同价款中；投标方应严格按照国家相关政策、法律法规和招标方有关施工安全和技术规范、规格、标准组织施工。

（2）投标方保证施工现场清洁规范、卫生达标，符合环境卫生管理的有关规定，施工过程中及时清理与本工程无关的任何多余物品及其垃圾等，做到工完场清，承担因违反有关法律法规和招标方规定造成的损失与罚款。

（3）投标方在进行项目实施时，应严格遵守国家及招标方在安全管理和环境保护方面的各种规章制度，**并签署安全相关方协议**，对于因投标方违反相关规定而造成的人员伤亡或设备损坏等事故，招标方不承担任何责任，投标方负全部责任，同时如对招标方环境造成破坏的，投标方应负责赔偿相应经济损失。

编制:　　审核:

会签:　　批准：