财政网络基础平台(升级改造)

项目采购需求

# 项目概况

## 项目背景

上海市财政局位于徐汇区肇嘉浜路800号，是主管上海市财政收支、财税政策、国有资本金的市政府组成部门。上海市财政局现有计算机网络系统主要包括政务外网、财政业务网以及互联网，自2010年起使用至今，除局部需求增加陆续添置设备外，未进行过结构优化及整体升级改造，目前大部分设备服役超过12年。

目前上海市财政局大部分网络设备服役年限也超过12年，稳定性受到极大挑战，各设备运行状态缺乏有效实时自动监控，无法做到主动运维，运维成本较高。且部分核心设备为国外品牌，不符合信创等相关要求；机房内UPS、精密空调等设备作为保障机房环境的核心基础设施，使用年限也超过12年。空调故障频发，通过频繁维修勉强维持。部分设备及配件如UPS电池等超过设计使用寿命，性能衰减且不稳定；机房动力环控系统仍采用早期485串口通讯方式，视频监控系统为模拟信号系统，维修难度高，缺乏备件。

因此市财政局基础设施系统在系统设备、安全防护、可靠运营三方面存在诸多薄弱环节，对财政局的日常业务产生了潜在的影响和风险。急需对市财政局计算机网络及基础设施进行升级改造，同时提升软件系统性能和安全保障，使网络基础设施及相关配套系统能更好地支撑市财政局各项业务的正常运行。

## 建设期限

建设期限：自合同签订之日起6个月。

## 建设地点

建设地点：肇嘉浜路800号（上海市财政局）

## 是否按信创要求建设

是否按信创要求建设：是

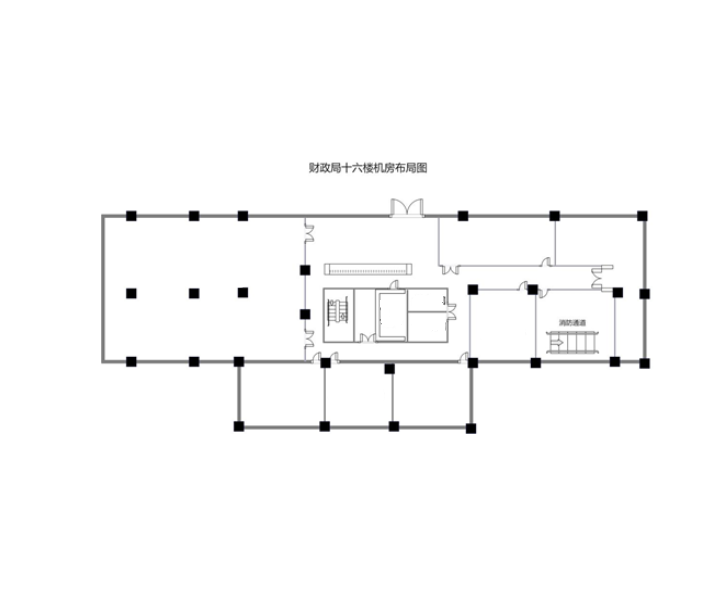
## 运维后所属大系统

运维后所属大系统：基础设施

# 机房和网络现状

## 现有机房结构情况

目前上海市财政局机房位于肇嘉浜路800号16楼，机房布局如下图所示：



## 网络现状

目前上海市财政局计算机网络系统整体分为物理隔离的业务网及政务外网，其中业务网上联财政部，下联16个区县财政，同时与财政直属单位等进行网络连接。

目前上海市财政局大部分网络设备服役年限超过12年，稳定性受到极大挑战，目前各设备运行状态的缺乏有效实时自动监控手段，无法做到主动运维，运维成本较高。且部分核心设备为国外品牌，不符合信创等相关要求。

政务业务应用已迁移至政务云，而原来提供负载均衡的设备存在必要性不强。政务外网出口部署两条链路，但需要手动机进行切换，可靠性不高。政务云服务目前通过单台防火墙访问财政部业务网，存在单点故障风险，其它较多接入设备同样存在单点故障风险，访问使用的稳定可靠性较低。

网络安全防范手段只限于局部边界防护，缺乏入侵防御、防毒、防APT等，防护手段单一，缺乏立体防护体系。缺乏安全管理中心、日志管理等，互联网出口安全防范缺失。

现有计算机网络体系无带外管理专网，流量混杂，无统一化的网络监控管理和运维管理平台，运维效率偏低，管理手段较为缺乏。

## 机房现状

上海市财政局机房内UPS、精密空调等设备作为保障机房环境的核心基础设施，使用年限超过12年，空调故障频发，通过频繁维修勉强维持。部分设备及配件如UPS电池等超过设计使用寿命，性能衰减且不稳定。

2022-2023年，空调及UPS系统已多次发生较大故障。

目前机房动力环控系统、门禁系统、视频监控系统、消防系统使用超过12年，性能较为落后，较多管理设备存在故障，系统无法正常有效使用。动力环控系统仍采用早期485串口通讯方式，视频监控系统为模拟信号系统，维修难度高，缺乏备件，管理设备存在故障。

# 建设目标

通过本项目的建设，打造一个在未来5-10年内能满足市财政局电子政务发展需求、安全可靠、性能先进、可视可管可控、具有较强拓展能力的计算机网络系统以及支撑计算机网络系统运行的基础环境。

当前市财政局计算机网络安全防护体系较为薄弱，通过项目建设，对网络安全进行合理地升级改造，打造较为完善的安全防护体系，满足《上海市电子政务外网建设和运行管理指南》及《信息安全技术网络安全等级保护基本要求》等规范要求，提高系统整体安全性。

市财政局机房环境基础设施老旧，难以为机房内部署的网络系统进行良好支撑，通过项目建设，对机房环境的基础设施进行升级更替。

## 设计原则

在财政局网络的设计和建设中，需严格遵循以下原则：

1. **兼容性：**在有线网络和无线网络设备选型上，必须在是行业成熟应用的设备，具备优秀的兼容性和高性能，在网络设计过程中采用国际标准协议兼容的网络，并能够兼容在将来扩容不同厂商的设备；
2. **高可靠：**应采用高可靠的产品和技术，充分考虑系统的应变能力、容错能力和纠错能力，确保整个网络基础设施运行稳定、可靠。当今，关键业务应用的可用性与性能要求比任何时候都更为重要，在行业有大量的应用案例，特别是关键业务、核心业务节点；
3. **高安全：**网络基础设计的安全性，涉及到业务的核心数据安全。应按照端到端访问安全、网络L2-L7层安全两个维度对安全体系进行设计规划，从局部安全、全局安全到智能安全，将安全理念渗透到整个财政局网络中，能够灵活地扩展安全插卡业务，通过分布式的安全技术，打造密不透风的安全防护体系；
4. **先进性：**本网络将长期支撑财政局的业务发展，而网络又是信息化业务的基础支撑平台，因此本项目的建设需要考虑后续的机会成本，采用主流的、先进的技术和产品，保证基础支撑平台5年内不会被淘汰，从而实现投资的保护；
5. **易管理：**整体网络建设中，设备繁多，各种协议和应用部署越来越复杂，对运维人员的要求也越来越高，单独依赖运维人员个人的技术能力和业务能力是无法保证业务运行的持续性的。因此需要提供完善的运维管理平台，对整个财政局网络的资源进行全局掌控，一旦出现故障，能够借助智能运维系统直观、快速定位，减少日常运维的工作强度。

## 主要技术指标包括

1) 计算机网络时延<30ms，抖动<20-30ms，丢包率<0.5%；

2) 对于单台网络设备要求MTBF大于5万小时；

3) 对于恢复单台网络设备故障MTTR小于30分钟；

4) 网络不出重大故障的比率不低于99.9%；

5) 对出现的网络安全问题提供调查的依据和手段；

6) 通过网络审计，可以记录访问者在网络中的活动。

7）通过有效排放设备产生的热量，帮助维持机房内的热平衡，防止设备过热，维持机房温度在25±2°。。

8）维持机房内适宜的湿度水平，有助于防止设备静电、腐蚀等问题，提高设备的可靠性，保证机房适度在50%±5%。

9）稳定的运行环境有助于提高设备的稳定性，减少硬件故障的风险，延长设备寿命。

10）能够过滤电力中的波动和噪音，提供干净、稳定的电源，有助于防止设备受到电力问题的损害，UPS备电在30分钟以上，保证不出现供电故障率在99%以上。

11）通过机房动力环境监控系统，实现“集中监控、精确定位故障、高效管理”的管理模式；并通过设置联动，使各子系统协同工作；同时还对整个系统的扩展性进行充分考虑，并在设计时预留相应接口，以方便将来的升级需和扩容。

12）保证机房综合安防系统适应趋势要求，完善监控系统，门禁系统的改造升级，并纳入机房动力环境监控系统，实现集中管理。

本项目业务绩效指标包括：

通过本项目的建设实现网络的集约化和高效管理，解决网络系统中存在较多单点故障风险。优化设计网络拓扑架构，提升整体网络系统运行效率，节约投入，同时确保系统性能、运行稳定、统一可管可控。通过机房基础设施的升级和优化，保证机房环境稳定，提升设备使用寿命和机房安全的监控管理。

# 项目建设内容

## 建设内容

1. **网络升级改造**

以“集中统一管理、按需共享交换、有序开放竞争、安全风险可控”为基本原则，政务信息化建设与管理进一步集约化，本次需通过重新优化设计网络拓扑架构，提升整体网络系统运行效率，节约投入，同时确保系统性能、运行稳定、统一可管可控，确保演进能力和运维能力。

通过高效一张网将现有的政务外网和财政内网参考“一网双平面设计”进行了优化整合，采用接入和核心的二层架构设计极大满足了建设与管理进一步集约化。

项目中核心交换、核心防火墙、关键出口区均采用冗余设计，同时多个功能区之间采用边界防护实现网络的可靠访问，各功能之间链路均采用了链路冗余设计，实现高可用。

网络改造内容主要分为以下几部分：

1.通过建设一个可靠性高的转发网络，将原有的政务外网和财政内网两个接入网进行融合，提供一个融合、可靠、快速的接入网络。

2.根据要求建立一个独立的安全管理区，通过专业的安全设备，配置安全规则对全网进行统一的安全防护。

3.在连接政务外网、财政部、区县财政接入的出口区部署接入路由器和边界防火墙，对出口接入区进行边界安全防护。

4.核心交换机、核心防火墙、路由器等均采用虚拟化的部署方式，提高整体网络的健壮性和易管理性，避免因为流量来回路径不统一被防火墙拦截的问题。

5.原有旧设备进行并网融合，在确保网络安全和稳定性的前提下，对部分网络设备利旧；

6.完成弱电间接入层网络设备更新，网络布线的优化整理，本次改造旨在对原有老旧核心交换、路由设备进行升级更新，替换老旧设备，并对原有网络架构和流量模型进行标准改造和升级，提升设备的性能和稳定性，保障网络架构的合理性。

1. **网络安全加固**

1.对计算机网络设备进行带外管理改造，将管理流量与业务流量进行物理分离。

2．建立部署一套统一的市财政局运维管理平台，打造“监管控营服一体化”理念，建立可控可管、全景可视的网络监管和运维体系，帮助市财政局面对当前较为复杂的网络业务需求，提升运维及管理协同能力。

3.通过部署日志审计，实时不间断地采集用户网络中各种安全设备、网络设备、主机、操作系统、以及各种应用系统产生的海量日志信息，并将这些信息汇集到审计中心，进行集中化存储、索引、备份、全文检索、实时搜索、审计、告警、响应，并出具丰富的报表报告，获悉全网的整体安全运行态势，实现全生命周期的日志管理。

4.通过部署防火墙和网管平台寻找现网设备，对其进行资产识别管理。可以对各类网络设备、安全设备和终端设备等进行综合检测。主要用于分析和指出存在的相关安全问题及被测系统的薄弱环节，给出详细的检测报告，在业务环境受到危害之前为安全管理员提供专业、有效的安全分析和修补建议。

1. **机房及配套设施升级改造**

调整机房布局及对应搬迁，对现有机房精密空调系统、UPS系统、消防系统、视频监控系统及动环监控系统进行升级改造以满足项目需求。

1）改进现有空调系统，以提高整体的能源效率，采用更智能的控制系统，根据实际需求调整设备运行状态。

2）精密空调提供更先进的故障诊断和预防功能，有助于提高机房设备的可用性，提高通风和空气流通性。

3）升级UPS系统有助于提高电力质量，确保机房在电力故障或波动时仍能保持正常运行，提高整体电力稳定性，满足机房不断增长的电力需求。

4）更新UPS系统支持更先进的系统集成和监控功能，能够与其他设备和监控系统无缝协同工作，提高系统可管理性，并以降低整个机房的能耗，符合节能环保的趋势。

5）动力及环境监控管理全新改造，包括动力系统的监控（配电柜、UPS、蓄电池等）、环境系统的监控（温湿度、空调、漏水等）、安防系统（门禁系统、视频监控系统）以及消防监控（消防烟雾检测）。

6）更新机房安防措施，采用数字监控和门禁系统系统，提供综合安防能力，提高安防保障水平，进一步加强安防效果，满足机房的安全要求。

## 硬件购置清单

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **类别** | **配置要求** | **数量** | **单位** |
| 1 | 网络设备 | 交换机-  核心交换机 | 1.交换容量≥70Tbps  2.包转发率≥ 57000Mpps  3.硬件可靠性所有单板支持热插拔、支持主控板、风扇、电源冗余，主控板主备切换无丢包、风扇模块冗余  ▲4.线卡/接口要求支持扩展防火墙和IPS业务卡  5.支持4K VLAN;支持VxLAN  6.支持MPLS L2VPN、VPLS、L3VPN、TE及MCE功能  7.支持虚拟化：支持一虚多技术、支持跨设备链路聚合  8.管理和监控支持SNMP V1/V2/V3、Telnet、RMON、SSH功能  9.支持OpenFlow1.3标准  10.支持IP分片重组、支持VoQ  **11.配置要求实配**：冗余主控、冗余交流电源、万兆光口≥16个，千兆光口≥24个，千兆电口≥48个、2个万兆多模模块、38个千兆多模模块  12.提供工信部入网证 | 2 | 台 |
| 2 | 网络设备 | 交换机-安全设备互联交换机 | 1.交换容量≥330Gbps  2.转发性能≥100Mpps  3.硬件规格高度1U，固定接口交换机  4.支持4K VLAN  5.支持IPv4静态路由、RIP、OSPF、支持IPv6静态路由、RIPng、OSPFv3  **6.配置要求实配**：千兆光口≥24个（含≥8个combo口）、万兆光口≥4个、2个千兆多模模块  7.提供工信部入网证 | 2 | 台 |
| 3 | 网络设备 | 交换机-楼层和机房接入交换机 | 1.交换容量≥430Gbps  2.转发性能≥80Mpps  3.硬件规格高度1U，固定接口交换机  4.支持4K VLAN  5.支持IPv4静态路由、RIP、OSPF，支持IPv6静态路由、RIPng、OSPFv3  **6.配置要求实配**：千兆电口≥48个、千兆光口≥4个、2 个千兆多模模块  7.提供工信部入网证 | 18 | 台 |
| 4 | 网络设备 | 交换机-楼层和机房接入交换机 | 1.交换容量≥330Gbps  2.转发性能≥50Mpps  3.硬件规格高度1U，固定接口交换机  4.VLAN支持4K VLAN  5.支持IPv4静态路由、RIP、OSPF，支持IPv6静态路由、RIPng、OSPFv3  **6.配置要求实配**：千兆电口≥24个，千兆光口≥4个，2个千兆多模模块  7.提供工信部入网证 | 26 | 台 |
| 5 | 网络设备 | 路由器-区财政接入区汇聚路由 | ▲1.体系架构支持主控板、转发板完全物理分离；为便于接口扩容，转发板采用子母卡架构设计，子卡母板均支持直接热拔插  2.交换容量≥70Tbps  3.包转发率≥6000Mpps  4.单槽IPv4、IPv6转发性能≥200Gbps  5.整机最大业务槽（子卡槽）位数≥8  ▲6.EIGRP支持EIGRP  7.支持IFIT随流检测技术  8.支持子接口切片技术  9.支持DRE、LZ、TFO等多种广域优化手段、支持WEB CACHE  10.支持并实配1个100M/155M模块  **11.配置要求实配：**双主控板，冗余交流电源，4个千兆多模光模块，1个100M/155M单模模块，4个OC-3c/STM-1 CPOS/ATM端口  12.提供工信部入网证 | 2 | 台 |
| 6 | 网络设备 | 路由器-政务外网出口区路由器 | 1.包转发率≥60Mpps，  2.交换容量≥100Gbps  3.槽位数≥6  4.电源系统冗余交流电源  5.虚拟化支持虚拟化特性，将物理上两台设备虚拟化成一台逻辑设备（提供第三方检测报告证明）  6.支持IPv6-IPv6报文前缀转换  7.支持IPv6 NetStream  ▲8.具备SRv6 Ready认证  9.支持Telemetry功能  10.支持iFIT随流检测技术  11.支持子接口切片技术  12.支持ssl vpn  **13.配置要求实配：**冗余交流电源，千兆电接口≥16个，万兆光口≥6个，1\*SFP+电缆3m，4个千兆多模光模块；  14.提供工信部入网证 | 2 | 台 |
| 7 | 网络设备 | 路由器-财政部出口区路由器 | 1.包转发率≥60Mpps，  2.交换容量≥100Gbps  3.槽位数≥6  4.电源系统冗余交流电源  5.虚拟化支持虚拟化特性，将物理上两台设备虚拟化成一台逻辑设备（提供第三方检测报告证明）  6.支持IPv6-IPv6报文前缀转换  7.支持IPv6 NetStream  ▲8.具备SRv6 Ready认证  9.支持Telemetry功能  10.支持iFIT随流检测技术  11.支持子接口切片技术  12.支持ssl vpn  **13.配置要求实配：**冗余交流电源，千兆电接口≥16个，万兆光口≥6个，1\*SFP+电缆3m，4个千兆多模光模块；  14.提供工信部入网证 | 2 | 台 |
| 8 | 网络设备 | 路由器-各区外联路由器 | 1.包转发率≥9Mpps  2.槽位数≥4  3.交换容量≥30Gbps  4.电源系统冗余交流电源  5.虚拟化支持虚拟化特性，将物理上两台设备虚拟化成一台逻辑设备  6.支持IPv6-IPv6报文前缀转换  7.支持IPv6 NetStream  ▲8.具备SRv6 Ready认证  9.支持Telemetry功能  10.支持iFIT随流检测技术  11.支持子接口切片技术  12.支持ssl vpn  **13.配置要求实配：**冗余交流电源，千兆电接口≥4个（含2个combo口），千兆光口≥2个  14.提供工信部入网证 | 17 | 台 |
| 9 | 机房建设 | 精密空调（40KW）-机房用精密空调 | 能效等级：1级；制冷量（KW）：41.2;制热量（kW）:9;制冷工质:R410a;风量（立方米/小时）:11000;送风方式:下送风;温度控制范围及精度:17-28℃±1℃;湿度控制范围及精度:40-60%±5%;噪音（dB）:55;余压（Pa）:75;  提供相关证明，指标需满足上表参数（回风工况、总冷量、显热制冷量、风量、能效比）  室内空调机组要求100%全正面维护，需可以靠装、并柜安装。操作及维修安全、方便，电控盒采用可抽拉设计，便于维护。  为保证产品运行可靠，投标产品优先选用高效节能产品，要求双压缩机系统每套独立的系统都为变频系统，不接受采用“一定一变”的配置。 | 2 | 台 |
| 10 | 机房建设 | 精密空调（80KW）-机房用精密空调 | 能效等级：1级；制冷量（KW）：80.2;制热量（kW）:9;制冷工质:R410a;风量（立方米/小时）:25000;送风方式:下送风;温度控制范围及精度:17-28℃±1℃;湿度控制范围及精度:40-60%±5%  提供相关证明，指标需满足上表参数（回风工况、总冷量、显热制冷量、风量、能效比）  室内空调机组要求100%全正面维护，需可以靠装、并柜安装。操作及维修安全、方便，电控盒采用可抽拉设计，便于维护。  为保证产品运行可靠，投标产品优先选用高效节能产品，要求双压缩机系统每套独立的系统都为变频系统，不接受采用“一定一变”的配置。 | 2 | 台 |
| 11 | 机房建设 | 精密空调（40KW）-配电间用精密空调 | 能效等级：1级；制冷量（KW）：41.2;制热量（kW）:9;制冷工质:R410a;风量（立方米/小时）:11000;送风方式:下送风;温度控制范围及精度:17-28℃±1℃;湿度控制范围及精度:40-60%±5%;噪音（dB）:55;余压（Pa）:75;  提供相关证明，指标需满足上表参数（回风工况、总冷量、显热制冷量、风量、能效比）  室内空调机组要求100%全正面维护，需可以靠装、并柜安装。操作及维修安全、方便，电控盒采用可抽拉设计，便于维护。  为保证产品运行可靠，投标产品优先选用高效节能产品，要求双压缩机系统每套独立的系统都为变频系统，不接受采用“一定一变”的配置。 | 2 | 台 |
| 12 | 机房建设 | 精密空调配套配件 | 传输系统要求:铜管液,2\*φ22，气管2\*φ28（80KW）；液管φ19，气管φ28（40KW），电缆ZB-YJVR4\*25+1\*16mm²（80KW）电缆ZB-YJVR4\*16+1\*10mm²（40KW） | 1 | 批 |
| 13 | 动力设备 | UPS主机 | UPS主机：  输出电源波形：≤1%（阻性满载）；电池类型：铅酸蓄电池；额定输出功率（最低）：60；整机效率：97；切换时间（ms）：0；通信功能：RS485、MODBUS、干接点.  高频UPS应具备发电机智能管理功能，更好解决发电机配置及控制；高频ups应能够设置发电机启动模式、发电机额定功率、启动发电机等参数；通过UPS管理界面重新定义发电机供电功率与UPS匹配。  主机应对其内部易损器件具有智能化管理功能，要求可开启或关闭母线电容使用年限告警功能、可设置母线电容使用年限、可开启或关闭风机使用年限告警功能、可设置风机电容使用年限等，智能化管理易损部件，减少运维工作。  智能化电池管理功能：具有电池管理功能丰富，具有电池标准测试/深度测试/取消测试，还可以开启或关闭定时均充、强制均充、强制充电等功能，既方便电池日常维护，也可延长电池使用寿命。  主机具备EPO远程干接点接口，灵活使用，确保现场紧急状况下能够快速断电，保护设备安全。 | 2 | 台 |
| 14 | 动力设备 | UPS电池 | UPS电池铅酸蓄电池免维护12V150AH蓄电池。  蓄电池品牌需与主机为同一品牌，方便设备统一管理和用户维护  输入电压范围：线电压138Vac~485Vac 或相电压80Vac～280Vac，输入电压宽，适应恶劣电网环境，过载能力：125%负载维持：≥10分钟，电池电压：±14～±24节可调，额定电池电压±168～±288V 。  中文触摸液晶屏：具有LCD+LED指示的操作界面，方便操作人员实时查看工作状态和运行信息，管理更加直观 。 | 72 | 个 |
| 15 | 动力设备 | UPS配电柜- UPS配套配件 | 含连接线，电池柜，开关箱和配电柜，配电柜内含内含4路输入3P160A输入开关、4路输出3P160A输出开关及其他配套材料。 | 1 | 批 |
| 16 | 机房建设 | 门禁系统 | 读卡器：  认证方式：刷卡、密码  读卡频率：13.56MHz  可识别卡：国密CPU卡  按键方式：触摸按键  通讯方式：RS485+Wiegand  工作电压：DC 12V  功耗：≤2W  安装方式：无底盒壁挂、86底盒、120底盒安装  工作环境：室内，不防水 | 1 | 套 |
| 17 | 机房建设 | 视频监控系统-高清摄像监控终端 | 400万海螺型网络摄像机： 最高分辨率可达2560 × 1440 @25 fps 支持用户登录锁定机制，及密码复杂度提示 支持SmartIR，防止夜间红外过曝 支持背光补偿，强光抑制，3D数字降噪，数字宽动态，适应不同环境 支持ROI感兴趣区域增强编码 支持开放型网络视频接口，ISAPI，SDK，GB28181协议，支持萤石平台接入 1个内置麦克风 采用高效阵列红外灯，使用寿命长，红外照射最远可达30 m 符合IP66防尘防水设计，可靠性高 | 21 | 套 |
| 18 | 机房建设 | 视频监控系统- 32路硬盘录像机（含硬盘） | 2U标准机架式8盘位网络硬盘录像机，ATX电源；支持满配8TB硬盘（总容量可达64TB)；2个HDMI接口、2个VGA接口，异源输出，可支持4K输；2个10M、100M、1000Mbps网口；接入能力：32路H.264、H.265格式高清码流接入；含4块6T硬盘 | 1 | 套 |
| 19 | 机房建设 | 视频监控系统-安防综合管理平台 | 综合安防一体化管理主机：  包含安防基础包、视频监控、门禁管理出入人员测温、视频联网、入侵报警、设备网络管理  ▲300路视频，50个门禁，1万人员，200个防区管理， 支持测温防疫、等热点报警事件，支持人员离岗等智能监控报警事件  【硬件规格】  2U标准机架式4盘位一体机，ATX电源  64位多核高性能处理器  DDR4高频率内存条  1个HDMI接口、1个DP接口  2个10M/100M/1000Mbps网口  2个USB2.0接口、2个USB3.0接口  【产品性能】  存储能力：32路  解码能力：最大支持8×1080P | 1 | 套 |
| 20 | 机房建设 | 视频监控系统-安防配套配件 | 包含国标六类非屏蔽网线，一台千兆32路POE交换机，KBG管道等配套材料。 | 1 | 批 |
| 21 | 机房建设 | 消防系统-消防设备 | 报警主机：工作电源：主电AC220V(+10% ～ -15%)50±1Hz；备电：DC24V 7AH  总线容量：4回路，每回252点，共计1008个地址；显示盘数：系统型32台，回路型8台(每回路)；属性识别：自适应式  功 耗：监控功率≤30W，最大功率≤300W（不包括联动电源） | 1 | 套 |
| 22 | 机房建设 | 消防系统-七氟丙烷机房气体充装 | 送检钢瓶，并预计填充320公斤气体，同时送检期间的临时消防设施租用 | 1 | 套 |
| 23 | 机房建设 | 环境监控系统-终端监测 | 检测监测内容包括：UPS检测、消防检测、空调检测、配电检测、环境检测、漏水监测、安防检测  保证系统的稳定性及降低故障点，要求UPS、空调、配电、温湿度、漏水等设备直连监控主机，无需通过其他设备中转。 | 1 | 套 |
| 24 | 机房建设 | 环境监控系统-动力环境集中监控系统 | 单机版管理软件：软件稳定可靠，可实现数据机房及其周边环境的全面监控和管理，支持多用户，用户可通过该软件实时掌握机房的运行状况，支持语音、短信、电子邮件等报警功能，实时监控各子系统运行状态、通讯状态、参数、配置;数据实时采集、分析、存储;统一管理，查询各节点数据。支持报表导出，及历史数据查询。  ▲提供软件国产化服务器、操作系统、数据库适配证明。 | 1 | 套 |
| 25 | 机房建设 | 环境监控系统-环控主机 | 环境监控主机技术要求：  ▲1、监控主机采用免受病毒侵扰的嵌入式Linux系统（非windows系统）主机，主机19英寸，1U机架式安装。  2、主机硬件能存储10万条以上数量的历史数据和报警数据，掉电不丢失。  3、嵌入式主机，集成度高，监控主机须内置短信、语音报警模块、短信报警模块，主机支持IP电话功能。  4、嵌入式主机内置嵌入式web，管理人员不通过任何软件、插件即可查看监控数据信息，对主机进行配置管理。  5、嵌入式主机据有远程升级的能力（不用拆卸主机即可完成升级）。   1. 嵌入式主机系统硬件需具备完整的监控报警功能，网络中断、PC（服务器）端软件、操作系统故障等，均不影响监控主机的监控报警功能，仍然可以实时发出报警信息。网络恢复正常，系统可以自动恢复，无需人工干预。   基本功能接口要求：  （1）双电源，双网口设计，10M/100M自适应以太网接入口；  （2）最少8路独立的RS232/RS485串口，RJ45接口形式（内置），支持软件定义接口工作模式；  （3）6路以上数字开关量采集接口，RJ45接口形式（内置）；  （4）4路以上远程输出控制端DO口（内置）；  （5）主机自带LCD预警屏，能直接显示系统状态。 | 1 | 套 |

## 安全产品购置清单

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **类别** | **功能说明/配置要求** | **数量** | **单位** |
| 1 | 边界安全 | 政务外网出口边界千兆防火墙 | 1.采用多核架构，具备可插拔冗余电源模块，可插拔冗余风扇模块；  2.支持配置自动备份和回滚（提供功能截图）；  3.要求具备接口扩展能力；  4.接口要求：千兆电口≥12个，千兆光口≥8个，万兆光口≥4个，实际配置IPS、防病毒、应用识别特征库升级授权≥3年；  5.性能要求：吞吐量≥4Gbps，并发连接数≥100 万，新建连接数≥8万，开启IPS、防病毒、应用识别模块后吞吐性能≥4Gbps；  6.支持路由模式、透明（网桥）模式、混合模式；  7.支持静态路由、策略路由、RIP、OSPF、BGP、IS-IS等路由协议；  8.支持一对一、多对一、多对多等多种形式的NAT  9.支持IPsec VPN智能选路，根据隧道质量调度流量；  10.应用识别支持至少9000条以上的应用识别  11.入侵防御支持超过18000条以上特征的攻击检测和防御；  12.防病毒本地库数量600万+ | 2 | 台 |
| 2 | 边界安全 | 财政部出口边界千兆防火墙 | 1.采用多核架构，具备可插拔冗余电源模块，可插拔冗余风扇模块；  2.支持配置自动备份和回滚（提供功能截图）；  3.要求具备接口扩展能力；  4.接口要求：千兆电口≥12个，千兆光口≥8个，万兆光口≥4个，实际配置IPS、防病毒、应用识别特征库升级授权≥3年；  5.性能要求：吞吐量≥4Gbps，并发连接数≥100 万，新建连接数≥8万，开启IPS、防病毒、应用识别模块后吞吐性能≥4Gbps；  6.支持路由模式、透明（网桥）模式、混合模式；  7.支持静态路由、策略路由、RIP、OSPF、BGP、IS-IS等路由协议；  8.支持一对一、多对一、多对多等多种形式的NAT  9.支持IPsec VPN智能选路，根据隧道质量调度流量；  10.应用识别支持至少9000条以上的应用识别  11.入侵防御支持超过18000条以上特征的攻击检测和防御；  12.防病毒本地库数量600万+ | 2 | 台 |
| 3 | 边界安全 | 互联网出口边界千兆防火墙 | 1. 设备采用多核多平台并行操作系统架构；网络处理能力大于6Gbps，并发连接≥200万，每秒新建连接8万/秒；  2. 设备至少满足8\*千兆电口，2\*千兆光口，2\*万兆光口；具备接口扩展插槽；具备冗余电源；  3. 应支持路由模式、交换模式、旁路模式接入，满足复杂应用环境的接入需求；  4. 支持对TTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀；本地病毒库规模大于2800+万；  5. 支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN等多种方式进行访问控制，并支持地理区域对象的导入以及重复策略的检查；  6. 支持基于不同安全区域攻击防御、病毒防护、内容过滤能力；并支持告警、丢弃、防护等多种防护措施；  7. 可在单条策略中启用病毒防护、入侵防御、网址过滤、文件过滤、文件内容过滤、终端过滤等安全功能策略；  8. 支持基于策略的路由负载，可以根据应用和服务进行智能选路，以源地址目的地址哈希、源地址哈希、轮询、时延负载、备份、随机、流量均衡、源地址轮询、目的地址哈希、最优链路带宽负载、最优链路带宽备份、跳数负载等不少于10种路由负载均衡方式； | 2 | 台 |
| 4 | 边界安全 | 安全管理区IPS | 1. IPS满减速率大于4Gbps，最大连接数大于180万，每秒新建连接数大于10万/秒；  2. 设备至少满足8\*千兆电口，2\*千兆光口，2\*万兆光口；具备接口扩展插槽；具备冗余电源；  3. 支持多种部署模式，支持路由、透明接入、虚拟网线等部署方案的工作模式；  4. 支持自定义应用协议，提供除五元组之外的应用技术、应用属性、风险级别、类型、子类、协议、匹配内容、应用层长度等多项设置；  5. 具备检测防逃逸技术，提供缓冲区溢出、SQL注入、扫描刺探、间谍软件、拒绝服务、病毒、木马后门、漏洞攻击、潜在风险的入侵防御特征库；  6. 支持在设备漏洞防护特征库直接查阅攻击的名称、CVEID、CNNVDID、CWEID、严重性、影响的平台、类型、描述、解决方案建议等详细信息；  7. 具备配置向导功能，通过引导用户配置，包括拓扑图、桥接口配置、地址区域流、IPS、可视、概览等多项元素实现快速配置上线；  8. 具备云端威胁情报功能，提供僵尸网络、钓鱼网站、恶意网站等10大类的威胁情报并把相关数据运用到产品防御策略中；  9. 支持多种病毒扫描模式，支持快速扫描和16层深度压缩文件的扫描模式，支持HTTP、FTP、IMAP、POP3、SMTP协议的病毒扫描能力； | 2 | 台 |
| 5 | 其他安全产品 | 综合日志审计 | 1. 自研安全专用操作系统，设备至少满足6\*千兆电口，具备接口扩展插槽；  2. 内存大于16G，磁盘大于4T，日志处理性能大于3000EPS；  3. 支持通过Syslog、SNMP Trap、Netflow V5、JDBC/ODBC、Agent日志代理(Windows/Linux) 、WMI、SFTP/FTP、文件共享(SMB、NetBIOS)、文件/目录读取、Kafka、WebService等多种方式完成各种日志的收集功能；  4. 支持点击事件任意属性字段，可以该字段为条件对事件进行统计分析，并展示Top 20排序，排序支持正序和倒序，并可对统计内容进行点击下钻；  5. 支持对资产IP地址的地理信息进行管理，设置单IP及IP段行政区及经纬度，支持地图显示；  6. 系统支持提供安全运维报告，帮助运维人员快速生成日常日志分析和运维报告；  7. 支持告警日志自动归并，有效抑制重复告警，归并规则可自定义；  8. 具备中国信息安全测评中心《信息技术产品安全测试证书》EAL3+； | 1 | 台 |
| 6 | 其他安全产品 | 网络管理运维综合平台 | 1.支持SNMP v1、v2c、v3协议管理设备；  2.支持手工增加设备，支持自动发现设备，自动发现设备任务可立即或周期性执行；  3.支持设备基本信息展示：设备标签、管理状态、IP地址等。  4.支持接口信息展示：展示接口状态、接口描述、接口别名等；  5.支持设备导入、导出、管理、取消管理、删除、修改基本信息等；  6.支持多厂商设备的管理；  7.支持接口收发速率、带宽利用率、丢包率等指标监控；  8.支持显示监控实时数据和历史监控数据  支持网络设备配置备份、查看、基线化、比较、导出等操作；  9.支持按照设备或区域周期性自动备份配置，并将备份报告发送至邮箱；  10.支持设备软件库，支持从本地或设备导入  11.支持网络拓扑的自动发现和动态更新，可发现设备及其链路关系；  12.支持网络拓扑信息的手工编辑：支持将设备加入不同的自定义视图管理，支持在拓扑上增加修改链路、支持将设备纳入不同的云图、分组进行呈现；  13.支持接收设备发送的告警；支持系统自动产生告警：  14.支持活动告警和历史告警查看；  15.支持告警的恢复、确认、删除和导出等操作；  16.支持大屏元素自定义设计，支持常见的图表、图片、文字、时间等组件；  **17.配置要求实配：**网络设备管理授权≥100个 | 1 | 台 |

注：

1）若投标产品属于工业和信息化部要求的实行进网许可制度的电信设备，则需提供投标产品获得工业和信息化部颁发的进网许可证

2）属于“中国强制性产品认证”（3C认证）范围的产品，则需提供投标产品符合性3C认证证书。

3）根据《财政部发展改革委生态环境部市场监管总局关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9 号） 以及财政部、发展改革委发布的《节能产品政府采购品目清单》，清单内的投标产品则需提供具有国家确定的认证机构出具并处于有效期之内的节能产品认证证书，

4）若投标产品属于《网络关键设备和网络安全专用产品目录》范围则投标产品需提供已按照相关国家标准的强制性要求，由具备资格的机构出具的安全认证合格证或者安全检测符合认证。

**5）上述4.2和4.3表格中的网络产品、网络安全产品、空调、UPS、监控产品等五类产品应当提供原厂质保承诺函（加盖原厂公章）。表格中标注▲参数为重要参数，需提供相应的第三方测试报告、适配证明、加盖原厂公章的产品官方技术资料白皮书或网页截图等证明文件。**

# 其他工作要求

## 售后服务要求

本项目从项目验收通过之日起3年内提供投标产品原厂7\*24小时免费技术支持和质保服务，3年后进入有偿维护期。

在质量保证期内，供应商将按照售后服务的承诺提供保修服务，如果厂商对项目中硬件设备和安全设备等产品中的部分保修期超过上述期限的，则按照厂商的规定进行有偿保修。

## 应急响应要求

供应商对网络系统、硬件设备、安全设备等故障应能够实时响应，若网络系统、硬件设备、安全设备等发生故障，接到通知后30分钟之内响应，专业工程师2小时内到达现场。特殊故障与客户沟通协商后，按照协商的方式制定解决方案并进行处理。

具体故障级别及对应的应急响应要求如下：

一级故障：在1小时内确诊，总故障解决时间不超过4小时。

二级故障：在2小时内确诊，并在4小时内由专家到达现场确诊并解决，总故障解决时间不超过8小时；

三、四级故障：在4小时内确诊故障，总故障解决时间不超过16小时。

## 培训要求

对采购单位和最终用户相关人员提供操作培训，应提供详细培训方案。

(1)在12个月的质量保证期内，提供2次与项目相关的必要培训。

(2)供应商需要开展分层次的人员培训工作，每次培训后应对参加培训人员进行测试，评估培训成果。培训应具有培训教材、培训环境和高水平的培训讲师。

(3)供应商应提供部门信息管理员的日常维护的培训，确保用户对象能够掌握对应的操作技能。

## 验收要求

本项目按下述方式开展验收。

（1）验收分初验和终验。

（2）初验前，供应商须完成硬件产品、安全产品的安装集成和调试等，并对本项目进行功能和运行检测，确保所有设备能够正常运行且已达到本项目约定的各类标准要求。供应商应以书面形式向招标方递交初验通知书。招标方应当在接到通知后的5个工作日内确定初验的具体日期，由双方按照本项目的约定完成本项目的初验。招标方有权委托第三方检测机构进行验收，对此供应商应当配合。

（3）初验时，供应商须提供文档包括《产品验收清单》、《机房改造竣工图》、《机房改造竣工文件》、《质量验收文件》等）。所交付的文档与文件应当是可供自然人阅读的书面和电子文档。软件文档及可安装的程序运行文件验收通过后，视为初验通过。如有缺陷，招标方应向供应商出具书面报告，陈述需要改进的缺陷。供应商应立即严格依照招标方的书面报告中的要求改进缺陷，并再次进行初验。

（4）自初验通过之日起，招标方享有供应商免费提供的30天的项目试运行现场驻场服务期。该期间内，供应商应当按照招标方的要求提供现场技术支持服务，解决网络系统和所有设备试运行期间可能出现的各类问题，或进一步提高与完善信息系统运行水平。

（5）初验通过且项目试运行期已经达到本项目约定的时间，经供应商确认网络系统和所有设备具备正常运行条件，且网络系统和所有设备通过运行测试，供应商应以书面形式通知招标方网络系统和所有设备已准备就绪等待终验。招标方在收到终验通知后的30个工作日内发起组织专家验收会。

（6）如果属于供应商原因致使本项目未能通过终验，供应商应当排除缺陷，直至本项目完全符合验收标准，由上述情形而产生的相关费用应由供应商自行承担。

（7）如果由于招标方原因导致本项目在终验通过前出现故障或问题，供应商应及时配合排除该方面的故障或问题。

（8）如本项目连续3次验收未通过（含初验未通过或终验未通过），招标方有权解除项目，并有权依照本项目约定的违约条款追究供应商的违约责任。

## 进度要求

投标人应根据建设内容，分阶段制定合理的时间进度，并且应根据招标方要求进行调整和细化。

总建设周期为6个月，分为4个阶段。

第一阶段为1个月，完成项目规划设计。

第二阶段为3个月，完成项目建设。

第三阶段为1个月，完成项目试运行。

第四阶段为1个月，完成项目验收。

## 项目团队及驻场人员要求

投标人须具有稳定的在职技术保障力量，能够提供及时的技术支援或服务，应针对本项目提供不少于10人的项目服务团队（包括项目经理、网络工程师、安全生产负责人、相关施工人员等），投标单位的相关服务人员需具备相应的服务能力，需提供相关证明。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **角色** | **主要职责** | **人员数量** | **人员要求** | **驻场要求** |
| 项目经理 | 负责项目质量和进度控制 | 1人 | 具备建筑施工二级建造师（机电专业）及以上资格证书，具有10 年（含）以上集成系统行业从业经历 | 不驻场 |
| 网络工程师 | 负责财政网络系统集成 | 1人 | 需要提供网络工程师资质证书具有5年（含）以上网络系统集成行业从业经历 | 不驻场 |
| 安全生产负责人 | 负责项目现场生产安全 | 1人 | 持有安全员C证 | 不驻场 |
| 相关施工人员 | 负责现场设备安装调试、网络系统集成测试等工作 | 7人 | 需要提供相关人员的特种作业证 | 不驻场 |

## 等级保护要求

本项目等级保护要求：参照等保三级要求建设。

## 商业密码应用需求

本项目为基础设施建设，无商业密码应用需求。

## 技术文件要求

投标人提供的书面技术资料应能确保系统正常运行所需的管理、运营及维护有关的全套文件。技术文件应该全面、完整、详细。投标人提供的技术文件至少应包括：

－ 技术手册(安装、测试、操作、维护、故障排除等)；

－ 项目文档，应该包括：

1. 机房改造设备清单及产品说明文件；
2. 机房改造施工组织设计；
3. 机房改造施工方案；
4. 机房改造质量验收文件；
5. 机房改造施工图及竣工图；
6. 机房改造竣工文件

提供全套技术文件纸介质3套以及电子文件1套。

# 供应商要求

供应商应当具有类似的政务信息系统建设经验，企业通过ISO9001质量管理体系认证、ISO27001信息安全管理体系认证、ISO20000 IT服务管理体系认证；具有建筑机电安装工程专业承包资质证书或电子与智能化工程专业承包二级及以上资质证书、省级公共安全防范工程设计施工单位核准证书。

# 供应商管理要求

1、在项目实施期间，中标人应严格执行国家、地方、行业有关本项目业务管理和安全作业的法律、法规和制度并按规定承担相应的费用。中标人因违反规定等原因造成的一切损失和责任由中标人自行承担。

2、中标人在投标书中承诺并经招标人认定的项目负责人及专业技术人员必须是本单位职工（在本单位缴纳社会保障金）和该项目实施现场的实际操作者，应具有类似本项目的实施经验，并应在软件应用调研、安装、试运行等期间常驻项目现场。未经采购人同意，中标人不得调换或撤离上述人员。如采购人认为有必要，可要求中标人对上述人员中的部分人员作出更好的调整。

3、中标人在项目实施期间，应按项目实际进度与环节落实所对应项目整体及各环节管理工作，按照规范做好项目实施期间相关管理与实施记录。

4、参与本项目的工作人员应严格遵循采购人的安全制度，保障采购人资料和设备的安全。中标方如需进入采购人机房工作，只能在采购人规定的工作区域内对项目涉及的设备进行操作，严禁触动与项目无关的任何设备（包括任何操作行为），如需跨区操作必须得到采购人项目联系人确认。

5、中标人在项目实施期间必须遵守采购人的规章制度并提供实施人员名单。

6、各投标人在投标文件中要结合本项目的特点和采购人上述的具体要求制定相应的管理措施，并在报价中列支相应的费用清单，投标人报价中未列支上述费用清单的，上述费用视为已包含在投标人的投标总报价中。

7、本项目软件开发及调试将纳入采购人的管理范围，中标人在此过程中须服从上述单位的管理协调。

# 知识产权及保密要求

**1、中标人数据、文件、资料知识产权**

中标人保证其所提供的服务和交付的成果以及在履行本项目义务中使用到的所有数据、文件、信息不会引起任何第三方在专利权、著作权、商标权等知识产权方面向采购人或采购人的关联方及合作方（包括但不限于采购人的主管单位和采购人的合作单位等）发出侵权指控或提出索赔。若有，中标人应负责与第三方解决纠纷，若因此导致采购人损失的，采购人有权要求中标人赔偿采购人因此遭受的全部损失，包括但不限于直接损失、间接损失、诉讼费／仲裁费、律师费、公证费、鉴定费等。

中标人因履行本项目而产生的所有成果的知识产权等权利均归采购人所有，中标人应配合采购人进行相关权利登记或申请。未经采购人书面同意，中标人不得以任何形式使用或许可他人使用本项目成果的相关内容，不得擅自对外公开发表或向任何第三方透露。

在不影响上述条款规定的由采购人取得所有成果的知识产权的前提下，双方因履行本项目而被授权接触或使用对方之知识产权（包括但不限于商标、专利、著作权等），和/或任何其他相关资料、数据等涉及的任何权利，均不视为向另一方转让上述权利或在本项目范围外授权许可另一方使用上述权利，上述权利仍应属于提供方，并仅可使用于本项目，被授权接触或使用方未经提供方书面同意，不得擅自挪作他用。

**2、项目保密要求**

中标人因履行本项目而知悉的所有数据、信息和资料（包括但不限于账号信息、图表、文字、计算过程、任何形式的文件、访谈记录、现场实测数据、采购人相关工作程序等）以及因履行本项目而形成的数据、信息和任何形式的工作成果，均是采购人要求保密的信息。未经采购人书面同意，中标人不得对外泄露采购人要求保密的信息，不得用于其他用途，否则中标人需承担由此引起的法律责任和经济责任，包括但不限于直接损失、间接损失、律师费、诉讼费/仲裁费、调查费、公证费等。

中标人应采取必要的有效措施保证其参与本项目的人员（包括中标人聘用的人员、借调的人员、实习的人员）无论是在职或离职后，以及中标人的合作方无论是合作中或合作终止后，都能够履行本项目约定的保密义务。若中标人人员或中标人合作方违反保密规定，中标人应承担连带责任。

中标人（含中标人参与本项目的人员以及其合作方）未经采购方书面许可，不得以任何形式自行使用或以任何方式向第三方披露、转让、授权、出售与本项目有关的技术成果、计算机软件、源代码、策划文档、技术诀窍、秘密信息、技术资料和其他文件。

以上内容的保密期限自中标人知悉保密信息起始至保密信息被合法公开之日止。

**3、临时账号等使用要求**

中标人对采购人提拱的临时使用账号要保密，不得公开，对组件开发的账号密码需进行加密，避免信息安全的泄露。未经采购人的同意不得利用采购人的网络及平台进行短信、彩信、微信发送,造成的一切后果由中标人负责。

# 项目的变更、解除和终止

如果中标人丧失履约能力、发生资不抵债或进入破产程序，采购人可在任何时候以书面形式通知中标人终止本项目的执行而不给予中标人补偿。该终止本项目将不损害或影响采购人已经采取或将要采取任何行动或补救措施的权利。

如遇国家、行业管理部门等机构的有关标准和规定调整的，导致本项目内容须做相应调整时，双方应按照公平、合理的原则共同协商修改本项目对应的合同的相关条款。

# 违约责任

1、如中标人未按约定的时间或服务标准完成建设工作，采购人可要求中标人在规定的时间内采取补救措施。中标人还应向采购人支付本项目费用总额30%的违约金，违约金不足以弥补采购人损失的，采购人有权要求中标人赔偿超过部分。

2、因中标人违反保密义务或知识产权约定的，采购人有权要求中标人支付本项目费用总额30%的违约金，违约金不足以弥补采购人损失的，采购人有权要求中标人赔偿超过部分。若中标人违反保密义务，采购人还有权立即单方解除合同而不承担任何违约责任。

3、中标人有其他违反本项目合同约定的行为，中标人应当支付本项目总价款金额的20%作为违约金，违约金不足以弥补采购人损失的，采购人有权要求中标人赔偿超过部分。

4、中标人有下列情形之一，采购人有权解除合同：

（1）因中标人服务质量问题导致采购人无法实现目的；

（2）擅自转让或者分包其应履行的义务的；

（3）违反或者未履行本项目合同约定的其他相关义务，且在采购人要求的合理时间内未能纠正的。