市机管局基础设施子系统

建设项目

采购需求

# 项目概况

随着市机管局“智慧机管局”业务大系统下的各应用子系统充分依托本市电子政务网络、电子政务云、大数据资源平台进行信息系统部署，市机管局办公人员通过政务外网和互联网实现对系统进行维护管理和办公，对局内部网络的健壮性和安全性以及终端用户的安全管控都提出了更高的要求。

2017年6月，《网络安全法》正式实施，其中第二十一条规定“国家实行网络安全等级保护制度”。2019年5月，国家标准化管理委员会正式发布了网络安全等级保护2.0核心技术标准。根据《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）的有关规定，市机管局政务外网需要按照等级保护2.0第三级要求进行安全建设。对网络资产进行区域划分，对不同的网络资产从通信网络防护、区域边界防护、计算环境防护等各方面进行不同级别的安全防护设计。

参照《上海市电子政务外网建设和运行管理指南》中网络安全设计规范的要求，政务外网各接入单位应在符合国家安全等级保护要求的前提下方能接入政务外网，并参照等保2.0的等级防护能力要求，匹配相应的网络安全防护措施。对于各单位网络接入到政务外网，应在政务外网边界设置安全接入区，需实现网络访问控制、入侵检测和防御、防病毒、APT检测、日志审计等功能。

需根据《信息安全技术网络安全等级保护基本要求》、《上海市电子政务外网建设和运行管理指南》对本单位信息系统进行升级改造。

建设期限：本项目于合同签订后6个月内完成

建设地点：黄浦区人民大道200号

预算金额：1,613,932元

采购金额（最高限价）：1,613,932元

组织形式：集中采购

采购方式：公开招标

是否接受联合体投标：否

是否按信创要求建设：是

运维后所属大系统：市机管局基础设施

# 建设目标

## 建设目标

考虑到上海市机关事务管理局信息系统即将面临的安全风险，本次项目进行机房及网络安全加固，建设完成后可具备以下能力：

1. 在统一的安全防护策略下具有抵御大规模、较强恶意攻击的能力，防范计算机病毒和恶意代码危害的能力；具有检测、发现、报警及记录入侵行为的能力；具有对终端用户进行集中管控的能力。
2. 实现对综合楼425机房的UPS、环境等设备进行集中联网监控；
3. 更换UPS主机以及机柜接入UPS设备，实现机房重要设备临时供电；
4. 参照网络安全等级保护2.0三级的标准进行建设。

**2.2、业务绩效考核目标**

本项目建成后业务绩效考核目标须满足以下指标：

业务绩效考核指标参数表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 一级指标 | 二级指标 | 三级指标 | 四级指标 | 指标值 |
| 1 | 通用指标 | 产出指标 | 产出数量 | 一次性验收合格率 | 100% |
| 2 | 产出指标 | 产出质量 | 安全事件发生次数 | 1次 |
| 3 | 产出指标 | 产出时效 | 项目建设周期 | 6个月 |
| 4 | 安全体系 | 安全建设水平 | 网络安全措施 | 达标 |

**2.3 技术绩效考核目标**

技术绩效考核指标参数表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 一级指标 | 二级指标 | 三级指标 | 四级指标 | 指标值 |
| 1 | 通用指标 | 产出指标 | 产出数量 | 硬件设备购置完成率 | 100% |
| 2 | 产出指标 | 产出质量 | 网络安全等级达标 | 完成等保三级备案 |
| 3 | 产出指标 | 产出质量 | 安全测试达标 | 达标 |
| 4 | 安全体系 | 安全建设水平 | 安全设备购置完成率 | 100% |
| 5 | 自定义指标 | (1)设备计划采购完成率100%，性能不低于系统软硬件配置清单中列出的配置参数；  (2)设备按时到货率100% | | | |

# 项目建设内容

本项目需采购网络安全设备、机房环控系统、机房监控系统和UPS系统所需的软硬件设备，并进行安装调试、集成测试等工作。

1. **网络安全设备**
2. 新增两台下一代防火墙设备；
3. 新增一台上网行为管理设备；
4. 新增运维管理区域：部署一台日志审计、一台堡垒机、一套安全感知平台、一套网管系统；
5. 新增核心交换机及接入交换机设备。
6. **机房环控系统**

新增机房环控系统，对市机管局局本部机房内的UPS、环境类等设备进行集中联网监控，并具备远程监控管理功能。

1. **机房监控系统**

对市机管局局本部机房监控系统升级改造，替换现有监控主机、监控摄像头，满足6个月视频存储需求。

1. **UPS系统**

对市机管局425机房UPS主机设备进行替换，新增接入3个机柜的PDU。

## 硬件购置清单

| **序号** | **名称** | **类别** | **产品配置** | **保修年限** | **数量** | **单位** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 机房建设 | 环境监控系统 | 网络型数据采集机： 8路光电隔离遥信接口输入 8路光电隔离继电器遥控输出，8路模拟信号遥测接口输入 1个100M全双工 以太口（物理接口：RJ-45插座） 4路RS485-422或RS232独立串口的协议以太转换接口（DB9，公 头） 1个4路DIP拨码开关 | 3 | 1 | 台 |
| 2 | 机房建设 | 环境监控系统 | 温湿度传感器： 额定电压 DC12V(10-24V AC/DC) 测量范围 温度：0℃～50℃  湿度：0～100%rh 测量精度 温度：±0.5℃ 湿度：±3%rh | 3 | 4 | 只 |
| 3 | 机房建设 | 环境监控系统 | 烟雾传感器： 电源：12～60V DC 工作电流：<10 mA 输出形式：缺省设置警戒状态输出开路 烟雾灵敏度：符合UL217号标准 | 3 | 4 | 只 |
| 4 | 机房建设 | 环境监控系统 | 水浸传感器： 供电电源：12-60V DC 灵敏度范围  档位1：0-250KΩ  档位2：0-600KΩ  档位3：0-5MΩ  档位4：0-50MΩ（高灵敏档，遇到极少水即可告警）  输出形式：干接点，水浸检出时输出ON/OFF可跳线选 | 3 | 1 | 只 |
| 5 | 机房建设 | 环境监控系统 | GSM网络型短信报警机： 通过以太网收发短信 内置4G模块 12V电源供电 支持UDP/TCP网络协议 支持Windows、Linux等流行操作系统 接口：10Base-T Ethernet RJ45网口 协议：UDP/TCP | 3 | 1 | 台 |
| 6 | 机房建设 | 环境监控系统 | 监控服务终端：网卡支持网络唤醒/PXE功能2\*WGI211AT千兆网卡芯片 操作系统Linux主板位 ITX(9.6\*9.6寸)、M-ATX  COM串口2\* DB9 RS232串口(1\*485) 显示接口 1\*VGA，1\*HDMI M.SATA 1\*MSATA插槽,支持SSD(默认)  网络接口 2\*RJ-45 动力环境模块：实现直观显示环境温湿度、漏水、UPS，通知报警事件，报警确认等，包括： 主页、当前告警、集中预警、分组显示、远程控制等功能项；  数据分析模块：对于所有采集参数做报警事件查询和统计，历史数据分类查询和统计，报表和打印管理，数据过滤统计，曲线比较分析，报警确认记录、报警日志记录等功能项；  监控管理模块、系统管理模块等 含物联网关软件：利用带智能监控接口的设备，比如UPS、精密空调上自带的RS485/232/网络通讯接口，读取电流表、电压表里的数据，或者设备的运行数据、实时显示并保存各监测参数的数值。实时设定修改电压、电流的上限值与下限值，当监测的电压或电流超过设定的允许值时，系统诊断为有故障（报警）事件发生，监控主系统发出报警。 | 3 | 1 | 套 |
| 7 | 机房建设 | 视频监控系统 | 高清摄像头： 400万像素半球网络摄像机 最大图像尺寸：2560\*1440 支持H.265/H.264 1个RJ45 10M/100M自适应以太网口 | 3 | 5 | 只 |
| 8 | 机房建设 | 视频监控系统 | 硬盘录像机： 存储接口：8个SATA接口 视频接口：1×HDMI，1×VGA 网络接口：2×RJ45 10/100/1000Mbps自适应以太网口 接入能力：8路H.264、H.265格式高清码流接入 显示能力：最大支持4K输出 | 3 | 1 | 台 |
| 9 | 机房建设 | 视频监控系统 | 监控硬盘： 6T，SATA硬盘 | 1 | 8 | 块 |
| 10 | 机房建设 | 视频监控系统 | POE交换机： 提供8个千兆PoE电口、2个千兆光口 | 3 | 1 | 台 |
| 11 | 机房建设 | 视频监控系统 | 视频监控系统 辅材： 网线、水晶头等辅材 | 3 | 1 | 项 |
| 12 | 动力设备 | UPS | UPS主机： 支持20kw | 3 | 1 | 台 |
| 13 | 动力设备 | UPS | 机柜配套PDU及线材：包含8位10A及10位16A PDU、3\*2.5PDU线材等 | 3 | 1 | 项 |

## 安全产品购置清单

| **序号** | **名称** | **类别** | **产品配置** | **保修年限** | **数量** | **单位** | **关键设备详细技术参数** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 边界安全 | 防火墙 | 性能参数：网络层吞吐量：39Gbps，应用层吞吐量：9Gbps，并发连接数：4000万，新建连接数（CPS）：23万。 尺寸：2U，内存16G，128GB SSD，冗余电源，6千兆电口+4千兆光口SFP+4万兆光口SFP+。 三年硬件质保。三年防火墙的入侵防御、防病毒规则库更新、软件升级，原厂上门服务。 | 3 | 2 | 台 | 详见4.1 |
| 2 | 主机及计算机环境安全 | 上网行为管理产品 | 性能参数：网络层吞吐量（大包）：5.8Gb，应用层吞吐量：750Mb，带宽性能：500Mb， 内存8G，1T SATA，单电源，6千兆电口+4千兆光口SFP。含三年上网行为管理的应用识别库更新、软件升级，原厂上门服务，三年硬件质保服务。 | 3 | 1 | 台 | 详见4.2 |
| 3 | 安全管理与支持 | 堡垒机 | 包含50点授权 尺寸：1U，内存16G，硬盘：64GB SSD+1TB SATA，单电源，6千兆电口+4千兆光口SFP。 三年硬件质保服务 | 3 | 1 | 台 | 详见4.3 |
| 4 | 安全管理与支持 | 日志审计 | 性能参数：包含主机审计许可证书数量：100，可用存储量：4TB（RAID0 模式） 内存16G，硬盘容量：128G SSD+4T SATA，电源：冗余电源，接口：6千兆电口+2万兆光口SFP+。 含：三年软硬件质保服务。 | 3 | 1 | 台 | 详见4.4 |
| 5 | 其他安全产品 | APT | 性能参数：网络层吞吐量：500Mbps。  内存16G，硬盘：128G MSATA+4T SATA，单电源，接口：6千兆电口+2万兆光口SFP+。 三年APT威胁检测系统特征库升级，三年软硬件质保服务。 | 3 | 1 | 台 | 详见4.5 |
| 6 | 其他安全产品 | 核心交换机 | 核心交换机： 交换容量：76.8/336Tbps，48个电口，4个万兆集群端口\*2，24个万兆光口+24个千兆光口，双电源，含SFP+-10G-高速电缆-3m，2个万兆多摸光模块，2个万兆单模光模块，硬件质保三年 | 3 | 2 | 台 | 详见4.6 |
| 7 | 其他安全产品 | 接入交换机 | 接入交换机： 48个电口,4个万兆光口，含SFP+-10G-高速电缆-3m，1个万兆多模光模块/硬件质保三年 | 3 | 10 | 台 | 详见4.7 |
| 8 | 安全管理与支持 | 网管系统 | 硬件配置：V2.7G主频 四核心 四线程，内存 32G，系统盘 固态128G 机械盘1T。  基本功能：提供系统基本平台处理和展现功能，包括用户管理、网络拓扑管理、综合监控,故障告警管理(包含告警规则设置、实时告警查看、告警日志分析、多种告警通知方式）监控范围：包括对各类网络设备、安全设备实现监控管理的授权；支持50个授权点，质保三年 | 3 | 1 | 套 | 详见4.8 |

# 关键设备详细技术参数要求

## 防火墙

| 功能项 | 功能要求说明 |
| --- | --- |
| 硬件要求 | 产品不少于6个千兆电口，4个千兆光口，4个万兆光口；内存≥16G，硬盘容量≥128GB，冗余电源。 |
| 硬件平台 | 产品应用多核并行处理架构，并采用国产处理器和国产操作系统。 |
| 链路状态探测 | 产品支持链路健康检查功能，支持基于多种协议对链路可用性进行探测，探测协议至少包括DNS解析、ARP探测和PING方式。 |
| 路由功能 | 产品支持静态路由、策略路由和多播路由协议，并支持BGP、RIP、OSPF等动态路由协议。 |
| 地址转换 | 产品支持多种地址转换功能，支持源地址转换SNAT，目的地址转换DNAT和双向地址转换双向NAT，支持IPv4／IPv6下地址转换。 |
| 访问控制策略 | 产品支持多维度安全策略设置，可基于时间、用户、应用、IP、域名等内容进行安全策略设置。 |
|  | 产品具备至少对ARP Flood、ICMP Flood、SYN Flood、DNS Flood、UDP Flood等泛洪类攻击防护的能力，并支持IP地址扫描和端口扫描攻击防护。 |
| 产品支持对SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP等协议进行病毒防御。 |
| 产品支持对多重压缩文件的病毒检测能力。 |
| 产品具备入侵防御检测引擎，支持对各类漏洞利用攻击进行检测与防护。 |
| ▲1产品支持僵尸网络检测功能，防止失陷主机威胁内网扩散，需提供相关证明。 |
| 产品具备Web应用攻击检测引擎，支持文件包含攻击、抵御注入式攻击（包含SQL注入、系统命令注入）、信息泄露攻击、跨站脚本（XSS）、网站扫描、WEBSHELL后门攻击、跨站请求伪造、目录遍历攻击、WEB整站系统漏洞等应用层攻击行为。 |
| ▲2具备识别与阻断外部扫描器发起的服务器恶意扫描行为，可对扫描器地址进行自定义封堵，需提相关证明。 |
| 产品支持对HTTP异常请求协议检测和防护攻击，检测内容包含HTTP请求信息的方法及参数长度等。 |
| 安全策略管理 | 产品支持在安全策略中可同时启用入侵防御、防病毒、URL过滤、文件过滤、Web应用防护等安全功能，简化安全策略部署。 |
| ▲3产品支持应用控制策略生命周期管理，包含安全策略的变更时间、变更类型和策略变更用户，并对变更内容记录日志，方便安全策略管控，需提供相关证明。 |
| 用户管理 | 产品支持三权分立功能，根据用户权限可设置为安全管理员、审计员和系统管理员三种角色。 |

## 上网行为管理

| 功能项 | 功能要求说明 |
| --- | --- |
| 硬件和性能参数 | 不少于6个千兆电口，4个千兆光口，内存≥8G，硬盘容量≥1T SATA |
| 国产化 | 产品采用国产处理器和国产操作系统。 |
| 系统管理 | 支持攻击、双机切换告警、移动终端管理告警、web关键字过滤告警、杀毒告警、设备流量超限告警、磁盘/CPU/内存异常告警等； |
| 实时监控 | ▲4支持首页分析显示接入用户人数、终端类型、认证方式；带宽质量分析、实时流量排名；（需提供产品功能截图证明） |
| 实时显示设置过滤条件的用户上网行为监控，支持手动设置刷新时间； |
| 实时提供用户流量排名、应用流量排名、连接监控信息； |
| 审计策略 | 支持对网页过滤和网页审计分开控制； |
| 支持审计指定类型的URL，其他URL类型不予审计，以提高审计效率； |
| 支持免除审计指定IP、指定域名的上网行为； |
| 安全审计 | 支持记录全部或者指定类别URL、网页标题等信息；审计记录网页正文内容； |
| 支持网页内容审计后的网页快照功能； |
| 支持审计Webmail邮件外发行为，支持webmail形式发送的附件审计，并能精准到原始邮件； |
| 支持记录用户在指定时间段内使用指定应用的总时长，并统计在指定时间段内网络应用产生的总流量 |
| 支持审计通过FTP上传的文件名和内容以及支持通过FTP下载的文件名； |
| 日志管理 | ▲5支持日志高性能模式处理，精简冗余日志；（需提供产品功能截图证明） |
| 支持查询和导出基于指定时间段/用户/用户组的防共享接入日志、移动终端发现日志、准入日志、登录注销日志等行为日志； |
| 支持基于时间段/用户/用户组的热门应用类型或热门具体应用的行为次数排行 |
| 日志中心所有导出都有对应管理员操作日志、系统日志的日志清理中记录数据删除日志、规则库升级有对应升级日志； |
| 流量管理 | 支持在设置流量策略后，根据整体线路或者某流量通道内的空闲情况，自动启用和停止使用流量控制策略，以提升带宽的高使用率；空闲值可自定义； |
| ▲6支持通过抑制P2P的下行丢包，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；（需提供产品功能截图证明） |

## 堡垒机

| 功能项 | 功能要求说明 |
| --- | --- |
| 硬件要求 | 不少于6个千兆电口，4个千兆光口，内存≥16G，硬盘容量≥64GB SSD+1TB SATA。 |
| 性能要求 | 资产授权≥50 |
| 国产化 | 产品采用国产化芯片和操作系统。 |
| 支持协议 | 字符协议：SSHv1、SSHv2、TELNET；图形协议：RDP、VNC；文件传输协议：FTP、SFTP、RDP磁盘映射、RDP剪切板 |
| 支持通过协议前置机进行协议扩展，至少支持扩展KVM、Vmware、数据库、http/https、CS应用等 |
| 动作流 | ▲7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，通过动作流配置都可以实现单点登陆和审计接入（提供截图） |
| 用户管理 | 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 |
| 内置三员角色的同时支持角色灵活自定义，可根据用户实际的管理特性或特殊的安全管理组织架构，划分管理角色的管理范畴 |
| 运维授权 | 支持一对一、一对多、多对多授权，如将单个资产授权多个用户，一个用户授予多个资产，用户组向资产组授权 |
| 支持在授权基础上自定义访问审批流程，可设置一级或多级审批人，每级审批可指定通过投票数，需逐级审批通过才可最终发起运维操作 |
| 访问控制 | 支持命令黑命单，对字符型设备（如linux/unix/网络设备）的高危命令执行进行阻断，如rm、shutdown、reboot等 |
| 运维方式 | ▲8支持web页面直接发起运维，无需安装任何控件，并同时支持调用SecureCRT、Xshell、Putty、WinSCP、FileZilla、RDP等客户端工具实现单点登陆（提供功能截图） |
| 审计日志 | 支持监控正在运维的会话，信息包括运维用户、运维客户端地址、资源地址、协议、开始时间等，并可以实时阻断 |
| 支持对常见设备运维操作进行记录（至少包括linux/unix主机、网络设备等），审计信息至少包括以下内容：用户账户、起止时间、登陆IP、设备IP、设备名称、设备类型、访问账号、访问协议等信息 |
| 支持标准SNMP v1、v2、v3管理协议，支持syslog等标准日志格式外发 |
| 客户端兼容 | ▲9全面支持Windows、linux、国产麒麟系统、Android、IOS等客户端操作系统下的H5页面一站式运维，实现跨终端适应性BYOD（Bring Your Own Device）（提供功能截图） |

## 日志审计

| 功能项 | 功能要求说明 |
| --- | --- |
| 硬件要求 | 不少于6个千兆电口，2个万兆光口，内存≥16G，硬盘容量≥128G SSD+4TB SATA，冗余电源。 |
| 性能要求 | 可用存储量≥4TB |
| 国产化 | 产品采用国产化芯片和操作系统。 |
| 日志采集 | 支持主动、被动相结合的数据采集方式，支持通过Agent采集日志数据，支持通过syslog、SNMP Trap、JDBC、WMI、webservice、FTP、文件\文件夹读取、Kafka等多种方式完成日志收集； |
| ▲10支持接入TLS加密方式的日志，支持对日志传输状态、最近同步时间进行监控，可统计每个日志源的今日传输量和传输总量。（需提供截图证明） |
| 日志标准化 | 支持通过正则、分隔符、json、xml的可视方式进行自定义规则解析，支持对解析结果字段的新增、合并、映射。 |
| 日志过滤 | 支持对每个日志源设置过滤条件规则，自动过滤无用日志，满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数，减少对网络带宽和数据库存储空间的占用。 |
| 日志转发 | 支持对单个/多个日志源批量转发，支持定时转发，可通过syslog和kafka方式转发到第三方平台，并且支持转发原始日志和已解析日志的两种日志。 |
| 日志存储 | ▲11支持日志文件备份到外置存储节点，支持ISCSI存储方式，并可查看外置存储容量、状态等信息。支持以FTP方式将日志数据备份至外部存储空间，支持备份数据的恢复和查询；（需提供截图证明） |
| 全文检索 | ▲12支持通配符、范围搜索、字段等多种输入方式、搜索框模糊搜索、指定语段进行语法搜索；可根据时间、严重等级等进行组合查询；可根据具体设备、来源/目的所属（可具体到外网、内网资产等）、IP地址、特征ID、URL进行具体条件搜索；支持可设置定时刷新频率，根据刷新时间显示实时接入日志事件；（需提供截图证明） |
| 支持解码小工具，按照不同的解码方式解码成不同的目标内容，编码格式包括base64、Unicode、GBK、HEX、UTF-8等； |
| 日志分析 | 支持自定义审计规则与关联规则，支持网站攻击、漏洞利用、C&C通信、暴力破解、拒绝服务、主机脆弱性、主机异常、恶意软件、账号异常、权限异常、侦查探测等内置关联分析规则，内置关联分析规则数量达到350条以上。 |
| 日志告警 | 支持告警事件归并、告警确认和告警归档，支持基于频率、频次、时间的设定条件。 |
| 系统管理 | 提供管理员账号创建、修改、删除，并可针对创建的管理员进行权限设置；支持IP免登录，指定IP免认证直接进入平台；支持只允许某些IP登录平台；支持页面权限配置和资产范围配置，用于管理账号权限，满足用户三权分立的需求；支持usb-key认证。 |

## APT

| **功能项** | **功能要求说明** |
| --- | --- |
| 硬件性能参数 | 不少于6个千兆电口，不少于2个万兆光口；内存≥16G，硬盘容量≥4T |
| 安全分析大屏 | ▲13支持安全态势的可视化呈现，以大屏的方式从全网安全态势感知大屏、安全事件态势、资产监控大屏、脆弱性态势、全球网络攻击态势、外联风险监控大屏、横向威胁态势等提供不少于7块大屏展示界面（需提供产品功能截图证明） |
| 资产中心 | 支持主机类资产识别，能够识别资产数据来源、IP地址、主机名、MAC地址、操作系统、操作系统详请、主机类型、服务与端口、状态、责任人、EDR状态、标签、最近上线时间、所属资产组、资产名称、应用、IP类型、识别方式、首次发现时间等。 |
| ▲14支持自定义资产多级分支管理，最多可至15级分支。支持责任人管理功能，可对资产进行全生命周期管理，包括自动识别资产、入库审核、离线资产识别、数据更新、主机资产退库、自定义资产名称等（需提供产品功能截图证明） |
| 告警中心 | 支持待处置安全事件描述、事件标签、攻击阶段、事件分类、失陷确定性、威胁等级、风险主机统计、发生时间、处理状态以及自定义待处置事件；支持攻击阶段分布和事件类型分布，热点事件统计。 |
| 支持将发生的所有安全事件默认按照处置状态，威胁等级，确定性等级，时间这四个字段排序，并结合事件类型、攻击结果、攻击阶段、处置状态、事件统计和事件趋势等进行统计和过滤显示、可设置关注的安全事件，可实时监控发生的安全事件，能复制攻击IP、XFF代理，并能够基于HTTP状态码进行事件筛选。 |
| 分析中心 | 支持安全检测日志，日志类型包括脆弱性风险、访问风险、服务探测、主机探测、网站攻击、后门通信、暴力破解、攻击利用、邮件攻击、DOS攻击、黑链、漏洞攻击、黑客工具、数据库攻击利用、访问恶意文件、感染病毒、主机异常、网络行为异常、流量异常、登录异常等 |
| 支持勒索专项检测页面，对勒索主题的安全告警进行展示和管理，支持以勒索病毒的感染途径/方式为维度进行分类，包括勒索常用端口、勒索常用漏洞、RDP爆破、感染勒索病毒、黑客勒索攻击、勒索C&C通信等维度，支持展示受害资产以及受害资产攻击数Top5，支持以列表的形式展示勒索事件，包括最近发生时间、威胁描述、勒索风险、攻击阶段、威胁等级、受害者IP、受害者资产类型、攻击者IP、攻击次数、处置状态等 |
| ▲15支持挖矿专项检测页面，支持基于规则的本地挖矿检测和基于主动探测技术的云端挖矿检测，支持挖矿实时检测播报本地和云端的挖矿检测分析结果，支持基于攻击阶段展示挖矿主机数量，支持以列表的形式展示挖矿事件，包括最近发生时间、威胁描述、挖矿阶段、攻击阶段、威胁等级、受害者IP、受害者资产类型、攻击者IP、攻击次数、威胁情报、处置状态等（需提供产品功能截图证明） |
| 支持对威胁情报的安全告警做专项性分析，比如通过情报匹配的风险主机分布、威胁趋势分析，将发生的所有安全事件默认按照处置状态，威胁等级，确定性等级，攻击结果、事件类型等维度进行筛选展示，并结合攻击阶段、事件统计和事件趋势等进行统计和显示、可实时监控发生的安全事件。 |
| 支持文件威胁分析，可展示文件分析过程、文件检测趋势、恶意文件TOP5；支持恶意文件的详情分析，包括支持记录恶意文件感染的主机、所属IP、文件名、病毒名称、传输协议等；支持导出文件威胁分析结果。 |
| 溯源中心 | 支持安全检测日志、审计日志存储；日志类型包括漏洞利用攻击、网站攻击、僵尸网络、业务弱点、DOS攻击、邮件安全、文件安全、网络流量、DNS、HTTP、POP3、SMTP、IMAP等。 |
| 日志检索：可根据时间、攻击类型、严重等级等选择项进行组合查询；根据具体设备、来源/目的所属（可具体到外网、内网资产等）、IP地址、特征ID、URL进行具体条件搜索。 |
| 报表中心 | 支持展示需要处理的风险主机与风险状况报告，报告内容包括业务与终端风险、业务风险与终端详情分析，提供危害解释和参考解决方案；适用于日常处理安全问题的运维人员。 |

## 核心交换机

| **功能项** | **功能要求说明** |
| --- | --- |
| 硬件参数 | 48个电口，4个万兆集群端口\*2，24个万兆光口+24个千兆光口，双电源，含SFP+-10G-高速电缆-3m，2个万兆多摸光模块，2个万兆单模光模块 |
| 交换容量 | 76.8/336Tbps |
| VLAN | 支持 4K 个 VLAN  支持 Access、Trunk、Hybrid 方式，支持 LNP 链路类型自协商  支持 VLAN 交换 |
| ARP | 支持 ARP Snooping |
| 环网保护技术 | 支持 STP（IEEE 802.1d），RSTP（IEEE 802.1w）和 MSTP（IEEE 802.1s）  支持 BPDU 保护、Root 保护、环路保护 |
| IP路由 | 支持 RIP、OSPF、ISIS、BGP 等 IPv4 动态路由协议  支持 RIPng、OSPFv3、ISISv6、BGP4+等 IPv6 动态路由协议 |
| 可靠性 | 支持 LACP、支持跨设备 E-Trunk  支持 VRRP、BFD for VRRP  支持 BFD for BGP/IS-IS/OSPF/静态路由 |
| 安全和管理 | 802.1x 认证，Portal 认证  支持防范 DoS 攻击、TCP 的 SYN Flood 攻击、UDP Flood 攻击、广播风暴攻击、大流量攻击 |
| 质保 | 硬件质保三年 |

## 接入交换机

| **功能项** | **功能要求说明** |
| --- | --- |
| 硬件参数 | 48个电口,4个万兆光口，含SFP+-10G-高速电缆-3m，1个万兆多模光模块 |
| VLAN 特性 | 支持 4K VLAN  支持基于 MAC/协议/IP 子网/策略/端口的 VLAN |
| IP路由 | 静态路由、RIPv1/2、RIPng、OSPF、OSPFv3、ECMP、ISIS、ISISv6、BGP、BGP4+、VRRP、VRRP6 |
| IPv6特性 | 支持 IPv6 Ping、IPv6 Tracert、IPv6 Telnet  支持 6to4、ISATAP、手动配置 tunnel |
| 安全特性 | 用户分级管理和口令保护  支持防止 DOS、ARP 攻击功能、ICMP 防攻击  支持 IP、MAC、端口、VLAN 的组合绑定  支持端口隔离、端口安全、Sticky MAC  支持 AAA 认证，支持 Radius、HWTACACS、NAC 等多种方式  支持 SSH V2.0  支持 HTTPS  支持 DHCPv4/v6 Client/Relay/Server/Snooping |
| 质保 | 硬件质保三年 |

## 网管系统

硬件配置：V2.7G主频 四核心 四线程，内存 32G，系统盘 固态128G 机械盘1T。

基本功能：提供系统基本平台处理和展现功能，包括用户管理、网络拓扑管理、综合监控,故障告警管理(包含告警规则设置、实时告警查看、告警日志分析、多种告警通知方式）监控范围：包括对各类网络设备、安全设备实现监控管理的授权；支持50个授权点，质保三年。

# 其他工作要求

## 售后服务要求

本项目软硬件设备到货验收通过后，提供三年的质保服务；从系统验收通过之日起3年内提供7\*24小时免费技术支持和售后服务。

在质量保证期内，供应商将按照售后服务的承诺提供保修和运行维护服务，如果厂商对信息系统中的软硬件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免费保修。

在质量保证期内，对本次招标需求范围内的设备提供季度巡检服务。

在质量保证期内，供应商负责信息系统的运行维护工作，确保信息系统安全、稳定、可靠地运行。本项目涉及的运行维护工作范围为：本次招标的需求范围。

## 应急响应要求

供应商对系统故障应能够实时响应，若系统发生故障，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

对系统使用单位提供业务操作培训，应提供详细培训方案。

(1) 在项目验收前，提供1次与项目相关的必要培训；在12个月的质量保证期内，提供1次与项目相关的必要培训。

(2)培训应具有培训教材、培训环境和高水平的培训讲师。

(3)供应商应提供一般用户的基础操作培训和部门信息管理员的日常应用维护的培训，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，供应商须完成软硬件安装和信息系统的调试等，并对本项目进行软硬件设备进行检测，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申请，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《设备到货验收单》、《测试报告》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。包括文档验收通过后，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天的信息系统试运行服务期。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，解决信息系统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）初验通过且信息系统试运行期已经达到本项目约定的时间，经供应商确认信息系统具备正常运行条件，且信息系统通过运行测试，供应商应以书面形式通知招标方信息系统已准备就绪等待终验。招标方在收到终验通知后的10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。本项目于合同签订后6个月内，完成项目建设和验收工作。

## 供应商综合能力要求

供应商具有ISO20000信息技术服务管理体系认证证书、ISO27001信息安全管理体系认证证书、ITSS信息技术服务运行维护标准符合性证书的优先考虑。

## 项目团队人员要求

1）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4人的项目服务团队（包括项目负责人、技术工程师、资料员），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** |
| --- | --- | --- | --- | --- |
| 项目负责人 | 负责项目总体质量和进度控制 | 1人 | 具有本科及以上学历；具有信息系统项目管理师（高级）证书；具备政务行业工作经验。10年及以上类似项目的实施经验。 | 不驻场 |
| 技术工程师 | 负责现场软硬件设备实施 | 2人 | 具有专科及以上学历；  具有网络工程师或信息安全专业人员（CISP）；具备政务行业工作经验。 | 不驻场 |
| 资料员 | 负责资料的编写 | 1人 | 具有专科及以上学历；  具备政务行业工作经验。 | 不驻场 |

2）投标人应针对本项目提供不少于2人的质保期间支撑团队（其中运维经理1人，维护工程师1人）；投标人的相关服务人员需具备相应的服务能力，需提供相关证明（最近一个季度依法缴纳社保费的证明）。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **角色** | **主要职责** | **人员数量** | **人员要求** | **驻场要求** |
| 运维经理 | 负责质保期间项目质量和运维进度控制 | 1人 | 具有本科及以上学历；  具有项目管理资质证书 | 不驻场 |
| 维护工程师 | 负责项目运行维护 | 1人 | 具有大专及以上学历；  熟悉软硬件基本维护 | 不驻场 |

## 等级保护要求

本项目等级保护要求：

拟按照信息系统安全等级保护2.0三级进行建设。

## 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：

－系统说明文件；

－技术手册(安装、测试、操作、维护等)；

－项目文档，应该包括：

(1)深化设计图

(2)项目过程文档

(3)设备移交清单

提供全套技术文件纸介质3套以及电子文件1套。

# 供应商资质要求

1、符合《中华人民共和国政府采购法》第二十二条规定的供应商。

2、根据《上海市政府采购供应商登记及诚信管理办法》已登记入库的供应商。

3、其他资格要求：

3.1本项目面向大、中、小、微型等各类供应商采购。

3.2未被列入“信用中国”网站(www.creditchina.gov.cn)失信被执行人名单、重大税收违法案件当事人名单和中国政府采购网(www.ccgp.gov.cn)政府采购严重违法失信行为记录名单。

# 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。

# 关于转让和分包的规定

本项目不得转让、不得分包。

# 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。

# 付款方式

本项目拟采用二期分期付款方式付款

a.合同签订生效且收到发票后10个工作日内，支付合同总价款的 70 %；

b.本项目通过最终验收且收到发票后10个工作日内，支付合同总价款的尾款。

付款条件备注：服务提供方应当在采购方每次付款前提前至少10个工作日向采购方提供有效发票。