# 上海博物馆文物保护科技中心信息系统项目（2025年升级改造）采购需求

# 项目概况

随着上海博物馆文物数量的不断增加和种类的日益丰富，传统的文物保护方法已经难以满足需求。通过网络升级改造，可以实现文物信息的数字化采集、存储、管理和利用，提高文物保护的效率和水平。同时，网络升级改造还可以加强文物安全监控和预警能力，通过系统手段及时发现和处理安全隐患，确保文物的安全。

上海博物馆文物保护科技中心现有的网络系统已经运行长达九年之久，部分设备老化、性能下降，无法满足日益增长的文物保护需求。同时，网络安全问题也日益突出，存在被黑客攻击、数据泄露等风险。因此，需要对现有网络系统进行全面升级改造，提升网络性能、安全性和稳定性。

为落实相关法律法规对于信息系统密码应用的要求，结合《国家政务信息化项目建设管理办法》《政务信息系统政府采购管理暂行办法》等规范性依据，我单位决定对已运行的电子公文处理系统进行密码应用改造。

通过对该系统的现状和密码应用需求分析，依据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》（以下简称《密码应用基本要求》）、GB/T 43207-2023《信息安全技术 信息系统密码应用设计指南》（以下简称《密码应用设计指南》），从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、密钥管理、安全管理等层面，设计了该系统密码应用的技术方案、安全管理方案和实施保障方案。

为落实国务院《关于进一步加强文物工作的指导意见》(国发2016-17 号)和《关于积极推进“互联网+”行动的指导意见》(国发2017-40 号)，把互联网的创新成果与中华传统文化的传承、创新与发展深度融合，深入挖掘和拓展文物蕴含的历史、艺术、科学价值和时代精神，彰显中华文明的独特魅力，丰富文化供给，促进文化消费，五部委特制定“互联网+中华文明”三年行动计划。

现有应用系统如下：

|  |  |  |
| --- | --- | --- |
| 序号 | 系统名称 | 主要功能 |
| 1 | 上海博物馆文物保护科技中心信息系统（以下简称本系统） | 主要是为了满足上海博物馆文物保护中心业务的需要，包含：文物修复系统、检测检验管理系统、科研项目管理系统、古代工艺管理系统、学术活动管理系统。 |

本系统部署在我单位机房中，系统网络划分为网络接入区、核心交换区、终端接入区、数据中心、安全管理区等五个区。

现有设备清单如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **产品名称** | **数量** | **单位** |
| 1 | 千兆三层核心交换机 | 2 | 台 |
| 2 | 千兆以太网交换机 | 4 | 台 |
| 3 | 千兆以太网交换机 | 8 | 台 |
| 4 | POE交换机 | 6 | 台 |
| 5 | 企业级路由器 | 1 | 台 |
| 6 | 安全审计系统 | 1 | 台 |
| 7 | VPN | 1 | 台 |
| 8 | 应用服务器（机架式） | 1 | 台 |
| 9 | 光纤交换机 | 4 | 台 |
| 10 | 网闸 | 1 | 台 |
| 11 | 刀片机箱 | 1 | 套 |
| 12 | 刀片服务器 | 1 | 台 |
| 13 | 机架式服务器 | 1 | 台 |
| 14 | 外网防火墙 | 1 | 台 |
| 15 | 上网控制网关 | 1 | 台 |
| 16 | 内网刀片机箱 | 1 | 套 |
| 17 | 内网刀片服务器 | 1 | 台 |

改造后清单及所需内容如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **产品名称** | **数量** | **单位** |
| 1 | 统一身份认证 | 1 | 台 |
| 2 | 安全管理平台产品 | 1 | 台 |
| 3 | 统一身份认证 | 1 | 台 |
| 4 | 防毒墙 | 1 | 套 |
| 5 | 防火墙 | 2 | 台 |
| 6 | 上网行为管理产品 | 1 | 台 |
| 7 | 入侵检测系统（IDS） | 1 | 台 |
| 8 | 路由器 | 1 | 台 |
| 9 | 交换机 | 7 | 台 |
| 10 | 交换机 | 2 | 台 |
| 11 | 光模块 | 44 | 台 |
| 12 | 交换机 | 13 | 台 |
| 13 | 其他安全产品 | 1 | 台 |
| 14 | 其他安全产品 | 1 | 套 |
| 15 | 其他安全产品 | 1 | 台 |
| 16 | 其他安全产品 | 10 | 套 |
| 17 | 其他安全产品 | 1 | 套 |
| 18 | 密码应用功能模块 | 2 | 人/月 |

是否按信`创要求建设：是

# 建设目标

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，本次网络安全等级保护建设完成后，系统应当具备如下安全保护能力：

应能够防护免受来自外部小型组织的、拥有少量资源的威胁源发起的恶意攻击、一般的自然灾难、以及其他相当危害程度的威胁所造成的重要资源损害，能够发现重要的安全漏洞和处置安全事件，在自身遭到损害后，能够在一段时间内恢复部分功能。

为满足上述安全保护能力，将通过系统性、体系化的需求分析、方案设计和风险控制等方式，达到以下4个方面的建设目标：

* 完善网络安全防护技术措施，通过“一个中心、三重防护”的安全设计，形成网络安全综合技术防护体系，满足第二级系统网络安全等级保护相关技术要求；
* 建立、健全网络安全管理制度、机构和人员要求，提升网络安全管理能力，满足第二级系统网络安全等级保护相关管理要求；
* 通过体系化的网络安全建设，满足第二级系统等级保护合法、合规要求，有效维护社会秩序、公共利益以及公民、法人和其他组织的合法权益。
* 综合考虑本系统在物理和环境、网络和通信、设备和计算、应用和数据等层面的密码应用需求，充分利用已有密码资源，设计合规、正确、有效的密码应用技术方案，以达到《密码应用基本要求》中二级指标要求，并为后续密码保障体系建设、密码应用测评和密码应用安全性评估奠定坚实基础。
* 项目效益：

1) 提高网络性能：通过更新网络设备，提高了网络带宽和传输速度，为博物馆的各项业务提供了更加高效的网络支持。

2) 加强安全防护：通过升级安全设备，构建了多层次的安全防护体系，有效保障了文物数据、管理信息的安全性和完整性。

3) 节约成本：通过充分利旧和选择性价比高的设备，我们实现了节约建设成本的目标。

# 项目建设内容

本次项目建设为网络及安全设备的升级改造，不涉及新业务的建设开发。不涉及软件系统的用户角色分配问题。不涉及服务器及存储的需求。不涉及新的业务系统开发建设。本项目涉及商密等要求，因此会涉及到已有系统的改造。

上海博物馆文物保护中心作为目前国内规模最大的文物保护科技中心，是我国文物保护科研的重要组成部分，应按照网络安全等级保护制度和行业法规标准的要求，开展网络安全等级保护建设工作，以建立、健全单位网络安全防护体系，提升系统整体网络安全防护能力，本项目将按照《信息安全等级保护管理办法》的规定，设定信息系统的安全保护等级为：二级。

本系统的安全性有较高的要求，系统的设计必须严格保障系统的安全性能，包括对整个系统管理、设备、软件、网络等全方位的体现。

由于在网络环境下，任何用户都有可能对任何资源包括硬件和软件资源的共享，所以必须通过制定相应的安全策略来防止非法访问者访问数据资源，对数据资源的存储以及传输进行安全性保护。在本系统中，参考OSI的七层协议，从网络级安全、传输级安全、系统级安全和应用级安全等几方面进行考虑，主要遵循下面的设计原则：

标识与确认（Identification & Authentication）

任何用户访问系统资源，必须得到系统的身份认证以及身份标识，如用户的数据证书、用户号码、密码。当用户信息与确认信息一致时，才能获准访问系统。在本系统中，对操作系统，数据库系统和应用系统都有相应的用户和权限的设置。

授权（Authorization）

对系统资源，包括程序、数据文件、数据库等，根据其特性定义其保护等级；对不同的用户，规定不同的访问资源权限，系统将根据用户权限，授予其不同等级的系统资源的权限。

日志（Logging）

为了保护数据资源的安全，在系统中对所保护的资源进行任何存取操作，都做相应的记录，形成日志存档，完成基本的审计功能。

加密（Encrypt）

为了保护数据资源的安全，在系统中对在网络中传输的重要信息必须经过高强度的加密处理来保证数据传输过程的安全性。

通过整体考虑来保证网络服务的可用性（Avaliability）、网络信息的保密性（Confidentiality）和网络信息的完整性（Integrity）。

综上，本次方案安全系统涉及建设规划如下：

**1、软件开发清单：**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **应用系统名称** | **模块名称** | **模块描述** |
| 1 | 密码应用适配开发 | 文物修复系统、检测检验管理系统、科研项目管理系统、古代工艺管理系统、学术活动管理系统等模块的密码应用适配开发 | 为实现网络和通信、设备和计算、应用和数据等层面的密码应用功能，开发适配文物修复系统、检测检验管理系统、科研项目管理系统、古代工艺管理系统、学术活动管理系统等密码应用的适配开发。 |

**2、网络产品购置清单：**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **类别** | **配置要求** | **数量** | **单位** |
| 1 | 网络设备 | 路由器 | 交换容量≥400Gbps；  包转发率≥400Mpps；  交换架构：集中式；  满足国产化要求，设备关键核心芯片（CPU/内存/以太网MAC（FPGA）/以太网PHY）采用国产化芯片；  配置万兆光接口≥6个，千兆电接口≥8个，光电复用口≥2个，提供官网链接及截图证明；  支持扩展槽数量≥8，提供官网链接及截图证明；  支持静态路由，RIP，OSPF，IS-IS，BGP；  支持内置智能管理中心功能，能作为管理中心，对接入设备进行统一智能化管理，提供官网链接及截图； | 1 | 台 |
| 2 | 网络设备 | POE交换机 | 交换容量≥672Gbps/6.72Tbps，包转发率≥171Mpps，L2以太网交换机主机,支持20个10/100/1000BASE-TPoE+电囗,4组GE/SFP Combo囗,4个1G/10G BASE-XSFP+端口,支持AC； | 7 | 台 |
| 3 | 网络设备 | 核心交换机 | 交换容量≥50Tbps；  包转发率≥37000Mpps；  支持主控≥2，独立业务槽位≥3，电源≥2，提供官网链接及截图；  为支持后续方案演进，支持FW防火墙和IPS防火墙业务卡，提供官网链接及截图；  为支持后续方案演进，支持PON插卡，提供官网链接及截图；  满足国产化要求，设备关键核心芯片（CPU/交换芯片）采用国产化芯片；  支持4K个VLAN，支持QINQ和灵活QINQ；  支持集群或堆叠多虚一技术，支持M-LAG或VPC技术，提供官网链接及截图；  支持IPv4、IPv6静态路由，RIP等三层动态路由协议支持策略路由器；支持RIP v1/2、RIPng；支持等价路由、VRRP、OSPFv1/v2、OSPF v3、BGP、ISIS等增强三层路由协议； | 2 | 台 |
| 4 | 网络设备 | 光模块 | 千兆多模 | 44 | 台 |
| 5 | 网络设备 | 楼层交换机 | 交换容量≥672Gbps/6.72Tbps；  包转发≥171Mpps；  L2以太网交换机主机,支持24个10/100/1000BASE-T电7,支持4个1G/10G BASE-XSFP+端口,支持AC； | 13 | 台 |

**3、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 | 安全设备 | 统一身份认证 | 规格：1U，内存≥16G，硬盘容量≥480G SSD，电源：冗余电源，接口：千兆电口≥6、千兆光口SFP≥4。  最大理论加密流量≥600 Mbps，最大理论建议并发用户数≥1200。  为保证产品稳定性和先进性，所投产品需采用零信任架构，满足默认不信任，持续验证的要求。  为满足身份安全要求，应支持多因素认证，至少包括：账号密码认证、短信认证、证书认证、动态令牌认证、扫码认证，以及对接统一认证平台实现单点登录等认证方式。账号密码认证应支持设备自带账号密码认证，或通过LDAP/Radius/HTTPS协议对接第三方认证服务器。扫码认证应至少支持零信任客户端、企微、钉钉、飞书扫码认证。单点登录应支持标准的CAS、OAuth2.0、OIDC协议对接；  为强化系统认证安全性，可配置在触发异常环境的条件时，用户需完成增强认证才可登录。可配置的异常环境包括但不限于：账号首次登录、账号在该终端首次登录、闲置账号登录、弱密码登录、异常时间登录、非常用地点登录等（需提供产品相关功能截图证明）  为满足组织灵活的管理要求，支持配置动态访问规则，可配置化的ACL规则引擎，可以灵活地将终端环境、用户身份、处置动作等进行配置，针对不同操作系统设定单独或多系统访问控制策略。动态访问控制策略支持“与”、“或”条件嵌套，并可通过单一条件或条件组的方式灵活组合嵌套，可支持多种条件变量设置，当检测到不符合安全条件时，支持如短信增强认证、告警等灵活的补救动作，实现灰度处置，有效平衡员工访问体验和安全保障（需提供产品相关功能截图证明）  为保障业务正常访问，客户端应兼容主流操作系统和芯片，操作系统至少包括Windows、macOS、Ubuntu、Android、iOS、UOS、Kylin、NFS、Harmony next，芯片至少包括兆芯、海光、飞腾、鲲鹏、海思麒麟、龙芯（需提供相关兼容性证明）  为了提升终端用户访问体验，支持时延优先的选路模式，支持周期性探测线路时延和多次探测确认恶化后切换（需提供产品相关功能截图证明）  为提升在弱网环境下访问体验，应支持优化TCP协议，增强隧道抗丢包、抗抖动特性，实现弱网环境的访问加速（需提供产品相关功能截图证明）；  ▲为降低业务访问时延，提升访问体验，应支持将短隧道资源新建连接耗时优化至 0RTT，大幅降低业务访问的网络时延，实现同等网络环境下访问速度接近甚至达到直连访问（需提供产品相关功能截图证明）  为方便管理员统筹查看管理零信任系统的整体运行状态，支持对设备自身的安全状态和策略配置进行巡检，对设备的整体状态进行打分，统计所有检查的正常项、异常项和告警项，并输出巡检报告；支持在设备上查看及下载巡检报告。报告应至少包含检测项、检查状态、存在的问题描述、建议改进措施等。  ▲支持对免认证应用的授信证书进行检查；支持对免认证应用的前端地址进行检查；支持检测是否启用了防中间人配置；支持HTTP监听端口开启检查；支持对启用的TLS协议是否安全进行检查；支持对是否启用应用防护策略进行检查（需提供产品相关功能截图证明）；  远程系统接入的用户身份安全、终端/数据安全、传输安全、应用权限安全和审计安全，符合国家商用密码标准，具有快速、易用、全面等优势特点。  SDP安全网关软件V2.0(\*1套)。 | 1 | 台 |
| 2 | 安全设备 | 安全管理平台产品 | 规格：2U，内存≥16G，硬盘容量≥128G minisata+2T SATA\*2，电源：单电源，接口：千兆电口≥6、万兆光口SFP+≥2；  包含主机审计许可证书数量≥50，最大可扩展审计主机许可数≥150，可用存储量：2TB（RAID1 模式），平均每秒处理日志数（eps）最大性能：2500；  支持 Deepin(深之度) Linux、Harmony(鸿蒙) OS、Ubuntu Kylin(优麒麟)、UnionTech(统信) UOS 等 25款 国产化操作系统日志接入；  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，以满足除内置解析规则之外未被覆盖的日志类型的解析（需提供产品相关功能截图证明）；  支持TLS加密方式进行日志传输，支持日志传输状态、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（需提供产品相关功能截图证明）；  ▲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，支持自定义关联分析规则（需提供产品相关功能截图证明）；  支持POC测试工具一键生成数据,验证日志数据采集是否成功，避免设备部署后采集失效但不被发现等风险（需提供产品相关功能截图证明）；  支持等保合规检测，用户可自查设备是否满足等保要求  日志审计分析管理系统软件V3.0(\*1套); | 1 | 台 |
| 3 | 安全设备 | 统一身份认证 | 规格：1U，内存≥8G，硬盘容量≥1.92T SSD，电源：单电源，接口：千兆电口≥6、千兆光口SFP≥4;  包含运维授权数≥50，最大可扩展资产数≥150，图形运维最大并发数≥100，字符运维最大并发数≥200;  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（需提供产品相关功能截图证明）;  支持首次使用手机动态口令由用户自行扫码配置;  用户登陆认证方式支持静态口令认证、手机动态口令认证、Usbkey认证、短信认证、AD域/LADP认证、Radius认证等认证方式；并支持各种认证方式和静态口令组合认证;  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（需提供产品相关功能截图证明）;  支持SQL语句阻断，对select、delete、drop等SQL语句执行进行阻断;  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，不改变运维人员操作习惯（需提供产品相关功能截图证明）;  图形资源访问时，支持键盘、剪切板、窗口标题、文件传输记录，并且对图形资源的审计回放时，可以从某个键盘、剪切板、窗口标题、文件传输记录的指定位置开始回放（需提供产品相关功能截图证明）  支持标准SNMP v1、v2、v3管理协议，支持syslog等标准日志格式外发;  所投产品需具备IPv6 Ready Logo认证证书，提供相关证书复印件； | 1 | 台 |
| 4 | 安全设备 | 防毒墙 | 产品以纯软件交付，包含管理控制中心软件及服务器客户端软件，软件授权不少于50;  支持跳转链接至云端威胁情报中心，针对已发生的威胁提供详细的分析结果，包含威胁分析、网络行为、静态分析、分析环境和影响分析。  ▲支持一键云鉴定服务，提供云端专家+沙箱+多引擎鉴定能力，结合云端威胁情报对已告警的威胁文件再次进行综合研判并给出100%黑白结果，用户可自助对管理平台告警的威胁快速判断是否误报和了解威胁详情（需提供产品相关功能截图证明）;  支持windows服务器RDP远程登录保护，可开启RDP远程登录二次认证，以防止黑客对服务器的入侵（需提供产品相关功能截图证明）；  支持Linux服务器SSH远程登录保护，可开启SSH远程登录二次认证，以防止黑客利用弱密码脆弱性对服务器的入侵；支持设置验证码验证或自定义密码验证，支持设置登录认证提示、生效时间段和免二次认证白名单（需提供产品相关功能截图证明）;  基于勒索病毒攻击过程，建立多维度立体防护机制，提供事前入侵防御-事中反加密-事后检测响应的完整防护体系，展示勒索病毒处置情况，对勒索病毒及变种实现专门有效防御（需提供产品相关功能截图证明）;  具备强力专杀云端下发通道，支持在管理端批量下发强力专杀工具到内网各终端快速响应终端威胁（需提供产品相关功能截图证明）;  ▲支持为同厂商的防火墙提供溯源举证功能，即本产品检测到僵木蠕毒的恶意域名访问时，会共享事件信息给同厂商的防火墙，包含事件相关的文件、进程、域名连接、注册表修改操作等关键项，并且可以在防火墙侧进行威胁事件的溯源分析。支持对根据回溯出的风险项一键根除，清除后进程无法被创建、运行（需提供产品相关功能截图证明）;  支持流行Windows高危漏洞的轻补丁免疫防御，支持Windows补丁批量一键修复;  支持基于威胁情报的病毒文件哈希值、行为、域名、网络连接等各项终端系统层、应用层行为数据在全网终端发起搜索，挖掘潜伏攻击，快速定位出全网终端感染该威胁的情况（需提供产品相关功能截图证明）;  终端安全管理系统软件V3.0（产品控制中心）; | 1 | 台 |
| 5 | 安全设备 | 防火墙 | 内存≥16G，硬盘容量≥128G SSD，电源：冗余电源，接口：千兆电口≥6;  网络层吞吐量≥20G，应用层吞吐量≥15G，防病毒吞吐量≥2G，IPS吞吐量≥2G，全威胁吞吐量≥1.5G，并发连接数≥800万，HTTP新建连接数≥16万;  所投产品采用自主知识产权的“高性能多核并行安全操作系统”;  所投产品支持静态路由、策略路由和多播路由协议，并支持BGP、RIP、OSPF等动态路由协议;  产品支持路由类型、协议类型、网络对象、国家地区等条件进行自动选路的策略路由，支持不少于3种的调度算法，至少包括带宽比例、加权流量、线路优先等（需提供产品相关功能截图证明）;  产品支持对不少于9000种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制（需提供产品相关功能截图证明）;  ▲产品支持云威胁情报网关技术，通过全球超过30+pop节点，实现对威胁流量就近进行实时检测&拦截，实现失陷外联实时阻断，保护资产安全。（需提供产品相关功能截图证明或具备 CMA标识的第三方检测报告）  ▲产品支持云端未知威胁主动探测技术，实现5min内未知威胁情报全网设备下发。（需提供产品相关功能截图证明或具备 CMA标识的第三方检测报告）  产品内置不低于16000种漏洞规则，同时支持在控制台界面通过漏洞ID、漏洞名称、危险等级、漏洞CVE标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义IPS规则（需提供产品相关功能截图证明）;  产品支持僵尸主机检测功能，产品内置僵尸网络特征库超过120万种，可识别主机的异常外联行为（需提供产品相关功能截图证明）;  产品支持独立的账号安全防护模块，具备事前账号脆弱性、事中账号爆破、事后账号失陷的全生命周期安全防护，在设备界面可以详细展示账号安全相关信息，包括风险业务、风险等级、存在账号入口、存在弱口令、遭受口令爆破、异常登录账号登（需提供产品相关功能截图证明）;  防火墙软件基础级(\*1套);云智订阅软件【云智+云威胁情报网关】(\*3套);云威胁情报网关订阅软件【云智+云威胁情报网关】(\*3年); | 1 | 台 |
| 6 | 安全设备 | 上网行为管理产品 | 网络层吞吐量≥5.8Gb，应用层吞吐量≥750Mb，带宽性能≥500Mb，支持用户数≥4000，包转发率≥90Kpps，每秒新建连接数≥10000，最大并发连接数≥500000；规格：1U；内存≥8G；硬盘容量≥480G SSD；电源：单电源；接口：千兆电口≥6。  全网行为管理系统软件V13.0(\*1套);URL&应用识别规则库升级(\*3套);  支持首页分析显示接入用户人数、终端类型；带宽质量分析、实时流量排名；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；  ▲支持客户端SSL解密，客户端会自动推送根证书安装（需提供产品相关功能截图证明）;  设备内置应用识别规则库，支持超过9000种以上应用规则数、支持超过6000种以上的应用；支持根据标签选择应用，并支持给每个应用自定义标签；支持根据标签选择一类应用做控制;  支持允许用户登录Webmail收邮件，而禁止发送Webmail邮件的功能（需提供产品相关功能截图证明）;  支持图形化查看当前内网IP使用情况，帮助管理员减少人工维护IP表的工作量;  ▲支持与同品牌下一代防火墙系统实现认证联动，可以转发用户认证信息到下一代防火墙，实现单点登录；支持与同品牌安全态势感知产品实现联动，实现资产信息上报；支持与同品牌EDR产品实现联动，当检测到终端未安装EDR产品时，禁止上网并提示需要安装EDR终端软件（需提供产品相关功能截图证明）;  所投产品需具备《网络安全专用产品安全检测证书》或同等效力的其他证书，提供相关证书复印件;  支持终端用户账号绑定手机号码和微信号，绑定后可以通过手机验证码和微信扫码实现上网快捷登录认证; | 1 | 套 |
| 7 | 安全设备 | 入侵检测系统 | 规格：1U，内存≥8G，硬盘容量≥128G SSD，电源：单电源，接口：千兆电口≥6、千兆光口SFP≥4;  网络层吞吐量≥1Gbps，应用层吞吐量≥500Mbps;  支持命令注入检测、PHP代码检测、XSS攻击检测、Webshell上传检测、SQL注入检测、XXE攻击检测、JAVA代码检测、SQL非注入型检测、MYSQL解析增强、php反序列化检测等自定义配置启用，针对命令注入检测、SQL注入检测等类型支持自定义高检出、低误报模式。（需提供产品相关功能截图证明）  ▲支持敏感信息检测功能，内置身份证、MD5、手机号码、银行卡号、邮箱等敏感信息，可自定义敏感信息检测策略选择组合的敏感信息，可基于IP统计和连接统计2种方式进行命中次数统计（需提供产品相关功能截图证明）;  支持基于IP和域名的旁路阻断，能够在实时镜像的流量中发现恶意IP并实现实时阻断，支持24小时/7天/最近30天/永久或者自定义时间阻断威胁（需提供产品相关功能截图证明）;  支持传输协议审计日志，包括https、http、DNS、邮件协议审计日志、SMB、AD域、WEB登录、FTP、TELNET、ICMP 、SNMP 、SSL 、SSH、SIP 、ONVIF 、NFS 、SOCKS 、dhcp、netbios\_nbns、流量元数据审计、数据库审计协议等（需提供产品相关功能截图证明）;  支持流量抓包分析，基于五元组灵活抓取数据包，可定义配置源IP、源端口、目的IP和目的端口、传输层协议选择添加抓包任务，并支持带标签抓取vlan、mpls等协议数据包，帮助安全工程师高效分析威胁（需提供产品相关功能截图证明）;  潜伏威胁探针系统软件V3.0(\*1套);安全感知系统探针特征库软件V2.0(\*2套); | 1 | 套 |
| 8 | 密码设备 | 其他安全产品 | 2U设备，支持双电源，支持国产操作系统，不少于8核16线程国产CPU X1，不少于1T硬盘，不少于32G内存，不少于6个千兆电口，不少于4个千兆光口，默认配备满模块;  SSL吞吐率（国际）不少于4.5Gbps;  SSL每秒新建连接数（国际）不少于3600;  SSL吞吐率（国密）不少于3.5Gbps;  SSL每秒新建连接数（国密）不少于9000;  四层吞吐率不少于4.5Gbps;  四层每秒新建连接数不少于750000;  四层并发连接数不少于15000000;  七层吞吐率不少于4.5Gbps;  七层每秒新建请求数不少于2400000;  七层并发连接数不少于4800000;  ▲支持后量子密码算法Dilithium、Falcon、Kyber，支持产生后量子证书请求、导入后量子密钥及证书、证书查看等后量子证书管理功能。支持通过后量子密码算法进行SSL通信，保证用户数据的传输安全（提供产品截图证明材料）;  支持QUIC/HTTP3协议（提供产品截图证明材料）;  支持OCSP stapling通过优化证书状态查询流程，显著提升SSL/TLS连接的效率和安全性。（提供产品截图证明材料）;  支持SSL拦截白名单，只允许通过指定的域名访问特定的SSL服务;  支持HTTP、HTTPS、HTTP3、TCP、DNS TCP、DNS UDP、Diameter、RDP、SIP over TCP、SIP over UDP、RTSP等虚拟服务类型。（提供产品截图证明材料）  支持基于OAuth、SAML、LDAP、Radius等方式的安全认证代理功能，可在应用无改造的情况下实现虚拟服务对应客户端的身份认证与单点登录功能。（提供产品截图证明材料）  所投产品具备适配国产化的操作系统：统信、银河麒麟的适配证明（提供证明材料）  ▲所投产品具备适配国产化的CPU 环境：海光和兆芯的适配证明（提供证明材料） | 1 | 台 |
| 9 | 密码设备 | 其他安全产品 | 2U设备，支持双电源，支持国产操作系统，不少于16核32线程国产CPU X1，不少于1T硬盘，不少于128G内存，具备高性能虚拟密码卡X1，不少于2个千兆电口，不少于4个万兆光口，默认配备满模块；  短信令牌(SM3)生成不少于4500次每秒  短信口令(SM3)生成不少于12700次每秒  动态令牌(SM3)验证不少于12000次每秒  同时支持基于SM3、SHA1算法的动态令牌(提供投标产品功能截图）  支持时间型令牌、挑战型令牌及挑战-时间型复合令牌，(提供投标产品功能截图）  ▲提供Radius认证服务，支持RADIUS PEAP、PAP、CHAP、MSCHAP、MSCHAPv2协议(提供投标产品功能截图）  支持系统登录时动态口令与静态口令验证方式一键切换功能(提供投标产品功能截图）  提供一键巡检功能，自动对系统软、硬件进行健康检查并生成巡检报告；  提供日志和审计功能，可分类审计系统日志，对日志进行审计和统计  支持NAS登录黑白名单控制机制，可自定义登录NAS的IP范围，防止未经授权的恶意访问(提供投标产品功能截图）。  所投产品具有《商用密码产品认证证书》（提供证明材料）。 | 1 | 套 |
| 10 | 密码设备 | 其他安全产品 | 1U设备，支持双电源，不少于4核国产CPU X1，不少于128G固态硬盘 X1，不少于8G内存，国产操作系统，不少于6个千兆电口，不少于4个千兆光口，默认配备满模块；  签名：RSA2048不少于0.25KTPS，SM2不少于2.5KTPS；  验签：RSA2048不少于4.8KTPS，SM2不少于1.8KTPS；  支持非对称算法：RSA、SM2、ECC；  支持摘要算法：SM3、MD5、SHA1、SHA256、SHA512；  支持对称算法：SM4、3DES、AES、DES、RC4、RC2；  支持PDF签名验签功能（要求提供产品截图证明材料）  支持大文件签名（要求提供产品截图证明材料）  ▲支持KEK和默认两种方式的密钥加密导入导出功能以实现多机部署（要求提供产品截图证明材料）  支持对非对称算法、摘要算法、对称算法进行弱算法过滤的设置（要求提供产品截图证明材料）  ▲支持XML封皮、封内、分离签名验签；支持支付宝XML签名验签；支持财付通XML签名验签（要求提供产品截图证明材料）  支持多台设备（包括生产系统和灾备系统）之间对称密钥同步（要求提供产品截图证明材料）  API和Server间可实现加密方式传输（要求提供产品截图证明材料）  可批量执行巡检指令实现一键巡检并生成巡检报告；包括日常巡检、应急巡检和深度巡检。（要求提供产品截图证明材料）。  所投产品具有《商用密码产品认证证书》，并标明GM/T 0028-2014密码模块技术要求中第二级要求（提供证明材料）。 | 1 | 台 |
| 11 | 密码设备 | 其他安全产品 | 用于密评网络和通信层、设备和计算层整改。遵循国密SSL协议规范的通用浏览器；  支持HTTP/1.1、HTTP/2.0协议、Web Workers、MathML、支持W3C标准、HTML5最新标准支持WebGL(Web图形库)；  支持页面解析、页面标签栏、标签栏支持标签分组、页面地址栏、书签栏、下载管理、登录密码自动保存、页面查找、网页内容字体自定义、页面缩放、页面恢复、超级拖拽、证书管理、扩展程序管理、网页静音、快捷键、鼠标手势、全屏模式、无痕浏览模式、新标签页背景个性化设置、新标签页自定义导航个数、网页翻译、保存网页为图片等功能；  支持沙箱机制、浏览器内核隔离域、跨域安全隔离、站点安全隔离防护、可信证书校验等功能；  支持兼容模式下开启数据执行保护，保证应用数据安全；  支持国密算法，包括：SM2/SM3/SM4；支持SSL单/双向协议；支持最新TLCP标准；支持极速、兼容模式下通过国密协议访问，针对国密网站优先通过国密协议访问； | 10 | 套 |
| 12 | 密码设备 | 其他安全产品 | 域名证书，部署在应用安全网关，用于在客户端和服务端之间建立国密SSL通道 | 1 | 套 |
| 13 | 密码应用功能模块 | 密码应用功能模块 | 配合密评开展针对内部系统做相应功能开发 | 2 | 人月 |

# 其他工作要求

## 售后服务要求

本项目从系统验收通过之日起质保3年。质保期内，成交供应商必须承诺提供免费技术后援支持，包括专业技术咨询、故障排查、紧急事件处理等工作；至少提供7\*8客户咨询服务，对用户的故障通知，成交供应商应在接报后1小时内响应，24小时内排除故障。

## 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)提供至少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。

## 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。

## 等级保护要求

本项目等级保护要求： 二级等保。

## 商业密码应用需求

本项目另一项内容主要对我单位电子公文处理系统进行密码应用改造，以达到《密码应用基本要求》对信息系统密码应用安全二级的要求，合规、正确、有效地使用商用密码对系统进行保护，并通过密码应用安全性评估。

本项目将依据方案中确定的密码应用需求、密码应用设计方案，使用经检测认证合格的商用密码产品、服务，对现有的应用进行开发改造、系统集成、联调测试等方式建设密码技术体系；依据安全管理方案，制定密码安全相关人员、制度、业务、运维、应急等方面的管理措施，同步建立密码安全管理体系。

密码建设内容如下表所示：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **产品名称** | **数量** | **单位** |
| 1 | 应用安全网关 | 1 | 台 |
| 2 | 动态令牌认证系统（含动态令牌TOKEN） | 1 | 套 |
| 3 | 签名验签服务器 | 1 | 台 |
| 4 | 安 全 浏 览 器（ 含 密 码 模块） | 10 | 套 |
| 5 | 域名证书 | 1 | 套 |
| 6 | 密码应用功能模块 | 2 | 人/月 |

# 其他

供应商具有质量管理体系认证、信息技术服务管理体系认证、信息安全管理体系认证的优先考虑。

# 附录

**若项目建设过程中需符合相关技术标准或规范文件的要求，请将相关文件作为附件列出。**

**参考如下：**

1、《政务网络安全监测平台总体技术要求》



2、《上海市电子政务外网建设和运行管理指南（试行）》

