**二、****采购内容及要求：**

### 一、项目概况：

**（一）、概述**

按照公安部《公安交通管理综合应用平台社会化服务系统升级改造技术方案》以及《陕西省公安交通管理综合应用平台社会化服务系统推广应用工作方案》的要求，为规范和加强公安交通管理综合应用平台社会化服务系统（以下简称“社会化服务系统”）的运行和使用，有效提升公安交通管理服务管理效能，强化信息系统安全，对我支队公安交通管理社会化服务系统进行升级改造。

**（二）、需求分析**

**1、车驾管业务信息系统现状**

随着公安交通管理信息化建设应用以及公安交管“放管服”改革措施的不断深入，西安市公安局交通警察支队车辆管理所（以下简称“西安车管所”）逐步建立了以公安信息通信网、互联网、查验检验专网以及科目二三考试专网为基础支撑环境的信息化技术架构。

其中公安信息通信网承载了公安交通管理的日常业务，业务系统“公安交通管理综合应用平台（六合一平台）”部署在省交警总队，西安车管所作为终端用户通过该平台办理车驾管相关业务。

查验检验专网、驾驶人考试专网（以下简称专网）连接了社会化机动车查验、检验机构以及驾驶人科目二、三考场，部署无锡科研所统一研发的机动车检验监管系统、科目二、三考试监管系统对机动车检验业务、驾驶人科目二、三考试进行监管，并通过支队公安信息通信网边界接入平台与“公安交通管理综合应用平台”进行数据交换。专网作为“放管服”改革措施的业务承载网络，目前接入机动车社会服务（查验）机构130家、检验机构72家、科目二、三考场148个，为机动车注册登记、机动车查验检验、驾驶人科目二、三考试等社会化服务提供了有力的支撑环境。

**2、存在的问题**

近年来，“放管服”改革的深入使社会化服务机构参与交通管理不断增多，对社会化服务系统的业务管理、运维保障、信息安全和技术服务能力提出了更高要求，而现有系统技术架构、运行模式与快速增长业务需求已不相适应。

**（1）、系统整体架构不统一，开发维护成本较高。**

现有社会化服务系统项目建设阶段不同、缺乏统一的规划设计，导致各系统间基础架构、运行环境、数据存储机制方面等差异性较大，后期新功能开发涉及环节较多、运行维护成本高、软硬件资源利用率低。

**（2）、信息关联共享不方便，制约业务发展。**

由于现有各信息系统之间存在物理和网络隔离，如我支队查验检验专网和科目二、三考试专网，信息不能有效共享，业务数据和音视频监控等资源不能有效融合，难以支撑业务流程优化再造和业务监管强化等管理创新，业务服务能力需要进一步提高。

**（3）、跨网数据交换效率不高，存在安全隐患。**

我支队在用的边界接入平台为2016年建设，设备普遍老化，且负荷较大，导致数据交换效率低、容错性差，存在安全隐患。

**（4）、系统运行环境复杂，安全防护能力较差。**

目前系统数据库服务器、应用服务器均分散部署，管理难度大，安全措施较难落实。社会化服务系统绝大部分用户为社会机构单位，终端接入数量大、用户类型和应用环境复杂，安全管理机制不健全，存在终端电脑非法接入、随意插入使用移动存储介质、私下使用无线网卡违规访问互联网等问题，信息安全隐患较大。

**（三）、项目目标和任务**

**1、改造目标**

按照《公安交通管理综合应用平台社会化服务系统升级改造技术方案》要求，升级改造社会化服务系统，全面提升社会化服务系统的运行效率、服务能力和信息安全防护水平：

**（1）、统一技术架构。**

统筹整合社会化服务网络系统中交管信息资源，推进机动车登记服务、机动车查验监管、机动车检验监管和驾驶证管理、驾驶理论考试、驾驶人考试监管等系统升级改造，应用统一版社会化服务系统，畅通业务流、数据流，提升系统运行效率，便捷运维管理。

**（2）、提升服务效能。**

全面梳理社会化服务系统业务流、数据流，厘清统一版软件与自建的音视频共享管理平台、音视频智能识别分析系统、机动车检验系统、科目二三考试系统、排队叫号软件等的关系和功能定位，规范开展外挂软件的升级改造和音视频管理应用，推进业务融合升级改造，提升服务群众水平。

**（3）、强化业务监管。**

畅通社会化服务系统与综合业务监管系统间数据通道，进一步完善基于大数据的业务监管指标体系及监管机制，融合应用业务数据和音视频非结构化数据，实现业务数据与音视频数据的精准关联、AI音视频监管，强化对社会化机构代办交管业务的监管能力，提升系统整体应用成效。

**（4）、夯实信息安全。**

从网络、数据交换、服务器部署、业务应用、终端电脑等方面提出安全管理要求，规范社会化服务网络的建设和使用，保障接入网络、用户终端电脑、驾驶理论考试考台及移动接入端的运行使用安全，全面提升系统安全防护能力。

**2、改造任务**

社会化服务系统作为公安交通管理综合应用平台一部分，是公安交通管理社会化服务的基础支撑系统，此次社会化服务系统升级改造任务具体如下：

**（1）、升级改造统一版系统**

全面整合社会化服务网络的机动车登记和查验、机动车检验、驾驶证管理、驾驶人考试、考试监管软件等系统的数据资源和功能模块，进行微服务技术架构改造和业务流程优化，提供统一平台和门户供用户使用，软件由公安部无锡科研所统一开发，本项目构建支撑微服务架构的社会化服务系统运行的软硬件环境，并完成支队级社会化服务系统安装部署。

全面升级和改造跨网交换服务系统，统一技术架构和实现方式，支持多边界、多通道并行的跨网数据传输，便捷运维管理和提升安全性。

**（2）、升级改造自建系统**

按照《人脸识别技术支撑服务系统建设要求》建设支队级人脸识别系统，对社会化服务系统中驾驶人考试业务系统进行人脸识别服务支持。

在社会化服务网络部署统一的时钟同步服务器系统，确保各系统及前端设备的时钟一致性。

**（3）、强化信息系统安全**

按照等保三级的安全标准建设社会化服务系统配套的安全产品，建立相应的安全运维管理机制，组织进行等保三级评测，并取得等保三级证书。

网络访问控制，基于先认证后连接架构配备网络安全准入设备和访问控制模块，确保接入终端电脑经认证鉴权后才能访问社会化服务网络资源。外部不能扫描到任何受控网络、资源地址，配备IDS、主机防护等安全产品，实现网络信息传输监控和检测。

终端安全，社会化机构用户通过终端电脑登录使用社会化服务系统应使用统一的社会化服务专网终端电脑用户安全管控设备（Ukey），本项目部署支队级社会化服务系统的电脑终端Ukey硬件管控模块，实现社会化服务系统终端设备的访问控制、用户登录认证和终端运行环境监测。

边界安全，更新边界接入平台设备，确保专网和公安信息通信网之间数据交换安全、畅通。

数据安全，一是建立数据库审计机制，实时记录数据库活动，对数据库操作进行细粒度审计的合规性管理，对数据库遭受到的风险行为进行告警并阻断攻击行为。二是建设数据容灾备份系统，对核心数据进行全库备份，防止原数据丢失、破坏，保证数据安全。

**（4）、建立系统运行保障机制。**

建立社会化服务系统的运行保障机制，部署运行监控系统，通过基础设施展示、通信实时状况展示、终端设备应用状态展示、系统服务及组件状态展示协助运维团队做好系统的运维工作。

### 二、采购内容

**（一）、系统构成**

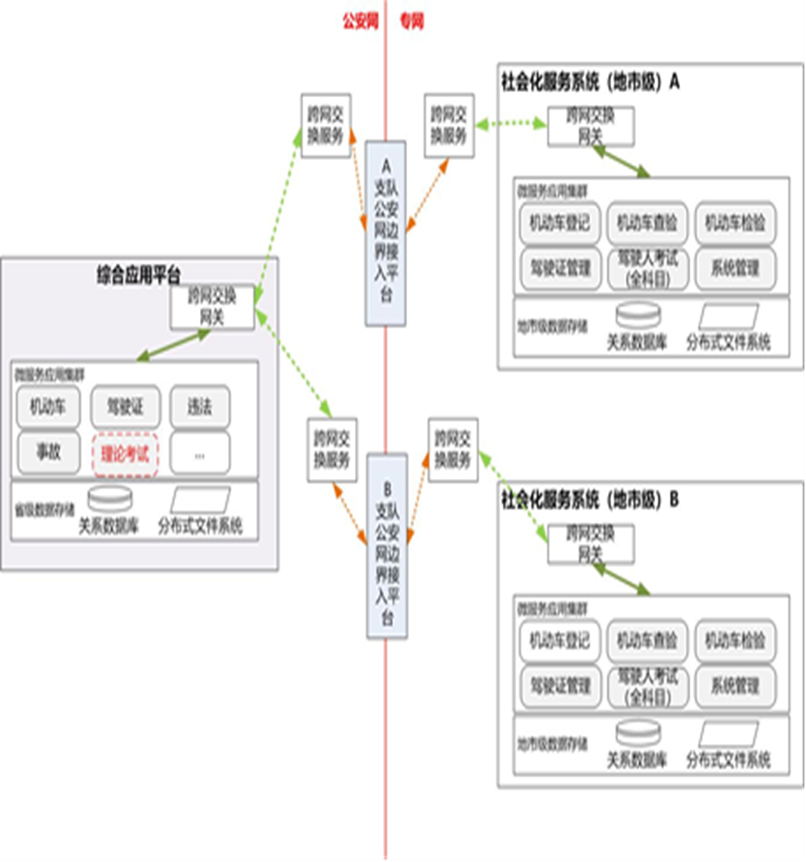
**1、总体架构**

社会化服务系统总体上由统一版系统、自建系统组成。统一版系统由社会化服务系统、跨网交换服务系统、统一终端设备管理软件和考台桌面软件组成。自建系统由人脸识别服务、音视频共享管理平台、音视频智能识别分析系统、科目二考试系统、科目三考试系统和排队叫号系统等组成，**本项目的自建系统只涉及人脸识别服务和时钟同步系统**。总体架构如下图所示：



**2、部署模式**

根据省总队《关于开展全省公安交通管理综合应用平台社会化服务系统升级推广应用工作的通知》，本项目采用支队集中部署模式。即机动车登记和查验系统、机动车检验业务与驾驶人考试业务（科目一四）、驾驶人考试监管系统（科目二三）均由支队集中建设，并在支队层级发布业务微服务。如下图所示：



**（二）、采购设备明细表**

**1、设备清单及参数要求**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **技术要求** | **单位** | | **数量** |
| **社会化服务系统统一版运行环境（含自建系统）** | | | | | |
| 1 | 超融合架构一体机（核心产品） | 1、硬件参数：规格：2U；CPU：2颗国产化CPU，主频≥ 2.7GHz（32C）；内存≥320GB DDR4 3200；系统盘≥480GB SATA SSD；缓存盘≥1920GB SATA SSD；数据盘≥24TB HDD；电源：白金，冗余电源；接口：4千兆电口+2万兆光口。 2、其他：超融合软件授权（\*2C）；万兆多模-850-300m-双纤\*2个;产品质保\*3年;软件升级\*3年; 软件功能： 1.为及时发现将来可能存在硬件问题，支持对超融合平台的硬件进行监控和大屏展示，包含CPU、内存、网卡、硬盘、存储、RAID等硬件健康检测，并提供相应异常检测项的恢复指导建议。  2.虚拟化软件应基于 KVM 开发，能够随着 Linux版本的升级而升级，部署时无需绑定安装OpenStack相关组件。  ▲3.虚拟化软件兼容 OpenStack Havana、Juno、Kilo、Mikata、Pike 等主流版本，并能提供标准接口实现与 OpenStack 平滑对接。满足本次项目软件平台的使用。  ▲4.支持对超融合平台的硬件进行监控和大屏展示，包含CPU、内存、网卡、硬盘、存储、RAID等硬件健康检测，便于及时发现问题并提供相应异常检测项的恢复指导建议。  ▲5.兼容现有市场上主流的存储阵列产品和存储协议，平台提供FC-SAN、iSCSI存储对接功能。  ▲6.每个超融合节点出厂自带管理软件，设备上电后可登录任意一台来做超融合管理节点，提升集群冗余度，提升集群资源实用效率，所有节点全部通用（均作为计算、管理、存储、网络来实用），不限制节点使用场景。  **其他要求见三、技术要求 （三）社会化服务系统统一版运行环境搭建章节** | | 台 | 8 |
| 2 | 分布式存储服务器 | 1.单台CPU：2颗国产化CPU，频率≥2.2G，核心数≥24C； 2.内存≥128G； 3.硬盘：≥1920G SAS + ≥120TB SATA； 4.网络：2\*GE+2\*10GE（光口，含光模块）； 5.RAID卡：支持Raid 0/1/5/6。  **其他要求见三、技术要求 （三）社会化服务系统统一版运行环境搭建章节** | | 台 | 2 |
| 3 | 统一版承载交换机 | 1、 万兆交换机，≥48个万兆SFP+光口（含光模块），≥4个40GE QSFP+光口（含光模块）；交换容量≥2.50Tbps/40.90Tbps，包转发率≥1260Mpps/1620Mpps，支持全端口线速转发；支持双电源模块，交流电源≥2个，电源风扇≥4个。 | | 台 | 2 |
| 4 | 人脸识别服务 | 按照《公安交通管理综合应用平台和互联网交通安全综合服务管理平台人脸识别技术支撑服务系统建设要求》，在社会化服务网络部署应用人脸比对服务。实现驾驶人考试、自助处理等业务中的人证一致性身份比对功能。   1. 支持1:1人脸照片比对能力; 2. 人脸检测、特征提取和人脸识别功能； 3. 支持 jpg、jpeg、png、gif、bmp、tif图片格式； 4. 支持比对水平偏转不超过60度，俯仰角度不超过45度的人脸图片；   支持对已存储的人脸抓拍库进行历史记录查询。  **详细要求见技术要求 三、技术要求 （二）、自建系统人脸识别服务章节** | | 套 | 1 |
| 5 | 时钟同步服务器 | 1. LED时钟显示面板 ２、同步时钟以NTP时间服务器为时间源。 ３、支持TPv1.v2.v3.v4(RFC1119&1305)SNTP(RFC2030) (RFC1321)时钟协议。 ４、支持所有NTP协议的服务器、PC、嵌入式设备。  ５、每秒可处理8000次以上的授时请求。   6、支持北斗授时。 | | 台 | 2 |
| 6 | 机柜 | 19英寸42U标准服务器机柜  应包含本项目服务器、交换机等设备安装所需的所有配件 | | 台 | 5 |
| **安全系统设备** | | | | | |
| 7 | 堡垒机 | 1、性能参数：默认包含运维授权数≥50，为综合应用平台社会化服务系统提供运维审计功能，保证运维操作可审计，可留痕，可追溯。为提升关键业务系统运维安全性同时防止密码丢失或忘记的事件发生，产品支持密码文件备份功能，密码文件需密文保存，密码包及解密密钥分别发送给不同管理员保存，并使用专用的解密器才可打开；产品包含软件规则库升级3年。 2、支持对用户指定限制登录IP、登录时间段（可循环，如每周一到周五9：00-17：00时）等规则，以确保可信用户登陆系统。 3、支持Windows AD域账号与堡垒主机账号周期比对，可自动删除、手动删除或锁定失效的域账号。 4、支持口令有效期设置，用户账号口令到期强制用户修改自身口令，口令强度必须符合密码策略要求。 | | 台 | 1 |
| 8 | 主机安全防护 | 1、服务器端杀毒软件，安全策略模板一体化设置，全网资产盘点与风险可视，自动化日志可视化报表一键导出。  2、产品包含软件规则库升级3年。  **其他要求见三、技术要求 （四）安全系统 章节** | | 套 | 11 |
| 9 | IDS | 1、国产化入侵检测设备，性能参数：网络层吞吐量≥20Gbps，IPS吞吐量≥2Gbps。并发连接数：≥8000000，新建连接数：≥160000。 2、硬件参数：规格：机架式设备，内存大小≥4G，接口≥4千兆电口； 3、产品包含软件规则库升级3年。  **其他要求见三、技术要求 （四）安全系统 章节** | | 台 | 1 |
| 10 | WAF防火墙 | 1、国产化WEB防火墙，性能参数：网络层吞吐量≥20Gbps，HTTP应用层吞吐量≥15Gbps，HTTP并发连接数≥2200000。 2、硬件参数：规格：内存大小≥8G，硬盘容量≥2T，接口：≥4千兆电口，≥2万兆光口，含光模块；  3、产品包含软件规则库升级3年。  **其他要求见三、技术要求 （四）安全系统 章节** | | 台 | 1 |
| 11 | 自动化安全检测装置 | 1、安全组件、功能授权：系统资产授权IP数：≥100，WEB资产授权URL数：20；识别和发现网络中的各类资产，高效、全面、精准地检查网络中的各类脆弱性风险，根据扫描结果提供专业、有效的安全分析和修补建议，全面提升客户网络环境的整体安全性。为综合应用平台社会化服务系统提供脆弱性扫描功能。 ▲2、支持全局风险统计功能，通过扇形图、标签、表格、条状图、等形式直观展示资产风险分布、漏洞风险等级分布、紧急漏洞、风险资产清单等信息详情。支持全面扫描、资产发现、系统漏洞扫描、弱口令扫描、WEB漏洞扫描、基线配置核查六种任务类型，其中全面扫描支持系统漏洞扫描、WEB漏洞扫描、弱口令扫描同时执行。 3、支持资产发现功能，可基于IP地址、IP网段、IP范围、URL等方式进行资产发现扫描； 4、支持国产操作系统的漏洞扫描，包括麒麟（Kylin）、统信（UnionTech OS）、中兴新节点（NewStart CGSL）等。 5、支持国产数据库的漏洞扫描，包括达梦、人大金仓、南大通用等。  6、支持从“严重”、“高危”、“中危”、“低危”四个安全级别展示资产的风险分布情况。 7、支持从“严重”、“高危”、“中危”、“低危”四个安全级别展示漏洞风险等级的分布情况。 ▲8、支持从紧急漏洞的视角展示主机风险，清晰呈现已发生和未发生的紧急漏洞类型，支持以报表形式展示紧急漏洞的风险等级、影响资产数、漏洞数量、最近发现时间，可关联漏洞详情。  9、产品包含软件规则库升级3年  **其他要求见三、技术要求 （四）安全系统 章节** | | 套 | 1 |
| 12 | 防火墙 | 1、国产化防火墙，网络层吞吐量≥20G，应用层吞吐量≥18G， IPS吞吐量≥4G，并发连接数≥800万，HTTP新建连接数≥15万。 2、硬件参数：规格：机架式设备，内存大小≥16G，电源：冗余电源，接口数量≥4千兆电口+4万兆光口，含光模块。 3、产品支持漏洞规则库、支持WEB应用攻击特征库。包含软件规则库升级3年。  **其他要求见三、技术要求 （四）安全系统 章节** | | 台 | 2 |
| 13 | 边界安全产品--安全数据交换系统 | 1、 产品形态：包含两台独立的硬件设备，两台设备均为标准机架式机箱。 硬件配置： 1、CPU：国产芯片； 2、操作系统：国产操作系统；硬件接口：每台硬件设备各不少于1个100/1000MBase-TX管理接口、5个100/1000MBase-TX网络接口、4个千兆SFP光网络接口、4个万兆SFP+多模万兆光网络接口。  性能参数：交换能力：≥4000Mbps；并发会话：30000个；数据库到数据库交换记录数（＞100Kb/记录）：≥10000条/秒；文件数据处理数（＞100Kb/个）：≥10000个/秒；最大支持服务个数：≥60；稳定性运行时间（MTBF）：＞50000小时；文件数据处理吞吐量：≥4000Mbps；应用层数据交换速度（FTP）：≥4000Mbps；最大数据文件：≥30G；任务调度粒度：秒级；目录监控触发时间：＜1秒；最大传输延时：＜20ms； 功能要求： 1、支持主流关系型数据库数据交换：Oracle、DB2、SQLServer、Sybase、MYSQL、PostGresql的各种版本，及支持dameng、Gbase、oscar、kingbase等国产数据库，及支持Cassandra、UDB、Hbase等大数据数据库,同时可支持KAFKA消息交换。 ▲2、支持IPv4/IPv6双协议栈网络环境，支持IPv4/IPv6两种网络互相转换。 3、产品包含软件规则库升级3年  **其他要求见三、技术要求 （四）安全系统 章节** | | 套 | 1 |
| 14 | 边界安全产品--安全隔离网闸 | 1、 硬件形态：标准机架式硬件设备，采用国产CPU;  网络接口：内外网不少于6个千兆电口、8个千兆光口、4个万兆光口、1个接口扩展槽、2个USB接口；不少于2个液晶显示屏；  2、 性能指标：  系统吞吐量≥8.4Gbps；并发数≥500000；  主要功能：  1、支持IPv4、IPv6双协议栈接入；  ▲2、支持支持oracle、Sql Server 、DB2、Sybase等主流数据库间的同种或异种数据库同步，支持单向和双向同步；  3、产品包含软件规则库升级3年。  **其他要求见三、技术要求 （四）安全系统 章节** | | 台 | 1 |
| 15 | 边界安全产品--集中监控管理系统 | 1.硬件形态：标准机架式机箱、冗余电源，采用国产CPU；  2.网络接口：标配≥8个千兆电口、4个千兆光口，2个USB接口；  3.软件功能：采用国产操作系统，具备面向边界接入平台的状态监控、边界运行态势展示和级联管理等功能；  ▲4.产品性能：系统吞吐量≥800Mbps，日志采集速率≥800EPS、级联上报延时≤10s；  5．主要功能：  产品满足公安部安全规范要求能够提供边界接入不同层次的信息注册和管理，包括接入平台的基础信息、建设情况、使用单位、运维信息等信息。  支持部、省、市三级平台体系级联功能，具备设备性能、网络状况监测功能，可自定义检测周期及历史记录生成周期；  6、产品包含软件规则库升级3年  **其他要求见三、技术要求 （四）安全系统 章节** | | 台 | 1 |
| 16 | 边界安全产品--集控探针 | 1.硬件形态：采用国产平台，标配≥4个千兆电口、2个USB接口；  2.软件功能：采用国产操作系统，支持通用网络设备日志采集，支持标准SYSLOG协议、支持SNMP协议；  ▲3.产品性能：系统吞吐量≥800Mbps，日志采集速率≥200EPS、上报延时≤10s；  4.功能要求：  支持采集交换机、路由器、防火墙、入侵检测、可信边界网关等边界接入链路外网侧常用设备的运行状态信息；  支持标准Syslog协议；  支持SNMP v2/SNMP v3协议；  5.产品包含软件规则库升级3年。  **其他要求见三、技术要求 （四）安全系统 章节** | | 台 | 1 |
| 17 | 边界安全产品--可信边界安全网关 | 1、标准机架式机箱，支持国产平台，采用国产CPU，国产操作系统。  2、性能参数：  接口：不少于4\*1000Mbps网口，万兆 SFP+口2个，1个管理串口；国密最大新建连接数：3000次/秒；国密最大并发连接数：30000；国密SSL事务处理速率：5000次/秒；加密带宽吞吐量：1.5Gbps；接入用户数：>50000；  功能参数：  1.支持国密算法；  ▲2.支持多证书链：支持为每个证书链配置不同的证书验证策略，支持CRL方式和OCSP方式证书有效性验证；支持基于证书内容的二次过滤；  3.持B/S应用和通用C/S应用、多服务功能、支持应用重定向功能；  4.支持被保护应用资源的注册、授权、应用策略的管理、应用存活状态实时监测；  5.支持自定义SSH服务端口、支持关闭SSH服务；  6.支持系统审计日志信息分级别记录；  7.支持内置网络诊断工具，至少包含PING测试、TCP测试、HTTP测试等；  8.产品包含软件规则库升级3年。  **其他要求见三、技术要求 （四）安全系统 章节** | | 台 | 1 |
| 18 | 准入直连网关 | 1、标准机架式机箱，交流冗余电源，国产化硬件平台；标准配置≥16G内存，系统盘≥64G,标准配置6个10/100/1000M Base-TX，4个千兆光口，2个扩展卡槽位；明文整机吞吐20G，国密加密吞吐量800M；支持SM2、SM3、SM4等国家商用密码算法，单台设备建议最大并发用户5000个；可集群方式实现横向扩展。 2、支持与SDP控制器和客户端组合联动实现网络隐身的功能，确保只有通过认证的主体才能接入SDP安全网关，SDP安全网关不响应未通过认证主体的连接请求；支持基于国密算法的传输加密，实现SDP安全网关和客户端之间数据传输的机密性及完整性保护；支持被保护资源的地址隐藏；支持与SDP控制器联动，实现基于终端风险感知的动态鉴权，当终端安全风险不符合预先设定的策略时，能够对接入主体进行权限限制或强制下线等处置动作。  3、为综合应用平台社会化服务系统提供终端网络准入代理功能。  4、 产品包含软件规则库升级3年。  **其他要求见三、技术要求 （四）安全系统 章节** | | 台 | 1 |
| 19 | 准入访问控制系统 | 1、标准机架式机箱，冗余电源，国产化硬件平台；标准配置≥16G内存，系统盘≥64G，存储盘4T≥硬盘；标准配置6个10/100/1000M Base-TX；4个SFP千兆光口；2个扩展槽位；建议最大支持并发用户数6000个；  ▲1.支持与SDP安全网关和客户端组合联动，确保只有通过认证的主体才能接入SDP安全网关；支持多因素身份认证，包括口令、证书、动态令牌、UKEY等多种认证方式灵活组合，支持基于国密SM2算法的数字证书的身份认证，支持基于LDAP、Radius、CAS、Oauth协议标准的第三方认证平台；  2.支持终端风险感知的安全评估，能够联动SDP安全网关对不符合安全策略的接入主体进行权限限制或强制下线等处置动作。为综合应用平台社会化服务系统提供终端网络准入控制审核功能。  3.产品包含软件规则库升级3年。  **其他要求见三、技术要求 （四）安全系统 章节** | | 套 | 1 |
| 20 | 准入授权、UKEY | 终端电脑访问社会化服务系统时应进行设备认证；未通过认证的设备应阻断访问，车管所统一采购，社会机构直接使用 | | 个 | 1500 |
| 21 | 网络行为审计设备 | 国产化网络行为审计设备  1、性能参数：支持带宽≥1G；8\*vCPU,16G,吞吐量≥1G。为综合应用平台社会化服务系统提供网络审计功能。 2、具备主动发送少量探测报文，发现潜在的服务器（影子资产）以及学习服务器的基础信息，如：操作系统、开放的端口号等； 3、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、传输层协议以及标签类型（vlan、vxlan、mpls）选择添加抓包任务，接口额外提供标签选项，帮助安全工程师高效分析威胁；  4、产品包含软件规则库升级3年。  **其他要求见三、技术要求 （四）安全系统 章节** | | 台 | 1 |
| 22 | 数据库审计（含日志审计）系统 | 1、 性能参数：带宽性能≥500M。为综合应用平台社会化服务系统提供数据库审计功能，保护访问数据安全，支持对日志模糊化处理，防止数据的二次泄密。用户能自定义策略配置，支持风险监控、白名单、黑名单不同策略类型，监控级别能分为高、中、低风险。支支持主流数据库：Oracle、SQLserver、MySQL、DB2、MariaDB、SyBase、Informix、PostgreSQL、TeraData、Cache、HANA等，审计日志存储需达6个月以上。产品包含软件规则库升级3年  2、日志审计性能参数：包含资产授权数量(个)：≥50。  为综合应用平台社会化服务系统提供数日志审计分析功能。支持设置过滤条件规则，自动过滤无用日志，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，从而降低对网络带宽和数据库存储空间的占用。支持单条事件进行展开，显示事件详细信息和事件原始信息，事件详情中任意字段作为查询条件实现二次检索分析  3、产品包含软件规则库升级3年  **其他要求见三、技术要求 （四）安全系统 章节** | | 套 | 1 |
| 23 | 数据库备份一体机 | 1、硬件参数：规格：2U；CPU：2颗国产化CPU，主频≥2.7GHz（32C）；内存≥256GB DDR4 3200；系统盘≥480GB SATA SSD；全闪盘≥30.72TB SATA SSD；电源：白金，冗余电源；接口：4千兆电口+2万兆光口。  2、其他：数据库备份软件；万兆多模-850-300m-双纤\*2个;产品质保\*3年;软件升级\*3年; 软件功能：  1.为及时发现将来可能存在硬件问题，支持对超融合平台的硬件进行监控和大屏展示，包含CPU、内存、网卡、硬盘、存储、RAID等硬件健康检测，并提供相应异常检测项的恢复指导建议。  2.虚拟化软件应基于 KVM 开发，可维护性好，能够随着 Linux版本的升级而升级，部署时无需绑定安装OpenStack相关组件。  ▲3.虚拟化软件兼容 OpenStack Havana、Juno、Kilo、Mikata、Pike 等主流版本，并能提供标准接口实现与 OpenStack 平滑对接。  ▲4.支持对超融合平台的硬件进行监控和大屏展示，包含CPU、内存、网卡、硬盘、存储、RAID等硬件健康检测，便于及时发现问题并提供相应异常检测项的恢复指导建议。  ▲5.兼容现有市场上主流的存储阵列产品和存储协议，平台提供FC-SAN、iSCSI存储对接功能，便于对原有旧存储设备投资保护，不浪费以往IT投资。  ▲6.每个超融合节点出厂自带管理软件，设备上电后可登录任意一台来做超融合管理节点，提升集群冗余度，提升集群资源实用效率，所有节点全部通用（均作为计算、管理、存储、网络来实用），不限制节点使用场景。  **其他要求见三、技术要求 （四）安全系统 章节** | | 台 | 3 |
| **运行监控系统及网络配套设备** | | | | | |
| 24 | 运行监控系统 | 1、支持不小于200节点；  2、支持虚拟机安装环境；  3、支持国产化设备及系统；  4、支持链路故障预警功能；  5、支持设备故障预警功能；  6、支持国产金仓、达梦、神舟等数据库；  7、支持集中式、分布式部署和容器化部署；  支持SNMPV1/V2C/V3、Telnet、SSH、WMI、JMX、HTTP、JDBC/ODBC、ICMP、TCP/UDP、IPMI、NetConf、GRPC、ONVIF、SYSLOG、WinRM、SMI、RedFish、ZabbixAgent（可选）、vCenter等标准管理协议，实现对网络设备、存储设备、计算机、服务器、虚拟化、私有云、中间件、数据库、网络服务的一体化监控和管理。  **具体要求见三、技术要求 （五）安运行监控系统 章节** | | 套 | 1 |
| 25 | 核心交换机 | 1、总装机箱（交流电源≥2个，电源风扇≥2个，2个主控槽位，6个通用业务槽位）  2、交换容量≥312Tbps、包转发率≥11664Mpps/57600Mpps；  3、支持平台统一管理、统一查看状态、VLAN等配置管理；  4、支持框可视化管理；  5、主控板≥2个。  6、≥48端口千兆电（RJ45）;≥48端口千兆光（SFP），含光模块；≥8端口万兆光（SFP+），含光模块; | | 台 | 2 |
| **服务** | | | | | |
| 26 | 社会化服务系统部署及调试、测试 | **具体要求见三、技术要求 （一）统一版系统章节** | | 次 | 1 |
| 27 | 等保评测 | **具体要求见三、技术要求 （四）安全系统 7、等保测评 章节** | | 次 | 1 |
| 28 | 保障服务 | 系统建设完成并通过验收后，应提供不少于3年的运行保障服务，要求驻场工程师不少于2人，确保社会化服务系统的正常运行。服务包括：1、日常巡检，对设备运行状态的定期检查和保养维护；  2、故障排除：在规定时间内对系统出现异常情况进行检查维修；  3、技术培训：对甲方进行不少于20人/天的技术培训。  4、提供足够数量的维修备件，设备故障后必须先行替换备件，保证系统连续运行；  5、外挂系统接入，配合完成社会化服务系统外挂软件系统的接入工作。  投标人应提供详细的售后保障服务方案。 | | 项 | 1 |
| 其它 | | | | |  |
| 29 | 辅材、线材、附件 | 所有为完成本项目所必须的辅材、线材、附件均应在投标报价表中列明并记入投标总价，投标人应在投标文件中全部列出详细报价明细表。辅材、线材、附件均需满足国标、防火的要求。 | | 批 | 1 |

**本次招标设备供货和安装所需相关设备（包括但不限于以上分项所列设备）以及所有为完成本项目所必须的辅材、**线材、**附件均应在投标报价表中列明并记入投标总价，投标人应在投标文件中全部列出详细报价明细表。**

**2、 报价要求**

（1）、 投标人应在投标文件中列出本次招标所必需的设备器材详细清单，以及本项目实施过程中中所需的相关辅材、配件及所需的其它材料。

（2）、投标人应在投标文件中全部列出对应设备器材清单的详细报价表。

（3）、本项目实施所必备的而投标人没有列出的设备及服务内容均由投标人负责提供和完成，没有列出设备价格和工程费用的均视为包含在报价中，不另外增加费用。

### 三、技术要求

**（一）、统一版系统**

**统一版软件由公安部无锡科研所研发，中标人应在基本运行环境搭建完成后完成软件系统的部署、相关功能的调试、测试以及所有社会化服务机构的接入，所需费用包含在项目报价内。**

**1、社会化服务系统**

融合机动车登记、机动车查验、机动车检验审核，以及驾驶证管理、驾驶理论考试和驾驶人场地、道路驾驶技能考试管理等业务服务功能。业务办理过程、结果信息交换汇聚至综合应用平台，生成电子签名、电子签章等信息，提升公安交管档案电子化应用水平。包括但不限于以下部分内容：

1. 专网部分基础软件环境安装

oracle数据库软件安装、数据库系统参数优化、操作系统参数调优。

数据库基础数据初使化，部局业务软件SQL语句优化测试。

分布式文件系集群软件安装部署、文件集群参数优化、集群性能测试、集群功能测试。

redis内存数据库软件安装、系统参数优化。

HA-PROXY MQ负载均衡组件安装与参数调优。

rabbit MQ 消息队列组件安装与参数调优。  
（2）公安网部分基础软件环境安装服务

oracle数据库软件安装、数据库系统参数优化、操作系统参数调优。

数据库基础数据初使化，部局业务软件SQL语句优化测试。

分布式文件系集群软件安装部署、文件集群参数优化、集群性能测试、集群功能测试。

redis内存数据库软件安装、系统参数优化。

HA-PROXY MQ负载均衡组件安装与参数调优。

rabbit MQ 消息队列组件安装与参数调优。

（3）专网应用软件安装调试与软件备案服务

专网业务系统数据库数据初使化。

web中间件安装与参数优化。

注册中心组件安装优化。

内部、外部与前端网关组件安装与参数优化。

跨网交换服务组件安装与测试（实现与公安网的数据、图片及文件交换）

系统管理组件服务安装与优化。

系统定时任务组件服务安装与功能测试。

公安服务组件安装服务与优化。

驾驶证管理业务组件安装与优化。

驾驶人考试业务组件安装与优化。

机动车查验与登记组件安装与优化。

机动车检验组件安装与优化。

协助用户共同完成以应用软件安装登记备案与软件初使化操作。

**2、跨网交换服务系统**

基于公安信息通信网边界接入平台，提供统一的公安网和社会化服务网络的数据交换服务。

**3、终端设备管理软件**

安装发布在用户终端电脑上，实现9500打印机、高拍仪、读卡器、条码枪、电子签名板、扫描仪等外接设备的集中配置管理。

**4、理论考试桌面软件**

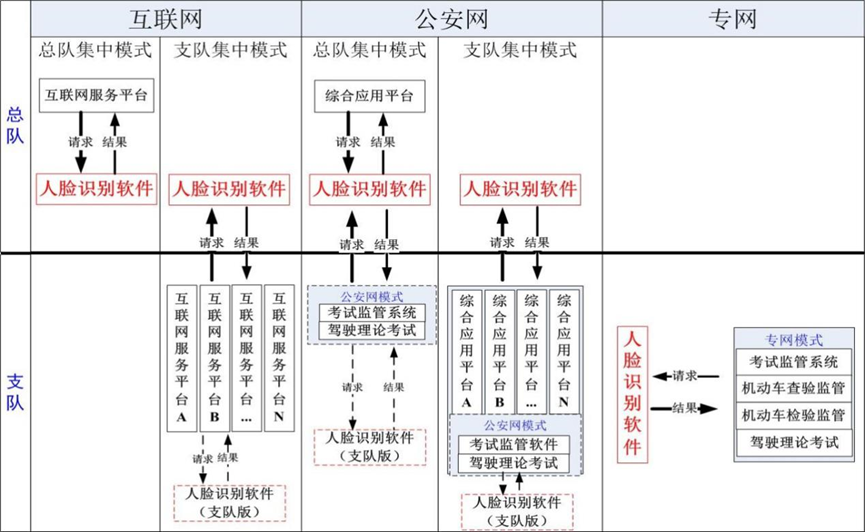
安装发布在理论考场考台终端电脑上，通过考台安全检测、考前人脸比对加强考试过程安全。

**（二）、自建系统**

**1、人脸比对服务**

按照《公安交通管理综合应用平台和互联网交通安全综合服务管理平台人脸识别技术支撑服务系统建设要求》建设人脸识别支撑服务系统，实现社会化服务专网驾驶人考试、自助处理、业务办理窗口等业务场景的人证一致性身份比对能力，提高交管业务监管水平和民警工作效率。

（1）系统架构



（2）系统功能

人脸识别支撑服务系统具备人脸检测、特征提取和人脸识别等能力，支持1:1人脸照片比对能力。

（3）应用场景

人脸识别支撑服务系统主要应用于社会化服务专网的查验终端查验员身份核验、驾驶人考试考前身份核验以及业务办理窗口的人证一致性核验等业务场景。

**2、时钟同步系统**

在社会化服务网络部署统一的时钟同步服务器系统，确保各系统及前端设备的时钟一致性。

**（三）、社会化服务系统统一版运行环境搭建**

**1、统一版运行环境**

统一版社会化服务系统由公安部无锡科研所采用微服务架构设计研发，为满足其功能要求，应采用具备计算虚拟化、存储虚拟化、网络虚拟化、网络安全虚拟化（含分布式防火墙与虚拟机版网络安全设备）功能的超融合架构服务器进行应用微服务架构承载环境的搭建，本项目规划8台国产化超融合架构服务器实现在满足现有资源需求的同时满足未来数据增量的业务承载并且满足信创国产化需求。

**2、文件存储**

根据公安部《公安交通管理综合应用平台社会化服务系统升级改造技术方案》，图片和视频存储采用文件系统存储，需安装fastDfs。文件系统所需服务器应使用物理机，机器数量2台，并可以根据实际数据情况适当扩容，扩容时应保持服务器数量为偶数台。

**（四）、安全系统**

**1、整体安全建设**

本次安全设计参照公安部最新颁发的《公安交通管理综合应用平台社会化服务系统升级改造技术方案》和《公安交通管理综合应用平台社会化服务系统升级改造指导意见》以及省交警总队针对综合应用平台社会化服务系统升级改造的具体通知以及部局建设要求中明确提到的“社会化服务系统建设应当符合《计算机信息系统安全保护条例》（国务院令147号）、《信息安全等级保护管理办法》（公通字〔2007〕43号）、《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）、《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）等文件规定，按照网络安全等级保护三级开展安全设计”内容等进行设计。主要包含边界安全设备（下一代防火墙，WEB应用防火墙，IPS入侵防御设备）、链路接入及访问控制设备（零信任直连网关、零信任访问控制系统）、审计类安全设备（日志审计、数据库审计、行为审计设备、堡垒机）、威胁检测类设备（流量分析探针、安全管理平台、漏洞扫描）以及终端安全设备。

整体安全建设应从车管所数据中心安全、联网机构安全准入两方面开展。整体安全建设而应该符合以下要求：

|  |  |  |
| --- | --- | --- |
| 数据存储安全 | 符合部所要求 | 采用加密算法保证数据存储的机密性和完整性，防止信息泄露和篡改 |
| 服务器安全 | 分域管理 | 防火墙 |
| 堡垒主机审计系统 |
| 自动化安全检测装置 |
| 行为审计流量分析系统 |
| 流量采集探针 |
| 安全网络综合管理平台 |
| 主机安全防护 | 防火墙和杀毒软件（EDR） |
| 网络安全 | 边界安全 | 公安信息网边界接入平台-数据边界 |
| 通用防火墙（FW）（需开通防病毒模块或为防毒墙） |
| WEB应用防火墙（WAF）（推荐放在服务器防护，此处不许单独部署） |
| 链路接入安全 | 终端准入认证SDW-R或零信任直连网关DGW |
| 网络访问控制 | 代理车管所业务系统，实现安全防护 |
| 确保接入终端电脑经认证鉴权后才能访问社会化服务网络资源，基于先认证后连接架构，收敛暴露面，抵御未授权连接 |
| 配备IDS入侵检测系统、恶意代码防护等安全产品 |
| 应用安全 | 鉴别授权 | 统一版软件平台实现 |
| 数据访问安全 | 统一版软件平台实现 |
| 操作日志审计 | 统一版软件平台实现 |
| 应用安全防护 | WEB应用防火墙（WAF） |
| 终端电脑安全 | Ukey硬件管控模块 | 电脑终端Ukey采购与分发 |
| 设备认证 | 零信任用户端 |
|  |  |
| 审计管理 | 日志信息进行记录和安全审计 | 数据库审计 |
| 日志审计 |

**2、边界接入平台设备更新**

（1）、概述

目前社会化服务系统在用的边界接入平台（社企链路）由支队于2016年建设，部署于支队科技处通信机房。为保证社会化服务系统升级改造后安全稳定运行，需对该边界链路中的防火墙、安全网关、入侵检测系统、数据交换系统、网闸等设备进行升级，替换为万兆链路，满足将来日益增长的业务需求。

**投标人需承诺，边界接入平台到货安装后，须在一个月内通过公安部安全与警用电子产品质量检测中心的检测，并获得检测报告。逾期每延迟一天，扣除合同总金额的1/1000。**

（2）、功能描述

边界接入平台划分为5个逻辑区域，分别是路由接入区、边界保护区、应用服务区、安全隔离区以及安全监测与管理区。

（3）、边界保护区

边界保护区主要设备包括：防火墙、可信边界安全网关、三层交换机、入侵防御系统等。

**防火墙**

防火墙的首要功能是根据数据包的源地址、目标地址、协议类型、源端口、目标端口以及网络协议等对数据包进行访问控制。防火墙还保证了边界接入平台内部的主机地址不被外部终端直接获得。

**可信边界安全网关**

可信边界安全网关对社会企事业单位接入终端进行身份认证，保证未通过身份认证的接入终端不能进入平台访问，还保证在网络传输过程中，接入终端与边界接入平台之间的通信内容全程加密。

**三层交换机**

利用三层网络交换机的IP路由和虚网功能，根据接入应用进行路由选择和虚网划分，保证不同业务应用通道之间的相互隔离。

**入侵防御系统**

入侵防御系统(IPS)部署在可信边界安全网关之后，其目标旨在准确监测网络异常流量，自动对各类攻击进行实时阻断。自动拦截黑客攻击、蠕虫、网络病毒、DDoS等恶意流量，使攻击无法到达目的主机。

（4）、应用服务区

根据实际业务需求，应用服务区放置了相应业务应用的前置服务器（包括应用服务器、WEB服务器、数据库服务器、文件服务器等）。作为外部终端网络连接的终点，提供给终端用户应用代理、数据暂存等功能服务。

本项目社会化服务系统统一版跨网交换系统独立部署在可信服务区。

（5）、安全隔离区

**安全数据交换系统**

安全数据交换系统由两台专用的数据交换服务器组成，根据业务配置建立业务数据通道，并对业务数据通道上传输的数据进行过滤和审计。只允许符合安全策略的业务数据进行交换，不允许任何其它的数据传输，设备应具备抗脆弱性扫描能力 。

具体描述如下：

**身份认证**

系统内部通过硬件数字证书进行双向身份认证，如果一旦系统内部的硬件数字证书被拔走，则数据交换过程马上终止。如果外网端其他服务器冒用地址向内网发送数据交换请求，则直接会被系统拒绝。

**数据加密**

系统根据认证产生的会话密钥对传输数据进行加密。

**区分内外网链路**

系统能够自动区分连接内外网链路的不同接口，外网接口保证数据源的合法性和数据的完整性，内网接口对数据进行检查、过滤、审计和分发等处理。

**单向通道主动获取数据**

采用单向通道技术，确保除了所配置的接入业务以外，没有任何其它软件能够利用数据通道传输数据或自行建立数据传输通道。

系统主动获取前置机上数据，所有数据请求都由内网交换服务器主动发起，根据用户事先定义的业务调度策略进行调度，每个业务在配置完成后即形成该业务的隧道，系统不接受前置机向系统发起的主动数据提交请求。

**验证数据源**

系统支持对前置机硬件设备证书双向认证，系统可以兼容各种证书体系所颁发的标准X.509证书。

**数据过滤**

系统能够根据用户事先定义业务规则对数据进行全面过滤，支持对每个业务单独设置过滤规则，过滤规则粒度细化到每个字段，包括类型、范围、长度、枚举、缺省值、特殊字段、字符编码、图像字段许可等等。

具备数据防泄漏安全功能：通过配置过滤规则，可防止关键内容、指定文件格式非法泄露，文件同步功能具备数据防泄漏功能；数据库同步功能具备数据防泄漏功能，设置数据库的列、内容格式（身份证号码）、字段长度、枚举值（内容关键字）和数字范围进行数据库同步过滤，可替换数据库记录内容信息（列转换）、过滤掉敏感关键字内容防止敏感信息泄路。

**审计与行为追溯**

系统提供对整个数据交换行为的完整审计，包括数据来源、交换发生时间、数据交换的目标、数据交换的内容、是否得到了授权、是否遵守交换规则、交换行为是否成功、交换结束时间等等。

**网闸**

通过网闸切断所有基于网络协议的连接，使外部终端无法直接访问公安信息网，确保公安信息网与外部网络隔离。对所有过往的流量都剥离通信协议，保证所有协议剥离和再生过程都接受安全审计，并且具有防范各种网络协议攻击的能力（如DDOS、LAND、滴泪攻击等）。

（6）、安全监测与管理区

安全监测与管理区内包括：集中监控与管理系统（简称集控系统），集中监控与管理系统由集控系统服务器和集控探针组成。

**集控探针**

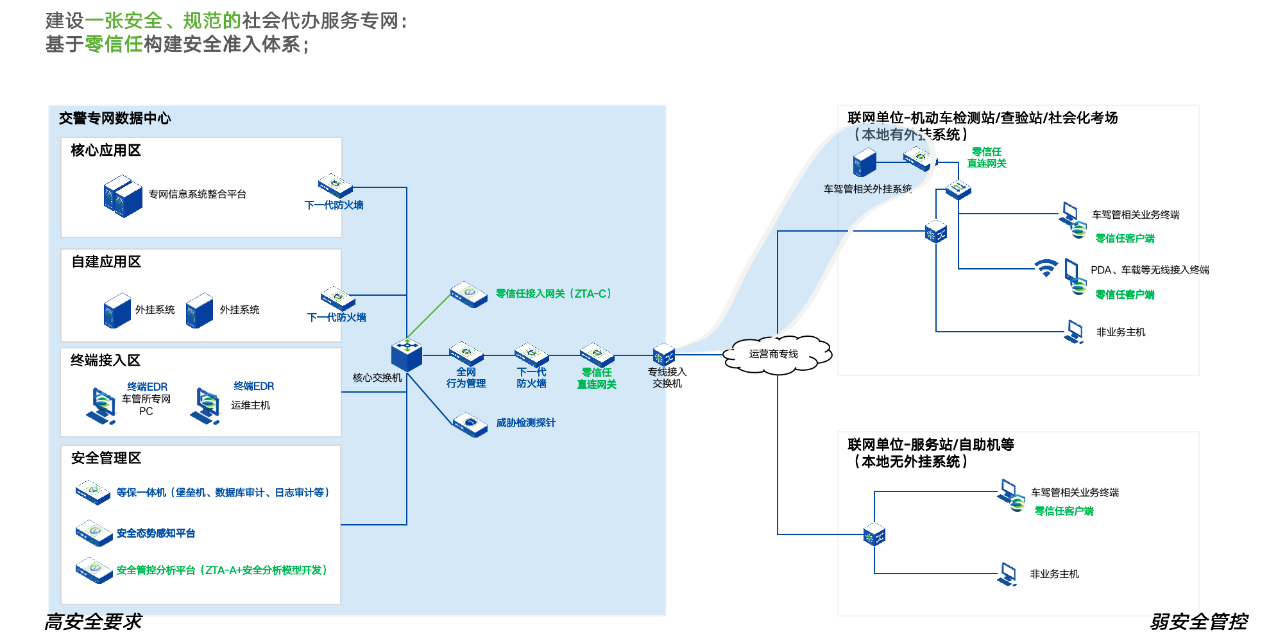
集控探针采集外网各种设备（如防火墙、三层交换机、可信边界安全网关、IDS、外网交换服务器、各种业务前置机）的日志信息，同时监听外网设备的使用状态、流量、异常报警事件等。

**集中监控管理系统**

集控系统功能包括：注册信息管理功能、运行监控管理功能、报警管理功能、安全审计功能。

**3、安全访问控制**

由于社会化服务系统涉及公安部门、社会化考场、检测站、4S店等众多单位，网络环境复杂，网络安全管理压力较大。配备网络安全准入和访问控制模块，确保接入终端电脑经认证鉴权后才能访问社会化服务网络资源，基于先认证后连接架构，收敛暴露面，抵御未授权连接。未经认证鉴权的接入终端不能与受控网络/资源建立任何连接。外部不能扫描到任何受控网络/资源地址；配备IDS入侵检测系统、恶意代码防护等安全产品，实现网络信息传输监控和检测，及时发现不正常或是具有伤害性的信息传输行为。



**4、服务器安全**

（1）、分域管理

社会化服务系统和自建系统应当实行数据库和应用服务器的集中管理，实施严格的分域管理。选择堡垒主机审计系统、自动化安全检测装置、行为审计流量分析系统、安全网络综合管理平台等加强运维管理安全，如下图所示：



按照社会化服务系统的技术架构和管理需求，将社会化服务系统划分为数据域、应用域、访问域、用户域和管理域等不同的安全域。数据库域只对应用域、管理域开放；应用域只对访问域和管理域开放；用户域只能连接访问域，通过Ngnix负载均衡对外开放的端口访问应用软件。通过防火墙实现各域间的网络访问控制。

基于微服务架构优势，服务区分域管理可采用分布式防火墙，与安全组件来实现内生安全建设。

（2）、主机安全防护

社会化服务系统应用服务器、数据库服务器应当安装防火墙和杀毒软件，具备漏洞扫描、病毒检测、安全基线检查、恶意代码检测、违规外联检测等安全能力；具备运行信息实时采集能力，采集的信息应当包括进程、服务、命令行、外设信息等。具备恶意行为检测能力，对进出WEB服务器的流量进行实时检测、分析，阻断攻击应用的行为。

**5、终端安全**

社会化机构用户通过终端电脑登录使用社会化服务系统应当使用全国统一的电脑终端Ukey硬件管控模块，用于用户身份鉴权和终端电脑安全检测。Ukey硬件管控模块内置安全检测软件，开机自启、定时对终端电脑进行安全检测、实时将检测结果上传社会化服务系统，对于检测有异常的，将自动阻断该用户使用社会化服务系统。安全检查内容包括：是否连接互联网、是否使用非法外挂（爬取数据）、是否开启远程桌面、操作系统补丁升级、杀毒软件安装等方面。终端电脑访问社会化服务系统时应进行设备认证，认证方式可采用MAC/IP绑定、硬件特征码、设备证书等，未通过认证的设备应阻断访问。

**6、数据安全**

（1）、社会化服务系统在建设和使用过程中，对个人身份敏感信息和重要业务数据采用国密加密算法保证数据存储的机密性和完整性，防止信息泄露和篡改。系统所采用密码产品及密码技术应当遵循密码局相关要求。对涉及个人信息的姓名、出生日期、身份证明号码、特定身份、生物识别信息、住址、联系电话、行踪轨迹等，信息应当依据“最小范围”、“最短保存期限”和“分类处理”的原则，采取加密存储、安全校验、定期清理等技术手段，防止信息泄露。

（2）、数据库审计

数据库审计系统能够对业务网络中的各种数据库进行全方位的安全审计，具体包括：

数据访问审计：记录所有对保护数据的访问信息，包括文件操作、数据库执行SQL语句或存储过程等。系统审计所有用户对关键数据的访问行为，防止外部黑客入侵访问和内部人员非法获取敏感信息

数据变更审计：统计和查询所有被保护数据的变更记录，包括核心业务数据库表结构、关键数据文件的修改操作等等，防止外部和内部人员非法篡改重要的业务数据

用户操作审计：统计和查询所有用户的登录成功和失败尝试记录，记录所有用户的访问操作和用户配置信息及其权限变更情况，可用于事故和故障的追踪和诊断

违规访问行为审计：记录和发现用户违规访问。支持设定用户黑白名单，以及定义复杂的合规规则，支持告警。

（3）、数据库业务系统备份设计

统一版社会化服务系统完成建设以后，将部署在西安市公安局交通警察支队车辆管理所五龙机房，为了保证机动车检验业务与驾驶人考试监管系统（科目二三）的正常运行，保证数据可靠性，计划针对机动车检验业务与驾驶人考试监管系统（科目二三）的核心数据库进行备份设计。当数据库系统出现故障时，可在数据库备份平台上对于数据库系统进行拉起恢复，保障业务进行正常的数据库读写操作。目前需要进行备份的数据库主要有两套，一套运行驾驶人考试监管系统的数据库业务，一套运行机动车检验业务的数据库业务，共四台数据库服务器，共计CPU核数160核、内存512G内存、55TB的可用容量，数据日增量为每天65GB。考虑到未来三年业务的持续增长，将预留一部分资源承载后续增量业务。采用3台数据库备份一体机实现在满足现有资源需求的同时满足未来数据增量业务的承载。

**7、等保测评**

中标人应按照等保三级的安全标准建设社会化服务系统配套的安全产品（包括但不限于本招标文件所要求的产品），建立相应的安全运维管理机制，组织进行等保三级评测，并在系统正式上线运行前取得等保三级证书并完成相关备案。

**（五）、运行监控系统**

一个平台实现全链路、联网设备的统一监控、告警及展现，支持分布式部署统一管理，各子系统间的数据关联共享，故障快速定位和告警，从全局视角把控系统运行态势，实现社会化服务系统的基础设施展示、通信实时状况展示、终端设备应用状态展示、系统服务及组件状态展示等功能。

**1、链路状态实时追踪**

实现从前端到后端全链路自动标记和追踪和深度诊断自动关联调用链，识别性能奇点，实现问题深度诊断，并清晰地给出关键性结论，更加方便用户去做分析和判断。

**2、全面数据采集及服务监测**

支持采集Metric、Log、Trace、事件、拓扑结构、元数据、用户会话等并将其转化为规范化的数据体系。

无需人工配置，自动从观测数据获得IT系统架构关联关系，实时更新并展示拓扑和关联关系。将代码、拓扑信息与元数据结合，提供完整的全样本全链路调用链追踪，以更快地了解每个微服务的执行情况，定位发生问题的位置。

可监控各类 Windows、Linux、UNIX等服务器系统运行状况，包括国产系统。

可对所有支持管理口IPMI及SNMP协议的服务器硬件进行监控，支持浪潮、华为、联想、曙光、紫光、华三等国内厂商通过管理口IPMI及SNMP获取硬件状态指标。

可监控各种类型的交换机、路由器、负载均衡、网关设备和其他启用了SNMP协议的网络设备。

支持对主流存储设备、磁盘阵列、磁带库以及分布式存储系统进行状态以及性能信息监控，包括华为、浪潮、曙光等国产设备。

可对业务系统的运行状况进行监控，包含系统服务、组件、会话、端口、进程等运行情况展示。

**3、智能数据分析**

从时间线和业务线上进行数据关联，随时随地从用户会话或者指标追踪到日志和链路，从链路追踪到代码堆栈和错误，从代码堆栈再到实体，从任意实体查看其上下游调用和纵向依赖，实现从宏观到微观的全局洞察。

**（六）、网络配套升级改造**

当前西安支队科目二、三考试专网与查验检验专网并没有联通，原有核心交换机提供的交换背板容量不足，不能满足构建公安交通管理综合应用平台社会化服务系统一体化社会服务数据中心要求。

本次计划一是采用千兆数字链路将科目二科目三考试专网与查验检验专网打通，二是更换核心交换机2台，三是满足网络带宽对业务应用处理需求。

### 四、服务要求

**（一）、****技术团队人员职责要求**

1、项目总负责：提供1名项目总负责，负责项目的总体协调工作。

2、项目经理：提供1名项目经理，主要负责项目整体的质量、进度、成本、风险进行管控，项目重大技术问题攻关及资源协调等工作。