密码监督管理信息平台（一期）

软硬件集成技术需求说明书

**国家密码管理局商用密码检测中心**

**2019年3月**

**目 录**

[一、项目概述 1](#_Toc5200649)

[二、项目前期情况 1](#_Toc5200650)

[三、安全集成总体要求 2](#_Toc5200651)

[四、采购内容 3](#_Toc5200652)

[五、硬件设备技术参数要求 4](#_Toc5200653)

[六、信息平台安全需求 12](#_Toc5200654)

[6.1网络安全需求 12](#_Toc5200655)

[6.1.1安全域设计 13](#_Toc5200656)

[6.1.2区域边界安全防护 13](#_Toc5200657)

[6.1.3网络防病毒 14](#_Toc5200658)

[6.2数据安全需求 14](#_Toc5200659)

[6.2.1数据安全防护需求 14](#_Toc5200660)

[6.2.2数据备份与恢复需求 15](#_Toc5200661)

[6.3应用安全需求 15](#_Toc5200662)

[6.4安全管理体系建设需求 15](#_Toc5200663)

[6.5安全维护需求 16](#_Toc5200664)

[6.6可靠性需求 16](#_Toc5200665)

[七、集成建设实施要求 16](#_Toc5200666)

[7.1实施总体要求 16](#_Toc5200667)

[7.2项目管理和实施计划要求 17](#_Toc5200668)

[7.3质量保证及风险管理要求 17](#_Toc5200669)

[7.4提交成果要求 17](#_Toc5200670)

[7.5验收要求 18](#_Toc5200671)

[7.6工期要求 18](#_Toc5200672)

[八、培训与技术支持 18](#_Toc5200673)

[8.1系统培训 18](#_Toc5200674)

[8.2售后服务及技术支持 19](#_Toc5200675)

# 一、项目概述

密码监督管理信息平台是提高商用密码材料审批效率的重要信息化手段。为了向全国的商密企业及省商用密码管理部门提供优质、高效、规范的服务，2015年初启动了密码监督管理信息平台（以下简称“信息平台”）建设工作，由于信息平台建设经费为分期拨付。为了不影响整体项目建设进度，将信息平台建设（一期）分两步完成，第一步，完成信息平台软件开发并搭建模拟测试环境；第二步完成信息平台通用软硬件采购、软硬件系统安全集成及平台部署。

信息平台将要与全国一体化在线政务服务平台进行对接，深入推进“互联网+政务服务”，努力将此平台建成具有高安全性、高可靠性、技术先进、信息统一发布、审批材料便捷的信息平台，为上报、审批及进度反馈提供安全通道。

# 二、项目前期情况

前期主要完成密码监督管理信息平台的软件定制，已经完成5个处室，13个业务模块的设计与开发。运用先进的信息科技手段，结合全国商用密码实际业务需求，搭建面向全国商密企业及相关管理部门的密码监督管理信息平台，实现政务公开，提高政府审批效率，降低审批成本，满足内部管理和对外服务要求。

目前密码监督管理信息平台的软件定制部分已完成，并完成了此平台的演示环境搭建。模拟环境示意图如下：



前期项目已采购软硬件设备清单如下：

|  |  |  |  |
| --- | --- | --- | --- |
| 货物名称 | 型号及规格描述 | 单位 | 数量 |
| 应用及数据库服务器 | 曙光天阔I840-G10，4U机架式服务器配置：Xeon E5-4607×2/8G DDR3×2/300G 2.5吋10K转SAS×3/曙光1G Cache SAS RAID卡×1/超薄DVD-RW×1/1000W电源模块×2、双千兆网卡，支持32位和64位的Windows/Linux操作系统，提供5年免费上门原厂质量保证与售后服务。含瑞星杀毒软件服务器版for linux。 | 台 | 4 |
| 签名验签服务器 | 三未信安SRJ1203 | 台 | 1 |
| 交换机 | （华为5700S－52P－LI）三层千兆交换机 | 台 | 2 |
| 数据库 | 南大通用安全数据库管理系统（GBase 8S V8.3.1.6 无限用户数） | 套 | 2 |
| 服务器操作系统 | 中标麒麟高级服务器操作系统软件(NeoKylin Linux Advanced Server V6.0版) | 套 | 4 |

# 三、安全集成总体要求

信息平台安全建设总体要求：

本次信息平台（一期）按照信息安全等级保护三级的要求建设。本次信息平台安全集成要从应用部署、数据存储等方面充分考虑系统的部署及访问的安全性，从而保证信息平台运行的连续性及高可用性。在系统的各个层次都必须消除单点隐患。在硬件方面，通过冗余配置加以保障。

建设密码监督管理信息平台需制定完备的安全策略和应急预案，加强安全技术和手段的应用，信息平台具备对网络攻击、病毒入侵、系统故障等风险的安全防范和应急处置能力，建立故障检查、告警和应急处理机制，保证数据不因意外情况丢失或损坏。

# 四、采购内容

| **序号** | **名称** | | | **参考品牌** | | **数量** | **技术参数要求** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **软件采购内容** | | | | | | | |
| 1 | 通用软件 | | 操作系统 | 国产 | | 6 | 企业版国产操作系统，要求详见第四章（1） |
| 2 | 数据库 | 国产 | | 2 | 要求详见第四章（2） |
| 3 | 双机热备软件 | 国产 | | 4 | 要求详见第四章（3） |
| 4 | 防病毒软件 | 国产 | | 2 | 要求详见第四章（4） |
| **硬件采购内容** | | | | | | | |
| 5 | 服  务  器 | | 应用服务器 | | 国产 | 2 | 四路机架式服务器，技术参数要求详见第四章（5）①。 |
| 6 | 数据库服务器 | | 国产 | 2 |
| 7 | 防病毒服务器 | | 国产 | 2 | 双路机架式服务器，技术参数要求详见第四章（5）②。 |
| 8 | 签名验签服务器 | | 国产 | 1 | 技术参数要求详见第四章（5）③。 |
| 9 | 安全设备 | | SSL VPN | | 国产 | 2 | 技术参数要求详见第四章（6）①。 |
| 10 | 防火墙 | | 国产 | 2 | 技术参数要求详见第四章（6）②。 |
| 11 | 防病毒网关 | | 国产 | 1 | 技术参数要求详见第四章（6）③。 |
| 12 | 网闸 | | 国产 | 1 | 2U机型，技术参数要求详见第四章（6）④。 |
| 13 | USBKEY+证书 | | 国产 | 100 | 采购100个第三方CA证书含USBKey，技术参数要求详见第四章（6）⑤。 |
| 14 | 网络安全审计系统 | | 国产 | 2 | 技术参数要求详见第四章（6）⑥。 |
| 15 | 入侵检测系统 | | 国产 | 2 | 技术参数要求详见第四章（6）⑦。 |
| 16 | 网络设备 | | 负载均衡 | | 国产 | 1 | 技术参数要求详见第四章（7）①。 |
| 17 | KVM | | 国产 | 2 | 含显示器和键盘，技术参数要求详见第四章（7）②。 |
| 18 | 交换机 | | 国产 | 4 | 三层千兆交换机，技术参数要求详见第四章（7）③。 |
| **其他采购内容** | | | | | | | |
| 19 | | 集成费用 | |  | | | |
| 20 | | 培训费用 | | 全国相关用户集中培训一次相关费用 | | | |
| 21 | | 安全评估费 | | 专家安全评审等相关费用 | | | |
| 22 | | 等级保护测评费 | | 公安部信息安全产品检测中心信息安全等级保护三级测评 | | | |
| 备 | |  | |  | | | |

# 五、硬件设备技术参数要求

该信息平台建设所需要的软硬件设备有：操作系统、数据库、双机热备软件、防病毒软件、服务器设备、安全设备、网络设备。应确保安全产品的采购和使用符合国家的有关规定，应确保密码产品的采购和使用符合国家密码主管部门的要求，使用符合国家密码管理规定的密码技术和产品，满足信息系统安全等级保护三级测评要求。

（1）操作系统

国产操作系统，需要满足以下性能指标：需要支持x86-64位架构；需兼容国内外主流的软件产品，获取国外Oracle、vmware、veritas厂商的双方认证；产品需要符合GB18030-2005标准、CGL5.0标准；兼容主流国产数据库产品；兼容Oracle Tuxedo、中创Inforsuite、金蝶Apusic、东方通TongWeb等中间件产品；兼容国产主流热备软件；支持国密算法，可将国产密码用于数据安全，如身份认证、访问控制、安全机制、备份还原等；**需要与已定制开发完成的密码监督管理信息平台做适配。**

（2）数据库

国产数据库，采用当前最成熟技术的数据库管理系统产品，并符合未来数据库技术的发展潮流；支持与原业务系统做适配；支持当前最流行的数据库技术标准，如：ANSI/ISO SQL-92；支持开发接口：ODBC 3.5、JDBC 3.0、ADO.NET、C API；支持字符型数据如nchar数据类型、nvarchar数据类型、text数据类型；支持数值型数据如int数据类型、float数据类型；支持时间类型数据如DATE 数据类型、DATETIME 数据类型；支持大对象数据,如blob数据类型,clob数据类型；产品需支持国密标准及算法要求，并满足《安全数据库产品密码检测准则》，需取得《密码检测证书》；必须完全支持中文国家标准的中文字符，如GB2312、GBK、UTF-8等；产品需获得《商用密码产品型号证书》，**需要与已定制开发完成的密码监督管理信息平台做适配。**

（3）双机热备软件

支持Windows、Linux、Unix等操作系统；支持磁盘镜像保护模式，提供简单的图形化配置及出错向导式处理；支持多种心跳模式；支持B/S管理界面，提供高可用集群资源、节点配置管理、监控及模板配置管理、图形化的系统性能状态查看及监控报表、系统主要事件审计、告警查看等功能；需要与采购的国产操作系统有良好的适配性性；产品需为发行的国产HA软件；具有软件产品登记证书和著作权证书。

（4）防病毒软件

企业网络版2套，每套包含1个控制中心+服务端10个+客户端100个，支持Windows、Linux操作系统，能对采购的国产操作系统有较好的支持性，适应多操作系统的复杂网络环境；支持管理员c/s架构远程管理；提供病毒趋势分析和报表系统；可自动或手动执行漏洞扫描及修复；支持多级管理模式。支持文件、引导区、内存、注册表、服务、进程、进出文件、目录、压缩文件、网页等恶意代码、恶意样本查杀。支持私有云查杀，具有百亿级云查病毒库，预置至少2亿黑名单及2000万全面的白名单，支持黑白名单方式，支持txt批量导入方式；文件被加入白名单，客户端不再查杀，加入黑名单，客户端不可执行此文件；终端威胁统一到控制中心查询黑白并进行查杀；支持扫描发现文件遭破坏或被感染时触发修复流程；支持在线或离线对服务器升级，可升级病毒库、补丁库等；可管理终端灰度升级，此外可定期清理系统日志；具备相关资质文件，包括但不限于公安部计算机信息系统安全专用产品《销售许可证》；产品必须为厂商独立自主研发，并获得《计算机软件著作权登记》证书。

（5）服务器设备

根据服务器的用途不同将服务器分为WEB应用服务器、数据库服务器、防病毒服务器和签名验签服务器。

①WEB应用服务器和数据库服务器采用高配设备；四路机架式服务器，X86架构处理器，CPU总核心数≥32核，主频大于2.0GHz，4\*8G内存，热插拔SAS\*3硬盘，每颗CPU三级缓存≥32MB，支持≥32个内存插槽，最大可支持4TB内存容量；配置热插拔1+1冗余电源；并支持Raid5，双万兆网卡；支持U盘软驱、DVD光驱，支持32位和64位的当前主流Windows/linux操作系统，含配套导轨。

②防病毒服务器，双路机架式服务器，2核 CPU，主频大于2.0GHz，8G内存，热插拔SATA/SAS\*3硬盘，支持Raid5，双千兆网卡，冗余电源，支持32位和64位的当前主流的Windows/linux操作系统，含配套导轨。

③签名验签服务器，应取得商用密码产品型号证书，符合《签名验签服务器技术规范》要求，提供基于数字证书的身份认证服务、数据签名与签名验证服务、加解密服务和数字信封服务；支持Windows、Linux、AIX等主流应用平台；支持Java、COM、C等应用集成接口；至少支持SM2算法的数字签名功能，提供对数据、消息、文件等多种格式的运算方式。硬件规格：1U； SM2签名速率不低于400次/秒，SM2验签速率不低于100次/秒，签名验签服务器的平均无故障工作时间应不低于20000h。

（6）安全设备

安全设备包括SSL VPN、服务器密码机、防火墙、WEB应用防护、USBKEY+证书。

①SSL VPN应经国家密码管理局批准并取得商用密码产品型号证书，符合《SSL VPN技术规范》要求。支持GUI和WEB两种界面，支持集中管理和统一密码设备监控功能，算法用硬件（加密卡）实现，能够实现管理人员远程接入并管理的网络互联需求，同时对远程网络中传输的数据提供私密性、完整性等安全防护。支持进行操作系统、文件、进程、注册表、用户接入IP、登录IP、登录时间、接入终端等规则的易用性“与或”组合进行登录前和登录后的客户端安全检测，可配置准入和授权策略。具有系统配置、策略配置管理、日志管理、状态检测等功能；要求加密速率不低于100Mbps，并发SSL用户数不低于300，标准1U设备,双冗余电源，≥8个10/100/1000M Base-TX；≥4个SFP光口插槽；整机吞吐≥4G，最大每秒新建连接数≥4万；最大并发用户数≥2000。

②防火墙设备，具备2U机箱，硬件采用模块化设计，要求至少具有3个接口板扩展槽位，可支持千兆接口；配置4个千兆光口（含模块）和12个千兆电口，要求具有独立的管理接口与双机HA接口；网络吞吐≥12Gbps；并发连接≥280万；支持路由模式、交换模式、混合模式、虚拟线模式，至少支持四对虚拟线配置；支持主备、负载均衡及连接保护多种高可用机制；要求系统平台具有良好的功能扩展性，可扩展支持SSL VPN、入侵防御、病毒防御、URL分类过滤、应用识别等安全功能模块，具有《计算机信息系统安全专用产品销售许可证》（千兆），《信息安全产品EAL4+等级认证证书》。

③防病毒网关，标准2U设备，具有检测出网络上的病毒入侵行为、违反安全策略的行为及各种突发的异常现象，并将相关事件记录到数据库中，作为管理员事后分析的依据，具有强大的日志及报表功能。要求双冗余电源，10/100/1000M Base-TX口≥6个；SFP光口插槽≥2个；吞吐量≥1.2GB；最大吞吐量3.5G；最大并发连接数≥200万；病毒库≥600万；支持多系统（≥3个）引导，并可配置启动顺序；支持系统分区备份，支持将系统A克隆至系统B；支持多个系统配置文件，可导入导出恢复配置；多系统设置可在Web界面上完成全部操作；支持IPv4和IPv6双栈协议下的病毒扫描与防护；支持隔离病毒源地址，防止病毒源主机访问内部网络，提高网络整体安全性；采用自有知识产权的病毒防护引擎（提供相关专利证明）；支持双防病毒引擎（标准引擎和增强引擎），杀毒强度可控，支持快速扫描、全面扫描模式；具有相关的资质文件，包括但不限于《计算机信息系统安全专用产品销售许可证》（增强级）、具备网关级计算机网络病毒的防范的相关证明、《信息安全产品EAL3+等级认证证书》。

④网闸：采用“2+1”系统架构，即由两个主机系统和一个隔离交换专用硬件组成；内外网主机各配置≥4个10/100/1000M自适应电口，≥4个千兆SFP光口，1个10/100/1000M Base-TX管理接口，1个10/100/1000M Base-TX HA接口（双机热备口）；系统吞吐量≥750Mbps；并发连接数≥6万；1个RJ45 CONSOLE口；内、外网主机系统分别采用冗余双系统启动模式，当A系统运行失败后，能从B系统启动，且A、B系统可互为备份；主机系统采用具有自主知识产权的多核并行操作系统平台，并提供该安全操作系统的软件著作权作为证明；支持设备健康状态实时自我检测，如散热系统状态，并能够进行正常/异常状态指示(非液晶屏显示)，且能在异常状态下进行声音报警；支持数据容错处理，当数据同步失败时，用户可以查询、复位、删除未能正常传输的数据；支持数据库同步客户端的双机热备技术（不仅仅是网闸的双机热备），为用户提供更高的冗余技术支持；采用专用国产知名病毒库；支持数据库同步事件邮件报警功能；支持HTTP请求类型（GET/POST/PUT/HEAD）过滤；支持HTTP请求头部大小限制；具备公安部颁发的《计算机信息系统安全专用产品销售许可证》；具备国家信息安全测评信息技术产品安全测评证书EAL3+。

⑤USBKEY，应取得商用密码产品型号，支持SM2、SM3、SM1密码算法，SM2签名速率不低于1次/秒，对称算法加解密速率不低于100kbps；证书应符合《基于SM2密码算法的数字证书格式规范》要求，并提供一年的第三方CA证书服务。

⑥网络安全审计系统，1U标准机架式设备；Combo千兆Combo接口≥4个，10M/100M/1000M自适应电接口≥10个；支持自定义关键字对象，在应用控制的时候匹配类型包含关键字和数字，关键字可选择等于，数字可选择“大于”、“小于”、“等于”、“不等于”四种匹配模式；具有web管理界面，支持Ping、Traceroute、TCP Syn诊断工具；支持WEB Portal认证功能，支持本地认证、Radius认证、LDAP认证 和LDAP用户同步，支持对接IMC、AAS、SAM等常见AAA服务器，支持配置强制重新认证间隔，支持配置认证通过后重定向URL，要求本机自身支持短信认证功能；具有相关资质文件，包括但不限于《计算机信息系统安全专用产品销售许可证》。

⑦入侵检测系统，标准1U上架设备，冗余电源，1个RJ-45 Console口，1个10/100 Base-Tx带外管理口，≥5个GE监听口，具备2个USB接口。设备最大数据处理能力≥600Mbps，每秒新建连接数≥2万，最大并发连接数≥50万，系统需支持完善的流量统计、异常流量分析、异常流量报警的能力；支持对今日总流量、Web流量、数据库流量、邮件流量的统计功能，以及历史均值的基线自动学习能力（截图证明），系统提供威胁的实时展示能力，实时显示内容需全面丰富，包括：威胁的中文名称、威胁的处理状态、威胁的等级、威胁流行程度、威胁的源ip、威胁的目标ip、威胁发生的时间段，系统需具备入侵定位能力，具有《计算机信息系统安全专用产品销售许可证》，《中国国家信息安全产品认证证书》等资质文件。

（7）网络设备

采用的网络设备主要为负载均衡、KVM和交换机。

①负载均衡设备，能够实现对网络出口链路和服务器资源的优化调度，轻松实现大规模的应用部署，同时达至最稳定的运行效果，最高的资源利用率，最佳的应用性能和用户体验。

②KVM包括显示器和键盘，8口KVM切换器，支持USB接口，并配备LCD折叠套件（每个机柜一个）；可支持PC、SUN和MAC等各种品牌计算机和服务器；适用于Windows、Linux、Unix、OS/2等各种操作系统和应用软件；可适配VGA、SVGA和XGA等各种分辨率显示器；有自动扫描、热键切换和OSD菜单等功能。

③交换机设备，三层千兆交换机，具有100Mpps包转发率，配置48个10/100/1000M自适应电口，提供虚拟化功能，支持虚拟以太网端口聚合，支持GVRP协议，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，并要求具有灵活的以太组网，多样的安全控制，成熟的IPv6特性。

针对本次所采购的服务器、安全设备、网络设备和数据库等承载本信息平台系统运行的软硬件设施，进行集中的安全配置策略加强，并部署防病毒软件，降低恶意攻击者利用安全漏洞威胁系统安全运行的几率，从而有效控制因系统配置不当等因素引发的业务中断及信息外泄等风险，将高风险漏洞和中风险漏洞降低至可接受的范围内，使得应用系统的安全状况提升到一个较高的水平。

# 六、信息平台安全需求

承建单位需按照《信息安全等级保护商用密码管理办法》第三级要求建设本信息平台，建成后的信息系统应满足信息系统等级保护第三级要求。因此，在充分利用已有设备基础上补充采购所需的软硬件设备，形成一体的安全防护体系，对前期建设的应用系统进行安全防护。

## 6.1网络安全需求

本信息平台网络安全保障体系拟采用以下安全措施和手段：

（1）进行一定的安全域划分；

（2）通过防火墙建立多层次、多级别防御机制；

（3）通过入侵检测措施，构建边界完整性检查与保护；

（4）通过对以上安全措施和手段的统一整合，实现本系统网络系统安全保障体系的全面安全保障体系。下面详细针对各安全措施进行说明。

### 6.1.1安全域设计

在安全支撑平台的整体管控下，进行安全域等级的划分。本系统在电子政务外网划分为内部应用域、内部数据域，在互联网划分外部应用域、外部数据域、安全管理域：

内部应用域——存放密码监督管理信息平台应用服务器的区域；

内部数据域——存放密码监督管理信息平台数据服务器和数据存储系统的区域；

外部应用域——指本系统中与互联网连接的应用区域，包括对互联网提供服务的WEB服务器；

外部数据域——指本系统中与互联网连接的数据区域，包括对互联网提供服务数据服务器；

安全管理域——对外部系统提供整体安全管理的区域；

### 6.1.2区域边界安全防护

区域边界安全要解决的核心问题是实现密码监督管理信息平台所在的计算环境边界及与安全通信网络之间的设施安全。其安全防护将从边界隔离与控制、边界安全审计、恶意代码防范、边界入侵监测等方面进行设计。

在外网边界部署WEB防火墙，通过WEB检测功能有效防护由外部对网站系统的危险行为，同时通过策略对外部应用域和数据域的访问进行有效控制。

在内网边界部署防火墙，对通过电子政务外网访问应用系统及数据系统的行为进行安全审计，并对区域之间的访问执行严格的访问控制策略，以有效保护重要的信息系统资源。

各区域边界防火墙安全策略配置如下：

（1）内网边界需配置安全策略，仅授权合法的各省管理部门用户按访问控制规则进行访问；

（2）外网边界需配置安全策略，仅授权互联网用户按访问控制规则访问应用服务。

### 6.1.3网络防病毒

按照“层层设防、集中控制、预防为主、防杀结合”的策略，建设统一的、覆盖全网的、立体的、集中控制的网络防病毒体系，使网络没有薄弱环节成为病毒入侵的缺口。在网络边界部署网络防病毒设备，同时系统内部所有主机部署防病毒系统，部署的防病毒服务器负责电子政务外网及互联网上服务器和终端的病毒升级和策略管理。

## 6.2数据安全需求

### 6.2.1数据安全防护需求

信息平台要求通过集成加密技术实现传输数据的加密，以及通过部署VPN实现通信信道加密传输。

### 6.2.2数据备份与恢复需求

随着信息平台审批材料的增加，数据量将会日益增多，为保证这些数据的安全，须建立数据备份灾难恢复机制，使用专业的数据备份存储及灾难恢复系统，可以安全、可靠、高效的对重要数据和应用系统进行整体备份、自动恢复，为业务数据和应用系统提供强有力的安全保障。因此系统中应部署设备软件对数据进行数据备份，保障本系统平台的数据安全。

此外，应通过配置数据库实现数据库系统备份定期自动进行；而且当遇到数据库出现问题时，可通过数据库恢复机制自动（或手动）恢复数据库。处理时间不大于30分钟。

## 6.3应用安全需求

为应用系统增加相应的物理主机，实现应用系统的冗余设计。为满足日常来自不同方面对业务系统的访问，需要在性能上为业务系统做到最佳保障，通过部署应用负载均衡系统，实现对业务系统访问的智能分配，避免因业务系统访问突增而引起的性能下降，继而影响业务系统的正常运行。

## 6.4安全管理体系建设需求

根据甲方本项目实际需求，建设一套完整的安全管理体系，包括制定和完善信息安全管理制度、系统运维体系、建立信息安全事件响应、处理和应急机制等，定期向甲方有关人员进行信息安全培训和意识宣贯，协助甲方培养一支信息安全管理团队。

## 6.5安全维护需求

针对信息平台随机出现的重大、疑难安全故障迅速做出响应和恢复，提供问题实体的恢复、故障查因、事件跟踪等服务，提高系统应对重大安全事件/事故的能力，保障业务连续性，最大程度上减少损失和负面影响。

具备事件管理机制，事件管理的重点是确保信息平台运行中出现的绝大部分问题都能获得良好的解决。通过建立事件管理流程，提供免费安全技术支持（必要时免费提供上门服务）负责对事件进行查明、记录、调查分析、跟踪、监控、事件解决与恢复服务等一系列活动。

## 6.6可靠性需求

要求系统能够确保7×24小时不间断运行及7×24技术支持。

# 七、集成建设实施要求

## 7.1实施总体要求

信息平台软硬件集成建设需要有实施、验收方案，方案中应描述应用系统集成的具体内容及工作日程表等。工作日程表应涵盖进场、软硬件部署、系统调试、功能验证确认、系统上线、系统试运行、项目验收、技术培训等方面。

合同签订后，承建单位应至少安排一次有相关人员（包括软件开发商）参加联络会，由承建单位主持确认具体工作范围及边界，并解决本项目交货、变更、技术细节、安装调试、测试验收等具体技术问题，并提出相应的计划安排。

承建单位在实施和维护中安装的系统软件必须是一套原开发商的全新软件，不得拷贝任何经过第三方定制、更改后的软件。

## 7.2项目管理和实施计划要求

承建单位应针对本项目提出完整的项目管理方案，其中包括关于项目进度控制、质量控制、风险控制、合同管理、文档管理、变更管理以及与本项目相关的协调工作等的详细描述。

承建单位需要提交完整的项目实施计划。项目实施计划要根据本系统集成的特点和要求确定。计划应包括时间安排、工作量测算、人员投入等。

## 7.3质量保证及风险管理要求

在项目建设实施过程中，应建立完善的质量管理体系和完整的项目质量保证计划，确保系统集成、调试、培训工作的顺利实施。

本项目的质量保证计划主要是针对本信息平台的软硬件集成工作而提出相应的质量保证计划，承建单位对本次集成工作提供各种必要的质量保证措施，以保证所交付的通用软件及硬件能够满足本项目的具体需求。

承建单位应充分认识到项目风险管理的重要性，分析项目中的各类风险因素，并采取相应的对策。

## 7.4提交成果要求

承建单位在项目开始、项目实施过程中和项目结束时应向用户提供技术文档。向用户提供（有但不限于）下列技术文档。

| **项目阶段** | **交付清单** | **交付内容描述** |
| --- | --- | --- |
| 承建单位进场 | 《软硬件集成实施计划》 | 项目集成具体计划安排 |
| 集成部署 | 《设备采购清单》  《软硬件集成实施方案》 | 依据项目推进情况提交信息平台集成实施方案、管理及维护手册等。 |
| 系统调试 | 《系统调试报告》  《设备运行维护安全管理制度》  《安全设备运维管理及操作手册》  《应急处理方案》等制度 |  |
| 培训 |  |  |
| 验收及交付 | 《验收报告》 |  |

## 7.5验收要求

在系统试运行结束后，由验收专家组依据《软硬件集成需求说明书》、公安部信息安全产品检测中心信息系统安全等级保护三级测评（测评费用由承建方承担）和招标方认可的变更记录、范围变更会议纪要等，评判软硬件集成工作是否满足功能、性能、安全性指标，评判系统运行的环境是否稳定、可靠以及具有容错能力等。并由验收专家组审查相关交付文档。最终由验收专家组签署《项目验收报告》，报告结果以纸质形式呈现，经签字确认，并给出明确结论。

## 7.6工期要求

在签订协议之后，要求承建单位在2个月内完成信息平台软硬件集成工作。

# 八、培训与技术支持

## 8.1系统培训

培训内容主要针对设备管理人员，采用集中培训的方式。培训结束后，学员们能够理解和执行交换机、防火墙以及VPN等安全设备的管理任务，具有一定的分析系统故障及排查故障能力。

## 8.2售后服务及技术支持

为满足系统的建设和运行要求，要求承建单位提供优质的售后服务，至少应满足以下要求：

（1）提供为期3年的软硬件原厂保修和3年原厂免费上门服务。对硬盘等存储介质提供介质保留服务。质保期从项目通过验收之日起开始计算。

（2）质保期内，提供技术咨询和技术支持，包括为用户提供通用软件应用咨询服务、为用户方设备配置变更需求及对于因用户非正常操作带来的数据修复工作提供技术支持。

（3）指定固定联系人，对影响软件正常运行、造成业务工作大面积无法运转的严重故障，须在1小时内响应，4小时内解决故障。

（4）承建单位须制定详细服务计划，每季度对信息平台运行环境进行巡检服务，并出具巡检报告。

（5）在质保期后，承建单位有义务在通用软硬件设备维护等方面以优惠的价格继续向甲方提供技术支持，同时为其它应用系统的集成等提供技术支持。