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5月**

**目 录**

[一、项目概述 3](#_Toc8384651)

[二、项目前期情况 3](#_Toc8384652)

[三、安全集成总体要求 4](#_Toc8384653)

[四、采购内容 5](#_Toc8384654)

[五、产品及服务技术参数要求 6](#_Toc8384655)

[5.1软件设备技术参数要求 6](#_Toc8384656)

[5.1.1操作系统 6](#_Toc8384657)

[5.1.2数据库 6](#_Toc8384658)

[5.1.3双机热备软件 7](#_Toc8384659)

[5.1.4防病毒软件 7](#_Toc8384660)

[5.2硬件设备技术参数要求 8](#_Toc8384661)

[5.2.1应用服务器 8](#_Toc8384662)

[5.2.2数据库服务器 9](#_Toc8384663)

[5.2.3防病毒服务器 9](#_Toc8384664)

[5.2.4签名验签服务器 10](#_Toc8384665)

[5.2.5 SSL VPN 11](#_Toc8384666)

[5.2.6防火墙 12](#_Toc8384667)

[5.2.7防病毒网关 13](#_Toc8384668)

[5.2.8网闸 15](#_Toc8384669)

[5.2.9 USBKEY+证书 16](#_Toc8384670)

[5.2.10网络安全审计系统 17](#_Toc8384671)

[5.2.11入侵检测系统 18](#_Toc8384672)

[5.2.12负载均衡 20](#_Toc8384673)

[5.2.13 KVM 21](#_Toc8384674)

[5.2.14交换机 21](#_Toc8384675)

[5.3其他采购技术参数要求 22](#_Toc8384676)

[5.3.1集成服务 22](#_Toc8384677)

[5.3.2培训服务 22](#_Toc8384678)

[5.3.3等保安全服务 22](#_Toc8384679)

[5.3.3.1渗透测试 22](#_Toc8384680)

[5.3.3.2策略加固 23](#_Toc8384681)

[5.3.3.3制度完善 23](#_Toc8384682)

[5.3.4等级保护测评服务 23](#_Toc8384683)

[六、集成建设实施要求 24](#_Toc8384684)

[6.1实施总体要求 24](#_Toc8384685)

[6.2项目管理和实施计划要求 24](#_Toc8384686)

[6.3质量保证及风险管理要求 24](#_Toc8384687)

[6.4提交成果要求 25](#_Toc8384688)

[6.5验收要求 25](#_Toc8384689)

[6.6工期要求 25](#_Toc8384690)

[七、培训与技术支持 26](#_Toc8384691)

[7.1系统培训 26](#_Toc8384692)

[7.2售后服务及技术支持 26](#_Toc8384693)

# 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 | 单位 | 数量 |
| 应用及数据库服务器 | 台 | 4 |
| 签名验签服务器 | 台 | 1 |
| 交换机 | 台 | 2 |
| 数据库 | 套 | 2 |
| 服务器操作系统 | 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安全管理制度，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** | | | **数量** | **技术参数要求** |
| **软件采购内容** | | | | | | |
| 1 | | 通用软件 | 操作系统 | | 6 | 详见产品及服务技术参数要求章节 |
| 2 | | 数据库 | | 2 | 详见产品及服务技术参数要求章节 |
| 3 | | 双机热备软件 | | 4 | 详见产品及服务技术参数要求章节 |
| 4 | | 防病毒软件 | | 2 | 详见产品及服务技术参数要求章节 |
| **硬件采购内容** | | | | | | |
|  | | 服务器 | 应用服务器 | | 2 | 详见产品及服务技术参数要求章节 |
|  | | 数据库服务器 | | 2 | 详见产品及服务技术参数要求章节 |
|  | | 防病毒服务器 | | 2 | 详见产品及服务技术参数要求章节 |
|  | | 签名验签服务器 | | 1 | 详见产品及服务技术参数要求章节 |
|  | | 安全设备 | SSL VPN | | 2 | 详见产品及服务技术参数要求章节 |
|  | | 防火墙 | | 2 | 详见产品及服务技术参数要求章节 |
|  | | 防病毒网关 | | 1 | 详见产品及服务技术参数要求章节 |
|  | | 网闸 | | 1 | 详见产品及服务技术参数要求章节 |
|  | | USBKEY+证书 | | 100 | 详见产品及服务技术参数要求章节 |
|  | | 网络安全审计系统 | | 2 | 详见产品及服务技术参数要求章节 |
|  | | 入侵检测系统 | | 2 | 详见产品及服务技术参数要求章节 |
|  | | 网络设备 | 负载均衡 | | 1 | 详见产品及服务技术参数要求章节 |
|  | | KVM | | 2 | 详见产品及服务技术参数要求章节 |
|  | | 交换机 | | 4 | 详见产品及服务技术参数要求章节 |
| **其他采购内容** | | | | | | |
|  | 集成服务 | | | 负责本次采购设备的安装、调试等工作。 | | |
|  | 培训服务 | | | 为检测中心设备管理人员集中培训一次。 | | |
|  | 等保安全服务 | | | 包含渗透测试、策略加固、制度完善服务。 | | |
|  | 等级保护测评 | | | 邀请入围全国等级保护测评机构推荐目录的第三方测评机构对密码监督管理信息平台进行等保三级测评 | | |

# 五、产品及服务技术参数要求

## 5.1软件设备技术参数要求

### 5.1.1操作系统

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
| 1 | 功能要求 | 需要支持Intel x86-64 (AMD 64)架构； |
| 2 | 兼容性 | 需兼容国内外主流的软件产品，兼容主流国产数据库产品及中间件产品； |
| 3 | 兼容国产主流热备软件； |
| 4 | 支持算法 | 支持国密算法。 |

### 5.1.2数据库

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
|  | 产品功能 | 需支持ANSI/ISO SQL-89、ANSI/ISO SQL-92标准。 |
|  | 需支持中文汉字内码，符合双字节编码。 |
|  | 需支持字符型数据如nchar数据类型、nvarchar数据类型、text数据类型； |
|  | 需支持数值型数据如int数据类型、float数据类型； |
|  | 需支持时间类型数据如DATE 数据类型、DATETIME 数据类型； |
|  | 数据库产品应具有良好的图形化用户界面（GUI），方便对数据库进行管理/数据库应具有良好的自我管理，自我配置与自我调优能力。 |
|  | 需支持在同一个硬件服务器上运行多个数据库实例。 |
|  | 需支持同一个实例上运行多个数据库，同一管理控制台完成所有管理工作，工具易于理解、使用同一产品中具有完整的管理、调优、调度与开发工具。 |
|  | 需支持网络上同构或异构数据库之间数据的有效传输和冗余性复制；具有多种复制功能模块。 |
|  | 需支持ODBC 3.5、JDBC 3.0、ADO.NET、C API等标准。 |
|  | 需支持分布式事务及两阶段提交功能。 |
|  | 需支持动态将锁粒度调整到合适的级别，支持动态行级锁定。 |
|  | 需支持高可用性组，可以创建和配置一个或多个可用性组。 |

### 5.1.3双机热备软件

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
|  | 操作系统 | 需支持Windows、Linux、Unix等操作系统；需要与采购的操作系统有良好的适配性性； |
|  | 磁盘保护 | 需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； |
|  | 心跳模式 | 需支持多种心跳模式； |
|  | 管理界面 | 需支持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； |
|  | 资质要求 | 具有计算机软件著作权登记证书 |

### 5.1.4防病毒软件

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
|  | 基本要求 | 需提供2套企业网络版防病毒系统，每套包含1个控制中心+服务端10个+客户端100个，需支持Windows、Linux操作系统，能对采购的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，包括64位系统。 |
|  |
|  | 产品采用B/S管理和C/S通信构架，具有良好的可扩展性和易用性，需支持大型网络跨地域跨网段的部署和管理，具有全网统一杀毒和升级的功能。 |
|  | 产品基本功能 | 允许管理员通过控制台，集中地实现所有节点上防毒软件的监控、配置、查询等管理工作，包括Windows系统上的防病毒软件。 |
|  | 控制台可以进行病毒扫描引擎和代码库的更新，并能将此扫描引擎和代码库自动提供给各种服务器和工作站,不需要另外设置升级服务器。 |
|  | 具备客户端部署管理功能，控制台需支持实时显示客户端的状态，可以自动扫描网络，帮助管理员快速掌控网络中哪些计算机未安装防病毒软件、哪些计算机病毒代码或扫描引擎过期、哪些计算机未安装系统补丁等。 |
|  | 实时监控及病毒处理能力 | 内存监控与杀毒技术：能够直接对运行程序的进程和线程进行扫描，并直接在内存中对正在运行的染毒文件进行清除病毒的工作。 |
|  | 实时和定时检测/清除病毒。实时检测和清除来自各种途径的各类恶意代码和特洛伊木马等黑客程序。对来自Internet、E-mail或是光盘、软盘、移动存储、网络等各种入口渠道的宏病毒、特洛伊木马、黑客程序和有害程序等全面进行实时监控。 |
|  | 能够对各种加壳的病毒文件进行病毒查杀；采用宏指纹识别技术更有效的查杀OFFICE宏病毒；需支持族群式变种病毒的查杀。 |
|  | 需支持白名单管理，免检区可以自由增加和删除文件及文件夹 |

## 5.2硬件设备技术参数要求

### 5.2.1应用服务器

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
| 1 | 机型 | 机架式服务器 |
| 2 | 处理器 | 配置≥2颗Intel Xeon 6130 CPU |
| 3 | 内存 | 配置≥128GB DDR4内存，内存最大扩展插槽≥48个，需支持内存保护、内存镜像、内存热备 |
| 4 | 硬盘 | 配置≥3块600GB 2.5吋10K 12Gb SAS硬盘，需支持≥2个M.2 SSD硬盘扩展，2.5寸热插拔硬盘扩展能力不少于26个。 |
| 5 | 硬盘控制器 | 配置磁盘SAS RAID控制器，需支持RAID 0/1/5/10，速率≥12Gb，Cache 缓存≥2GB；配置电容掉电保护；所有硬盘需支持同时配置JBOD及直通方式 |
| 6 | 网卡 | 配置≥1块双口千兆网卡， 需支持NCSI、网络唤醒，网络冗余，负载均衡等网络高级特性；配置≥1块双口万兆光纤网卡（含模块） |
| 7 | 扩展插槽 | 需支持≥14个PCIE 3.0槽位（含≥4个PCIE X16插槽） |
| 8 | RAID | 配置2G Cache 硬盘控制器，需支持RAID 0/1/5/6/10等 |
| 9 | 电源 | 配置热插拔2+1冗余电源； |
| 10 | 可维护性 | 需支持离线光诊断功能，可断电环境下诊断主板关键信息故障；需支持SD卡日志记录系统，可持续记录服务器全生命周期系统日志； |
| 11 | 管理 | 集成系统管理芯片，需支持：1. iKVM和KVM Over IP高级管理功能，本地固件更新、错误日志，提供系统状况的可视显示； 2.配置独立的远程管理控制端口，需支持远程监控图形界面,可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、虚拟设备挂载等操作；3.可实现监控服务器内部主要部件的状态，包括CPU、内存、硬盘、PCI功耗、风扇、电源、功率、温度等信息； |

### 5.2.2数据库服务器

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
| 1 | 机型 | 机架式服务器 |
| 2 | CPU | 配置≥2颗X86架构 CPU ( 每颗CPU配置≥24核，≥2.0GHz主频） |
| 3 | 内存 | 配置 ≥128GB DDR4，需支持≥32个内存插槽，最大可支持4TB内存容量，需支持内存ECC保护、内存镜像、内存热备 |
| 4 | 硬盘 | 配置3块 600GB SAS（企业级）热插拔2.5硬盘，需支持≥24个前置热插拔2.5硬盘，可选配2\*后置SAS/SATA/SSD硬盘 |
| 5 | 网卡 | 配置≥1块双口千兆网卡， 需支持NCSI、网络唤醒，网络冗余，负载均衡等网络高级特性；配置≥1块双口万兆光纤网卡（含模块） |
| 6 | 电源 | 冗余电源 |
| 7 | 硬盘扩展 | 需支持≥4个NVME U.2 SSD，不需PCE-E转接卡 |
| 8 | RAID | 配置2G Cache 硬盘控制器，需支持RAID 0/1/5/6/10等 |
| 9 | PCIE扩展 | 最大支持≥10个PCI-E 3.0插槽（2个内置专用插槽） |
| 10 | 维护管理 | 需支持独立的远程管理控制端口，实现与操作系统无关的远程对服务器的完全控制，远程开机、关机、重启、虚拟设备挂载等操作； 实时监控服务器内部关键部件运行状态和温度信息，CPU、内存、硬盘、风扇、电源、扩展卡； |
| 11 | 安全性 | 配置基于国密算法的内存加密安全保护功能，加密内存中的程序和数据，可支持TCM和TPM安全模块 |

### 5.2.3防病毒服务器

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
| 1 | 机型 | 机架式服务器 |
| 2 | CPU | 配置≥2颗X86架构 CPU ( 每颗CPU配置≥16核，≥2.0GHz主频） |
| 3 | 内存 | 配置 ≥32GB DDR4，需支持≥32个内存插槽，最大可支持4TB内存容量，需支持内存ECC保护、内存镜像、内存热备 |
| 4 | 硬盘 | 配置3块 600GB SAS（企业级）热插拔2.5硬盘，需支持≥24个前置热插拔2.5硬盘，可选配2\*后置SAS/SATA/SSD硬盘 |
| 5 | 网卡 | 配置≥4\* 1GE网口 |
| 6 | 电源 | 冗余电源 |
| 7 | 硬盘扩展 | 需支持≥4个NVME U.2 SSD，不需PCE-E转接卡 |
| 8 | RAID | 配置2G Cache 硬盘控制器，需支持RAID 0/1/5/6/10等 |
| 9 | PCIE扩展 | 最大支持≥10个PCI-E 3.0插槽（2个内置专用插槽） |
| 10 | 维护管理 | 需支持独立的远程管理控制端口，实现与操作系统无关的远程对服务器的完全控制，远程开机、关机、重启、虚拟设备挂载等操作；实时监控服务器内部关键部件运行状态和温度信息，CPU、内存、硬盘、风扇、电源、扩展卡； |
| 11 | 安全性 | 配置基于国密算法的内存加密安全保护功能，加密内存中的程序和数据，可支持TCM和TPM安全模块。 |

### 5.2.4签名验签服务器

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
|  | 硬件规格 | 标准机架式硬件设备。 |
|  | 接口要求 | ≥2个100/1000M自适应网口。 |
|  | 数字签名效率 | SM2+SM3 算法，不低于 800 次/秒；验签能力，SM2+SM3 算法，不低于 650 次/秒。 |
|  | 应用许可数量 | 至少含4个应用许可。 |
|  | 功能要求 | 提供pkcs1/Pkcs7 attach/Pkcs7 detach/xml Sign 等对多种格式数据的数字签名和验证功能，需支持RSA算法。 |
|  | 提供文件数字签名和验证功能, 需支持对文件进行MD5、SHA-1等方式的数字摘要后在进行签名。 |
|  | 提供证书验证功能，需支持对X.509 Version 3、PKCS系列证书的DER和PEM格式的应用与验证。 |
|  | 提供数据加密、解密功能，需支持数字信封加密，需支持DES、Tri-DES算法、以及国产密码算法。 |
|  | 提供CRL的证书有效性验证，CRL更新配置可自动定时进行。 |
|  | 服务器证书管理：实现对业务系统服务器端密码设备及服务器证书进行配置与管理，可生成服务器证书申请文件。 |
|  | 信任源管理：可同时配置多条证书链，验证不同CA的用户证书。 |
|  | 动态黑名单管理：可自动更新CRL黑名单、动态更新，不需要重新启动服务。 |
|  | 安全存储：基于密码技术构建安全存储区，用于对可信根证书及黑名单文件进行分类安全存储，防止非法操作。 |
|  | 签章服务 | 产品生产厂商需提供电子签章服务，以帮助招标人满足国家统一电子印章系统签章技术要求、印章技术要求和系统接口要求等规范，建立从制作、状态发布到应用的完整的电子印章服务体系。 |
|  | 资质 | 具有国家密码管理局颁发的《商用密码产品型号证书》 |
|  | 具有公安部颁发的《销售许可证》 |
|  | 具有公安部计算机信息系统安全产品质量监督检验中心颁发的《检验检测报告》 |
|  | 具有中华人民共和国国家版权局颁发的《软件著作权登记证书》 |

### 5.2.5 SSL VPN

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
| 1 | 性能参数 | 要求加密速率≥950Mbps，并发SSL用户数≥300，整机吞吐≥5Gbps，最大并发用户数≥20000，≥8个10/100/1000M Base-TX；≥4个SFP光口插槽，双冗余电源，标准机架设备 |
| 2 | 功能特征 | 需支持网关模式、单臂模式、双机模式、集群模式的部署 |
| 3 | 专业VPN设备，采用标准SSL、TLS 协议，同时需支持IPSec VPN、SSLVPN两种VPN，非插卡或防火墙带VPN模块设备。同时需支持软件化交付 |
| 4 | 需支持终端使用包括IE6、7、8、10、11或其他IE内核的浏览器，以及最新版本的非IE内核浏览器，如Windows EDGE，Google Chrome，Firefox，Safari，Opera最新版登录SSLVPN系统，登录后可完整支持各种IP层以上的B/S和C/S应用。 |
| 5 | 产品必须支持防中间人攻击，产品可在用户登录SSLVPN时智能判断存在中间人攻击行为，断开被攻击的连接，并可提示异常现象。 |
| 6 | 产品应具有用户/用户组细粒度的权限分配功能：可以针对被访问资源的IP地址、端口、提供的服务、URL地址等进行权限控制；针对同一B/S资源，可对不同用户做到细致到URL级别的授权。 |
| 7 | 需支持主从认证账号绑定，必须实现SSL VPN账号与应用系统账号的唯一绑定，VPN资源中的系统只能以指定账号登陆，加强身份认证，防止登录SSL VPN后冒名登录应用系统 |
| 8 | 产品应支持Local DB 、USB KEY、短信认证、硬件特征码、动态令牌、数字证书认证、LDAP、RADIUS、等认证方式；可针对用户/用户组设置认证方式的与、或组合，可进行用户名/密码、LDAP、USB KEY、硬件特征码、短信认证或动态令牌的五因素捆绑认证 |
| 9 | 需支持利用网页进行动态寻址的方法，客户端无需安装插件、不依靠IP地址库、不依赖于第三方动态IP寻址、直接根据速度探测实现用户端接入线路的自动优选,用户通过访问寻址代理页面（简称Webagent页面），通过Webagent页面自动寻找VPN设备IP(非DDNS）,该方法不必单独注册域名或占用IP地址，大大降低了系统部署难度。 |
| 10 | 需支持系统实时监控，图形化显示一段时间内的运行状况，可查看CPU占用率、各条线路网络吞吐量、各条线路的IP地址及发送接收流速、并发会话数、SSL并发用户数；可查看历史最高并发用户数并显示时间记录；可实时查看SSL接入用户的用户名、发送流速、接收流速、发送流量、接收流量、接入时间、并发会话数、接入IP、虚拟IP、认证方式等信息，并可在线中断指定用户 |
| 11 | 需支持独立日志中心进行SSLVPN实时日志记录，可详细记录用户访问资源记录（用户、主机IP、资源、时间）、管理员日志（管理员、主机IP、时间、管理行为、对象）、系统日志、告警日志；可根据用户名、主机IP等信息进行用户行为查询；可提供用户组/用户流量排行及查询、资源流量排行及查询、资源活跃程度、用户活跃程度等记录；提供暴破登录记录；可提供用户登陆SSLVPN采用非绑定账号访问应用系统的记录 |
| 12 | 产品应具备基于状态监测技术的防火墙功能，能够抵抗常见的网络攻击，能够进行包过滤或WAN、LAN、DMZ口之间访问控制；为了避免人为配置错误，产品必须支持对防火墙的过滤规则能够进行在线虚拟测试。 |
| 13 | 资质 | 投标设备具有国家密码管理局颁发的《商用密码产品型号证书》 |

### 5.2.6防火墙

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
|  | 硬件架构 | 标准机架式设备，采用非X86多核架构，处理器最低配置为4核并行处理CPU |
|  | 需支持≥2个通用扩展槽，配置冗余电源 |
|  | 配置≥８个电口，≥４个千兆光口（含模块） |
|  | 性能指标 | 网络吞吐≥８Gbps |
| 新建连接数≥１２万，并发连接数≥３００万 |
| 扩展性要求 | 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 |
|  | 网络适应性 | 需支持IPv4和IPv6的静态路由、等价路由、策略路由，以及BGP、RIPv1/v2、OSPF、ISIS等动态IPv4路由协议（非透传），需支持ISP路由并内置多运营商路由表 |
|  | 需支持透明、路由、混合、旁路四种工作模式 |
|  | 访问控制 | 必须支持抵御所列所有攻击类型，包括：DNS Query Flood、SYN Flood、UDP Flood、ICMP Flood、Ping of Death、Smurf、Winnuke |
|  | 必须支持会话控制功能，要求能够限制并发数和会话新建速率 |
|  | 必须支持对防火墙策略命中次数进行统计和策略冗余检查功能 |
|  | 具备对应用程序的识别和控制能力。应用程序特征库不少于3400种，并支持在线更新； |
|  | 可扩展支持对多层级管道进行最大带宽限制、最小带宽保证、每IP或每用户的最大带宽限制和最小带宽保证 |
|  | 可扩展支持两层八级管道嵌套 |
|  | 管理功能 | 需支持中、英文操作界面；需支持console、telnet、SSH管理；需支持http和https两种方式web管理 |
|  | 需支持通过手机APP方式实时监控防火墙等设备状态、网络流量、及威胁信息 |
|  | 产品资质 | 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》防火墙（IPv6）增强级(2015国标) |
|  |
|  | 国家保密科技测评中心颁发的《涉密信息系统产品检测证书》千兆 |

### 5.2.7防病毒网关

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
| 1 | 接口要求 | 需支持≥8×10/100/1000千兆电口（含三路Bypass）、≥2个Slot扩展槽（标配四口千兆SFP扩展卡）、≥1个Console接口(RJ-45) 、≥2个USB外置接口,机架式设备，采用冗余电源。 |
| 2 | 性能要求 | 网络吞吐量≥10Gbps,防病毒吞吐量≥3Gbps，并发连接数≥400万。 |
| 3 | 引擎要求 | 要求为专业级防病毒过滤网关产品，不可嵌入第三方防病毒引擎。 |
| 4 | 系统要求 | 需支持应急系统，用于系统应急故障处置。 |
| 5 | 网络场景 | 需支持透明模式、端口汇聚等复杂网络环境场景应用； |
| 6 | 协议栈支持 | 需支持对IPv4、IPv6环境的接入和综合性防御； |
| 7 | BYPASS功能 | 需支持设备前液晶屏面板操作。WEB管理界面的BYPASS开启与关闭；需支持在BYPASS开启状态下，WEB管理界面仍可继续操作。 |
| 8 | 链路连续性保障 | 需支持串行部署模式下的连接状态传递和自动BYPASS功能。用于HA环境或全互联环境下的链路切换状态传递。 |
| 9 | 接入方式 | 需支持串行部署、并行部署、串并混合部署； |
| 10 | 并行防御模式 | 需支持在旁路模式下，通过策略路由方式对链路进行病毒过滤和威胁拦截。 |
| 11 | 病毒类型 | 需支持可执行病毒、宏病毒、木马、蠕虫、间谍软件、恶意脚本等混合型病毒文件的过滤。 |
| 12 | 手机病毒 | 需支持针对苹果或安卓手机平台下的恶意APP程序监测、过滤； |
| 13 | 协议过滤支持 | 需支持HTTP、SMTP、FTP、POP3、IMAP、SMB协议过滤； |
| 14 | 协议支持模式 | 需支持每项协议过滤的多种工作模式，且无需人工设定协议过滤端口，为自适应和自动识别模式； |
| 15 | 病毒文件处理 | 需支持对协议层病毒文件的放行、告警、破坏、隔离、阻断处理模式；且支持对每项协议病毒过滤策略的单独设定，且不影响其他协议过滤策略。 |
| 16 | 病毒名称白名单 | 需支持对病毒名称的白名单设定，设定后此类病毒名称将被放行。 |
| 17 | 病毒样本扫描 | 需支持将病毒文件、恶意PCAP包进行界面上传、扫描、结果输出。 |
| 18 | 恶意通讯威胁 | 需支持处于活动状态下的蠕虫扩散、木马通讯、僵尸网络通讯、邮件蠕虫等恶意代码行为的识别及阻断。 |
| 19 | 恶意网络威胁 | 需支持针对系统级的漏洞攻击、恶意站点、WEB攻击网络威胁的识别及阻断； |
| 20 | 口令探测防御 | 需支持对具有认证机制的协议探测防御，如SMTP、POP3、IMAP、SMB、HTTP、FTP协议的探测扫描、暴力破解防护。 |
| 21 | 威胁防御策略 | 需支持对活动、通讯状态下的网络恶意行为的阻断功能、阻断时长、自动黑名单加入、白名单的参数设定。 |
| 22 | 威胁库数量 | 需支持1200万以上数量的恶意代码库； |
| 23 | 恶意代码库更新 | 需支持在线更新、离线导入、指向升级、定时更新，更新途径必须采用加密协议，确保库更新过程的完整性和安全性； |
| 24 | 恶意代码库回滚 | 需支持对恶意代码库的旧版本回滚功能，回滚版本应支持三个版本以上。 |
| 25 | 管理方式 | 需支持HTTPS、SSH、Console登录管理，需支持CLI下的SHELL操作； |
| 26 | 远程协助 | 需支持互联网环境下的设备远程登录功能，且链路为加密方式，以此解决互联网环境下的地址映射和厂商技术的快速支持。 |
| 27 | 管理协议 | 需支持SNMP、SYSLOG、NTP、Radius协议； |
| 28 | 账户设定 | 需支持账户的权限分离、本地账户操作、Radius账户同步下发、安全性检查操作等功能； |
| 需支持对可信主机的设定，如IP限制、端口服务限制操作； |
| 29 | 集中管理 | 需支持单台设备对多台分布式或分级式部署的集中管理功能； |
| 30 | 分级管理 | 需支持单台设备对节点设备的远程管理功能，至少包括：策略远程下发、配置备份与还原、界面操作、远程关机重启、远程BYPASS操作、特征库更新。 |
| 31 | 风险分析 | 需支持风险分析报告生成，应体现出是活跃病毒的信息，包含对病毒的类型、协议、触毒节点，以及对探测账户、失窃账户重要信息的体现。 |
| 32 | 风险分析报告，应支持在线自动生成、手动生成、邮件定时发送功能，便于安全管理员及时获取相关风险提示。 |
| 33 | 安全报告 | 需支持对数据的安全报告生成，可定时生成，手动生成，定制化操作，导出格式至少支持PDF、DOC、MHT； |
| 34 | 类型查询 | 需支持对病毒、木马、蠕虫、恶意代码、安全漏洞、口令探测、WEB攻击、垃圾邮件、内容过滤的综合条件查询。实现对恶意代码各层威胁数据的综合分析。 |
| 35 | 日志分析展示 | 需支持趋势图、柱状图实现的威胁类型、IP地址、周期内的威胁展示； |
| 36 | 日志查询 | 可实现对各项威胁数据的综合条件查询及结果的导出，格式为xls； |
| 37 | 资质要求 | 需提供本产品软件著作权和公安部颁发的产品销售许可证。 |

### 5.2.8网闸

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
|  | 性能参数 | 吞吐量 ≥1Gbps，内网主机接口配置千兆电口≥6个，千兆光口SFP≥4个，外网主机接口设置千兆电口≥6个，千兆光口SFP≥4个，串口(RJ45)≥1个，冗余电源，标准机架式设备 |
|  | 系统架构 | 1、采用2+1系统架构即内网单元+外网单元+FPGA专用隔离硬件。不能采用网线等形式直通。 2、采用基于linux内核的多核多线程专用安全操作系统，加固内核。 |
|  | 部署模式 | 设备支持透明、代理及路由三种工作模式，管理员可依据实际网络状况进行相应的部署。 |
|  | 功能特性 | 产品内置各类应用支持模块，无须用户增加投资，功能模块至少包含：邮件模块、安全浏览模块、视频交换模块、数据库访问模块、数据库同步模块、文件交换模块、OPC模块、MODBUS模块、WINCC模块、组播代理模块、用户自定义应用模块等各类应用模块,并可控制相应应用协议的的动作、参数、内容。 |
|  | 需支持的数据库种类包括ORACLE、SQLSERVER、MYSQL、SYBASE等主流数据库支持多种关系型数据库通信。需支持SQL语句的白名单 |
|  | 需支持Samba、FTP、HTTP等多种通信协议 需支持文件类型黑白名单传输控制 可通过专用客户端或共享方式提供安全的文件同步功能 需支持一对多或多对一传输 |
|  | 需支持TCP应用层数据单向传输的控制，保证TCP应用数据的0 反馈，以满足二次防护对数据传输的安全性需求。 |
|  | 采取系统策略配置管理员、安全管理员与日志管理员三种角色分立的权限分配模式，用户只能维护操作本类基础管理角色的功能与操作，权限各不交叉。 |
|  | 需支持根据时间自动切换的安全策略。需支持时间段以24小时制，支持以星期为周期，支持指定时间点一次性运行 |
|  | 系统可存储和审计包含：系统日志；管理日志；网络活动日志；入侵报警及处理日志；访问控制日志。 |
|  | 需支持双机热备及多机热备功能，最大化的保障业务可用性。 |
|  | 资质 | 需具备公安部计算机信息系统安全专用产品销售许可证（增强级）； |

### 5.2.9 USBKEY+证书

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标要求** |
|  | USBKEY功能要求 | 需支持USB2.0接口 |
|  | USBKey容量不小于32K字节 |
|  | USB Key自身的安全要求：具备完善的PIN校验保护功能 |
|  | 需支持国产商用密码算法。 |
|  | 数字证书要求 | 证书应符合《基于SM2密码算法的数字证书格式规范》要求， |
|  | 标识个人用户网络身份。 |
|  | 证书颁发机构应具有电子政务电子认证服务资质。 |
|  | 证书格式标准遵循x.509v3标准。 |
|  | 需支持存放介质：智能USBKey。 |

### 5.2.10网络安全审计系统

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
|  | 性能及硬件要求 | 整机吞吐量：≥1Gbps |
|  | 最大并发连接数：≥50万 |
|  | 新建并发连接数：≥2万 |
|  | 接口数：配置≥16个千兆光口（含8个模块）和≥8个千兆电口 |
|  | 扩展能力：≥2个接口板扩展槽位，可支持千兆、万兆接口扩展 |
|  | 电源：双电源 |
|  | 部署方式 | 需支持透明在线模式、网桥模式、网关模式、旁挂模式部署，需支持分布式与集中式部署，对于分布式部署，可分权分域与集中管理 |
|  | 网络特性 | 需支持VRRP、基于状态的双机热备，需支持路由模式和透明模式的HA |
|  | 需支持TR069管理协议。 |
|  | 需支持NAT功能，需支持源NAT、目的NAT、一对一NAT的等功能 |
|  | 可以识别并检测802.1Q、MPLS、QinQ、GRE等特殊封装的网络报文 |
|  | IPv6协议支持，包括审计、流控、访问控制、URL过滤、关键字过滤、质量感知 |
|  | 需支持策略路由协议、动态路由协议，包括RIP、OSPF、ISIS、BGP |
|  | 行为审计及流量分析 | 可以识别协议数量超过4000个，通过告警、干扰、阻断等模式可提供万种以上应用规则，需支持根据IP、端口、协议等自定义应用规则。 |
|  | HTTP审计需支持智能过滤，设备能够过滤掉大部分无用的日志，产生的日志都是用户访问页面的日志。 |
|  | 需支持审计记录目的IP的实际地理位置。 |
|  | 需支持用户新建连接、并发连接数分析及图表。 |
|  | 需支持对上网终端的审计，包括终端类型、操作系统类型、系统版本号、浏览器类型等终端信息 |
|  | 需支持实名认证与审计日志关联 |
|  | 设备告警 | 需支持智能告警系统，当CPU、内存、硬盘、设备温度、接口带宽利用率、接口CRC错误达到预设阈值时，可通过E-mail、短信、SNMP Trap三种告警方式向用户发送告警信息 |
|  | 系统管理 | 全中文管理界面，需支持HTTP、HTTPS登陆WEB界面管理 |
|  | 需支持基于串口、Telnet、SSH的命令行管理 |
|  | 需支持热补丁功能，在线升级无需重启 |
|  | 需支持SNMPv1、v2、v3版本，使用SNMP访问设备地址可进行设置 |
|  | 需支持保存5个以上软件版本，需支持本地和在线升级 |
|  | 需支持NTP时钟client和serverp模式 |
|  | 控制和转发平面分离，即使超过设备处理性能也可以正常进行管理 。 |
|  | 需支持VIP网段和普通网段，当超过设备处理性能时VIP网段优先bypass。 |
|  | 产品资质 | 《计算机信息系统安全专用产品销售许可证》（千兆） |
|  | 《计算机软件著作权登记证书》 |

### 5.2.11入侵检测系统

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
|  | 性能及硬件要求 | 设备最大数据处理能力≥1Gbps |
|  | 最大连接数：≥100万 |
|  | 每秒新建连接数：≥1万 |
|  | 接口：配置≥1个RJ-45 Console口，≥1个10/100/1000 Base-Tx带外管理口，≥5个GE监听口，具备≥2个USB接口 |
|  | 扩展能力：≥1个接口板扩展槽位 |
|  | 部署方式 | 需支持透明、透明桥接、旁路等部署模式，需支持带内、带外管理 |
|  | 基本攻击检测 | 内置特征库，特征规则数量不少于6100条，并可根据CVE编号查询具体的攻击特征；具备系统一键修改特征级别的功能，用户可根据自身安全需求将特征内容根据流行度规则高低进行检索，并可一键修改流行度规则级别（警告、一般、严重、致命、废除）。 |
|  | 入侵检测事件库应符合国家信息安全CNNVD漏洞库标准，事件描述为中文；事件特征库在线升级频率不少于一周一次 |
|  | 需支持自定义特征，可基于方向、协议、字符串、正则表达式、源端口、目的端口等维度进行特征自定义，并可自行设置特征严重等级（警告、一般、严重、致命、废除），满足用户定制化需求。 |
|  | 需支持畸形包攻击检测，需支持针对协议漏洞的畸形包攻击检测，对LAND、死亡之Ping、IP分片重叠、UDP Fraggle、WinNuke、ICMP Smurf、Tear Drop等常见攻击的检测，并可根据用户自身安全需求设置相应策略。 |
|  | 病毒检测 | 集成第三方专业防病毒厂商的专业病毒库，特征规则数量不少于10000条 |
|  | 具备对病毒感染主机或黑客主机的网络检测功能，用户可以根据自身的安全需求设置高、中、低三种流行度规则，可以设置告警等方式进行防御，并且用户可以自定义配置告警推送内容。 |
|  | 网络特性 | 可以在IPv4/IPv6双栈、MPLS等复杂网络环境下良好的工作，可以识别并检测QinQ、PPPoE、MPLS、GRE、Vlan等特殊封装的网络报文，具备面向下一代网络的各种特性 |
|  | 攻击取证 | 需支持攻击取证功能：需支持查看攻击事件明细，分析攻击源目的IP及端口，并可针对攻击事件分析攻击报文内容，便于分析提取关键攻击特征。 |
|  |  | 需支持未知威胁监控平台，可实时展示未知威胁日志，需支持恶意域名、恶意IP、恶意邮箱、恶意FTP的排名统计与展示。 |
|  | 系统功能 | 系统具备健康状态异常告警机制，发现异常状态时可通过邮件、短信等各种方式及时通知管理员，告警触发条件可设置 |
|  | 需支持基于物理接口或vlan配置虚拟引擎，每个虚拟引擎能够支持资源分配，如：吞吐量、CPU使用率、内存使用率等，每个虚拟引擎可由超级管理员分配独立的用户名和密码，并且各个虚拟引擎可独立配置防护策略。 |
|  | 需支持IPv4、IPv6环境下部署，NTP时钟同步可提供Server、Client两种模式，需支持认证加密。 |
|  | 需支持实现配置的自动同步和手动同步，保证会话同步 |
|  | 需支持页面登录、指纹登录方式，需支持Web图形界面配置，需支持SSH、、TELNET、CONSOLE命令行模式配置和集中管理模式 |
|  | 设备管理及运维 | 需支持在线自动升级，本地升级，并支持热补丁导入，并可查看补丁版本号及状态； |
|  | 需支持三权分立管理，提供超级管理员，系统管理员和审计员角色。 |
|  | 日志管理 | 需支持网管软件统一网管，需支持SNMPv1，SNMPv2c和SNMPv3；需支持通过SNMP用户进行认证，需支持认证加密和数据传输加密功能； |
|  | 提供Syslog日志，操作日志，业务日志的查询功能并提供对日志的多种查询方式；可以根据日志监控到接口状态信息、设备状态信息变更；可以基于时间维度、IP地址范围、关键字查询操作日志，监控到访问者的IP地址以及访问的功能模块。 |
|  | 产品资质 | 《计算机信息系统安全专用产品销售许可证》（千兆） |
|  | 《计算机软件著作权登记证书》 |

### 5.2.12负载均衡

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
|  | 性能参数 | L4吞吐量≥5Gbps，L4并发会话数≥3,000,000，网络接口千兆电口≥6、千兆光口≥2 |
|  | 产品形态 | 需采用独立的专用硬件AD应用交付设备，而非通过添加功能模块的方式实现 |
|  | 多合一功能集成 | 需提供针对多条出口线路的链路负载均衡功能，实现inbound 和outbound流量的均衡调度，以及链路之间的冗余互备 |
|  | 需提供针对L4/L7内容交换的服务器负载均衡功能，可在单一设备上支持多个应用和服务器集群，可以根据多种算法和要求分配用户的请求 |
|  | 需提供针对多站点业务发布的全局负载均衡功能，通过智能DNS等机制实现内外网用户对多个数据中心的最优接入路径选择 |
|  | 单一设备可同时支持包括链路负载均衡、全局负载均衡和服务器负载均衡的功能。三种功能同时处于激活可使用状态，无需额外购买相应授权。 |
|  | 可编程流量控制 | 通过某种编程语言实现自定义的流量编排，对TCP、SSL、HTTP种HTTPS等类型的流量进行分发、修改和统计等操作。 |
|  | 负载均衡 | 需支持服务器被动式健康检查，可根据对业务流量的观测采样，辅助判断应用服务器健康状况；对常规HTTP应用可配置基于反映URL失效的HTTP响应状态码的观测判断机制，对于复杂应用可配置基于RST关闭连接和零窗口等异常TCP传输行为的观测判断机制。 |
|  | 需支持非对称式部署的TCP协议优化技术，提升远端用户访问应用服务的速度。 |
|  | 需支持图片优化技术，通过对图片格式的转换，减少传输流量，提升web页面加载速度，优化加速效果。 |
|  | 需支持对防火墙、IPS、行为管理等网络设备进行流量负载均衡和故障切换，使以上网络设备获得Active-Active 运行的能力 |
|  | 免费开通HTTP压缩、HTTP缓存、TCP连接复用、SSL加速功能，无需额外购买相应授权。 |
|  | 需支持面向服务器健康度的弹性调控机制，可通过监控业务流中的TCP传输异常来衡量服务器节点的有效性，尝试对性能不足的服务器临时开启过载保护。 |
|  | 需支持DNS透明代理功能，可基于负载均衡算法代理内网用户进行DNS请求转发，避免单运营商DNS解析出现单一链路流量过载。 |
|  | 需支持基于链路负荷情况的繁忙保护机制，能根据链路的上行/下行带宽占用率情况执行对出站/入站流量的高级调度策略。 |
|  | 运维管理 | 需支持全中文管理界面和HTTPS方式登录、用户角色管理、多级授权管理 |
|  | 需支持应用配置模版功能，提供WebLogic、WebSphere、Oracle等主流商业应用的配置模版，管理员可直接套用完成应用系统的部署上线，简化配置与调试工作。 |
|  | 设备内置数据中心，需支持自动订阅和手动生成两种方式输出PDF格式的报表。报表可对链路和服务器的稳定性进行统计。可查询服务器的异常状态信息，并提供对故障原因的分析。 |
|  | 资质 | 具备国家工业和信息化部颁发的《电信设备进网许可证》（提供复印件） |

### 5.2.13 KVM

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
|  | 硬件参数 | 标准机架式设备 |
|  | 接口数量 | ≥8口 |
|  | 切换方式 | OSD、键盘热键 |
|  | 支持设备 | 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； |

### 5.2.14交换机

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
| 1 | 性能及硬件要求 | 交换容量：≥330Gbps |
| 2 | 包转发率：≥128Mpps |
| 3 | 配置≥48个10/100/1000M自适应电口，≥4千兆光接口（含模块） |
| 4 | MAC地址用户数 | 要求设备单端口支持的MAC地址用户数≥4k |
| 5 | 路由协议 | 支持静态路由、RIP、OSPF、BGP。 |
| 6 | OSPF路由表容量≥12K |
| 7 | 风扇 | 为保障设备稳定性，要求采用无风扇设计 |
| 8 | 静音 | 为减少噪音污染，要求设备符合国家标准GB3096-2008中最高级别0类噪音标准 |
| 9 | 绿色环保 | 为节能环保考虑，降低UPS电源的功率，要求设备最大功耗≤34W |
| 10 | 要求设备支持802.3az能效以太网技术 |
| 11 | 产品资质 | 《电信设备入网许可证》 |

## 5.3其他采购技术参数要求

### 5.3.1集成服务

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
| 1 | 服务内容 | 针对软硬件设备开展上架、安装、调试工作，完成信息平台软硬件产品的集成工作。 |
| 2 | 服务范围 | 针对本项目涉及的所有软硬件产品 |
| 3 | 服务频次 | 1次 |

### 5.3.2培训服务

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
| 1 | 服务内容 | 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。 |
| 2 | 服务范围 | 针对设备管理人员 |
| 3 | 服务频次 | 1次 |

### 5.3.3等保安全服务

#### 5.3.3.1渗透测试

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
|  | 服务内容 | 需在不影响业务正常开展的前提下，通过模拟黑客攻击的方式，验证信息系统抵御黑客攻击的能力，从而发现信息系统的安全隐患和脆弱点，并提出安全整改建议，以指导相关人员对系统进行安全优化和加固。 |
|  | 服务要求 | 考虑到本项服务对服务工程师技术能力要求，投标人须明确本服务项的服务人员名单，所派遣的服务人员须具备软考信息安全工程师证书。 |
|  | 服务范围 | 针对密码监督管理信息平台 |
|  | 服务频次 | 1次 |
|  | 服务成果 | 《渗透测试报告》 |

#### 5.3.3.2策略加固

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
|  | 服务内容 | 需通过技术手段对信息系统相关的操作系统、数据库、中间件、网络与安全设备进行安全策略加强、调优，加强网络、系统和设备抵御攻击和威胁的能力，整体提高网络安全防护水平。 |
|  | 服务要求 | 投标人需在投标方案中明确策略加固工作的流程、服务方式等。 |
|  | 服务范围 | 针对密码监督管理信息平台内的设备 |
|  | 服务频次 | 1次 |
|  | 服务成果 | 《策略加固报告》 |

#### 5.3.3.3制度完善

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
|  | 服务内容 | 需基于信息系统安全等级，根据信息安全等级保护管理要求，从信息安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理五个方面对现有信息安全管理制度进行优化和修订，达到国家信息安全等级保护管理要求。 |
|  | 服务要求 | 考虑项目所需人员能力要求，投标人须明确本服务项的服务人员名单，所派遣的服务人员须具备等级保护建设专业人员资质。 |
|  | 服务范围 | 针对密码监督管理信息平台 |
|  | 服务频次 | 1次 |
|  | 服务成果 | 完善后符合等保要求的《安全管理制度报告》 |

### 5.3.4等级保护测评服务

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
|  | 服务内容 | 投标人须邀请具备信息安全等级保护测评资质的测评机构针对招标人指定的信息系统展开等级测评，信息系统安全等级测评是依据国家相关政策文件要求，遵循公开、公平和公正原则，对用户信息系统的安全保障状况进行符合性安全测试和评估，评价该信息系统是否满足安全等级测评要求中的各项安全技术指标和安全考核目标。 |
|  | 服务要求 | 考虑到本项服务对服务工程师技术能力的要求，投标人须明确本服务项的服务人员名单，所派遣的服务人员须具备信息安全等级测评师高级证书。 |
|  | 服务范围 | 针对用户指定的1个系统 |
|  | 服务频次 | 1次 |
|  | 服务成果 | 《信息系统等级测评报告》 |

# 六、集成建设实施要求

## 6.1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）参加的联络会，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。

## 6.2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、人员安排等。

## 6.3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。

## 6.4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（包括但不限于）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》 | 提交设备调试报告 |
| 培训 | 《培训签到表》《培训材料》 | 提交培训记录表单 |
| 验收及交付 | 《验收报告》 | 提交所有验收成果 |

## 6.5验收要求

在系统试运行结束后，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。

## 6.6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。

# 七、培训与技术支持

## 7.1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。

## 7.2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）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招标人提供技术支持，同时为其它应用系统的集成等提供技术支持。