**一、说明**

**1 总则**

1.1 投标人应具备国家或行业管理部门规定的，在本市实施本项目所需的资格（资质）和相关手续（如果有），由此引起的所有有关事宜及费用由投标人自行负责。

1.2 投标人对所提供的系统应当享有合法的所有权，没有侵犯任何第三方的知识产权、技术秘密等权利，而且不存在任何抵押、留置、查封等产权瑕疵。

1.3 投标人提供的货物应当是全新的、未使用过的，货物和相关服务应当符合招标文件的要求，并且其质量完全符合国家标准、行业标准或地方标准。

1.4 投标人应如实准确地填写投标货物的规格型号、技术参数、品牌、产地等相关信息，因上述信息内容填写不完整、不准确，而导致投标文件被误读、漏读，由投标人自行负责，为此投标人需承担其投标文件在评标时被扣分甚至被认定为无效投标的风险。

★1.5若本项目涉及国家强制认证产品（信息安全产品、3C认证产品、强制节能产品、电信设备进网许可证等），则根据国家有关规定，投标人提供的产品必须满足强制认证要求。（详见第一章投标人须知及前附表21.3（9））

★1.6投标人提供的产品和服务必须符合国家强制性标准。

1.7 采购人在技术需求和图纸或图片（如果有）中指出的工艺、材料和货物的标准以及参照的技术参数或型号仅起说明作用，并没有任何限制性和排他性，投标人在投标中可以选用其他替代标准、技术参数或型号，但这些替代要在不影响功能实现的前提下，并在可接受范围内接受偏离。

1.8 投标人在投标前应认真了解采购人的使用需求、使用条件（使用空间、能源条件等）和其他相关条件，一旦中标，应按照招标文件和合同规定的要求提供货物及相关服务。

1.9 投标人应根据本章节中详细技术规格要求，采用市场主流产品或按照要求提供定制产品参加竞标。同时，**请投标人务必注意：无论是正偏离还是负偏离，都不得与招标要求相差太大，否则将可能影响投标人的得分**。一旦中标，投标人应按投标文件的承诺签订合同并提供相应的产品和服务。

1.10本项目如涉及软件开发，则开发软件（包括软件、源程序、数据文件、文档、记录、工作日志、或其它和该合同有关的资料的）的全部知识产权归采购人所有。投标人向采购人交付使用的软件系统已享有知识产权的，采购人可在合同文件明确的范围内自主使用。支撑该系统开发和运行的第三方编制的软件的知识产权仍属于第三方。如采购人使用该软件系统构成上述侵权的，则由投标人承担全部责任。

1.11投标人认为招标文件（包括招标补充文件）存在排他性或歧视性条款，自收到招标文件之日或者招标文件公告期限届满之日起七个工作日内，以书面形式提出，并附相关证据。

**二、项目概况**

**2项目名称**

上海市公安局浦东分局网络信息安全加固升级项目

**3项目地点**

上海市浦东新区内用户指定地点。

**4 招标范围与内容**

**4.1 项目背景及现状**

近年来公安部、市公安局出台多个网络安全等级保护相关文件，新区政府发文要求落实网络安全主体责任。本项目将国家有关法律法规、公安部、市局、浦东新区有关政策文件作为建设依据，对照浦东分局公安信息网络安全现状及实际需求，运用安全技术、安全管理、安全运营和安全服务理念，开展网络安全加固升级工作，进一步完善浦东公安分局信息网络基础安全防护体系建设。

**4.2 项目招标范围及内容**

**4.2.1建设目标**

本项目旨在针对浦东公安分局公安信息网、公安视频传输网、公安移动信息网以及分局互联网接入平台进行整体安全框架设计，并针对性地进行安全加固，符合公安部、市局对相关网络安全的相应要求，堵塞漏洞、消除安全隐患，全面落实安全运行监管职责，提升边界安全保障能力和网络安全防护水平。具体建设目标包括：

（1）对公安信息网、公安视频传输网进行网络安全加固，满足网络安全等级保护三级的相应技术要求；对照网络安全等级保护二级的相应技术要求，对互联网接入平台、交通专网、公安移动信息网（公安信息网II类区）进行网络安全加固。

（2）建设公安信息网与公安视频传输网、公安信息网与与电子政务外网边界、公安视频传输网与电子政务外网（视频层）、公安视频传输网与VPDN专网的4条边界，满足市局对公安信息网、视频传输网等非涉密网络边界建设及使用要求。

（3）开发安全管理平台软件，在公安信息网、公安视频传输网中各部署1 套。实现安全态势可知、可控、可查、可溯，提升网络安全风险的监测、预警、分析效率，增强对突发网络安全事件监测和处置能力。

（4）对公安信息网和公安视频传输网开展网络系统密码保护应用，通过商用密码应用安全性评估。

**4.2.2建设范围**

浦东公安分局公安信息网、公安视频传输网、公安移动信息网、交通专网及分局互联网接入平台各信息机房。

**4.2.3建设内容**

**（1）网络安全加固**

 1）公安信息网信息安全加固升级建设

基于三级等保技术要求，开展安全技术措施加固，完成流量监测系统、高级持续性威胁检测设备、攻击诱捕系统、API应用安全审计设备、网络管理系统、交换机的建设；完成采购人提供设备配件及软件的配套建设。

2）公安视频传输网信息安全加固升级建设

基于三级等保技术要求，开展安全技术措施加固，完成流量监测系统、高级持续性威胁检测设备、网络管理系统、交换机的建设；完成采购人提供设备配件及软件的配套建设。

3）互联网接入平台安全升级改造

参照二级等保相应技术要求，开展安全技术措施加固，完成流量监测系统、设备安全准入控制系统、网络安全综合防护设备的建设；完成采购人提供设备配件及软件的配套建设。拓展互联网接入平台网络覆盖范围，完成南片区骨干节点交换机、分支节点交换机，接入平台核心交换机、RADIUS服务器、宽带接入服务器及数据库存储盘阵的建设。

4）交通专网加固升级

参照二级等保相应技术要求，开展安全技术措施加固，完成采购人提供设备配件及软件的配套建设。

5）公安移动信息网（公安信息网II类区）安全建设

参照等保二级相应技术要求，开展安全技术措施加固，完成网络安全综合防护设备、API应用安全审计设备、态势流量探针的建设；完成采购人提供设备配件及软件的配套建设。

**（2） 网络安全边界建设**

1）公安信息网与公安视频传输网的安全边界

实现视频流和图像数据（包括图片、特征值及其结构化描述信息等）从视频传输网至公安信息网的单向传输。完成边界安全网关、集控探针、视频安全交换系统（前/后置）、数据安全交换系统（前/后置）、边界安全集中监控管理系统、流量监测系统、交换机的建设；完成采购人提供设备配件及软件的配套建设。

2）公安信息网与电子政务外网安全边界

实现公安信息网与电子政务外网以文件交换的方式进行双单向文件导入。完成边界安全网关、集控探针、高级持续性威胁检测设备、数据安全交换系统（前/后置）、流量监测系统、交换机的建设；采购人提供设备配件及软件的配套建设。

3）公安视频传输网与电子政务外网（视频层）边界

实现视频流和图像数据（包括图片、特征值及其结构化描述信息等）的双向传输。完成设备准入控制系统、集控探针、视频安全交换系统（前/后置）、数据安全交换系统（前/后置）、边界安全集中监控管理系统、流量监测系统、交换机的建设。完成采购人提供设备配件及软件的配套建设。

4）公安视频传输网与VPDN专网边界

实现视频流双单向传输、图像数据（包括图片、特征值及其结构化描述信息等）从VPDN专网向公安视频传输网的单向传输。完成设备准入控制系统、集控探针、视频安全交换系统（前/后置）、数据安全交换系统（前/后置）、流量监测系统、交换机的建设。完成采购人提供设备配件及软件的配套建设。

**（3）安全管理平台建设**

开发安全管理平台软件，在公安信息网、公安视频传输网中各部署1 套。包括数据采集、分析识别、安全防护、检测评估、监测预警、主动防御、事件处置、系统管理、态势可视化、信息互通管理、安全风险警示服务等子系统。

**（4）密码应用建设**

完成分局主控机房国密门禁系统和视频监控国密改造系统的建设；完成公安信息网和视频传输网密码应用改造。完成采购人提供设备的配套建设。

**4.3 工期**

本项目工期为自合同签订之日起365个日历日内，项目竣工日期以合同验收通过的日期为准。

本项目进度要求：

（1）项目开工令下达后30个日历日内，完成主要硬件设备的到货；

（2）项目开工令下达后60个日历日内，完成安全边界调试与开通；

（3）项目开工令下达后120个日历日内，完成软件《需求规格说明书》的确认工作；

（4）项目开工令下达后300个日历日内，系统具备试运行条件；

（5）项目开工令下达后365个日历日内，系统试运行完成，具备合同验收条件。

**5 承包方式**

5.1 依据本项目的招标范围和内容，中标人以包系统设计、包供货、包安装集成调试、包质量、包安全的方式实施总承包。

5.2本项目不允许分包。

**6 合同的签订**

6.1 本项目合同的标的、价格、质量及验收标准、考核管理、履约期限等主要条款应当与招标文件和中标人投标文件的内容一致，并互相补充和解释。

**7 结算原则和支付方式**

**7.1 结算原则**

7.1.1本项目合同结算价以审计价为准，中标人的中标单价不变，实际工作量以采购人或第三方按照招标文件规定的验收标准核定为准。

7.1.2发生设备维修的，如该设备尚在质保期内的，采购人不另行支付相关费用；如在质保期外的，单价按照投标文件中明确的备品备件单价（含维修人工费）计取，数量按实结算。如投标文件中没有类似备品备件单价可参照的，则由合同双方协商确定维修单价。

7.1.3本项目审核收费按照下列方式支付（1）项目送审价核减率在5%以内的（含5%），由采购人负担审核费用；（2）核减率在5%以上的，5%以内的（含5%）审核费用由采购人负担，超过部分由中标人负担；（3）项目核减、核增部分分别计算审核费用，核增部分由中标人负担审核费用。

**7.2 支付方式**

7.2.1 本项目合同金额采用**分期付款**方式，在采购人和中标人合同签订，按下款要求支付相应的合同款项。

7.2.2分期付款的时间进度要求和支付比例具体如下：

（1）第一笔付款：在合同签订后30日内，采购人向中标人支付合同金额的30%；

（2）第二笔付款：主要设备到货后30日内，采购人向中标人支付合同金额的20%；

（3）第三笔付款：项目完成合同验收通过后30日内，采购人向中标人支付合同金额的10%；

（4）第四笔付款：项目完成整体验收通过后30日内，采购人向中标人支付合同金额的10%；

（5）第五笔付款：在项目审计结束后30日内，按审计结果及合同履约情况支付剩余款项。

7.3中标人因自身原因造成返工的工作量，采购人将不予计量和支付。

7.4采购人不得以法定代表人或者主要负责人变更，履行内部付款流程，或者在合同未作约定的情况下以等待竣工验收批复、决算审计等为由，拒绝或者延迟支付中小企业款项。如发生延迟支付情况，应当支付逾期利息，且利率不行低于合同订立时1年期贷款市场报价利率。

**三、技术质量要求**

**8 适用技术规范和规范性文件**

《计算机信息系统安全等级保护划分准则》（GB 17859-1999）

《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T 25070-2019）

《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 网络安全等级保护安全管理中心技术要求》（GB/T 36958-2018）

《信息安全技术 网络安全等级保护实施指南》（GB/T 25058-2019）

《信息安全技术 网络安全等级保护实施指南》（GB/T 25058-2019）

《信息安全技术 信息系统密码应用基本要求》（GB/T39786-2021）

《信息安全技术 信息安全产品类别与代码》（GB/T25066-2020）

《公安视频图像信息系统安全技术要求》（GA/T1788-2021）

《公安视频图像信息系统安全技术要求 第1部分：通用要求》（GA/T 1788.1-2021）

《公安视频图像信息系统安全技术要求 第2部分：前端设备》（GA/T 1788.2-2021）

《公安视频图像信息系统安全技术要求 第3部分：安全交互》（GA/T 1788.3-2021）

《公安视频图像信息系统安全技术要求 第4部分：安全管理平台》（GA/T 1788.4-2021）

《公共安全视频监控联网系统信息传输、交换、控制技术要求》（GB/T 28181-2022）

《公共安全视频监控联网信息安全技术要求》（GB 35114-2017 ）

《公安移动信息网技术要求》（GA/T1737-2020）

《公安大数据安全 总体技术框架》（GA DSJ 300-2019）

《公安大数据安全安全防护体系技术设计要求》（GA/DSJ 352-2019）

各投标人应充分注意，凡涉及国家或行业管理部门颁发的相关规范、规程和标准，无论其是否在本招标文件中列明，中标人应无条件执行。标准、规范等不一致的，以要求高者为准。

**9 招标内容与质量要求**

**9.1工作量清单**

**工作量清单**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **具体内容** | **数量** | **工期** | **备注** |
| 1 | 网络安全加固升级 | 详见9.1.1网络安全加固升级 | 1  | 365个日历日 | **●** |
| 2 | 网络安全边界建设 | 详见9.1.2网络安全边界建设 | 1 | **●** |
| 3 | 安全管理平台建设 | 详见9.1.3安全管理平台建设 | 1 | **●** |
| 4 | 密码应用建设 | 详见9.1.4密码应用建设 | 1 | **●** |

**说明：上表中所列为本次招标的主要工作内容，其中“●”标记的内容为本项目的核心工作内容，投标人不得减少核心工作内容数量。**

**9.1.1网络安全加固升级**

| **序号** | **项目** | **技术参数** | **单位** | **数量** | **备注** |
| --- | --- | --- | --- | --- | --- |
| **1** | **公安信息网安全加固** |
| 1.1 | 流量监测系统 | 详见10.2.1 | 套 | 2 | **●** |
| 1.2 | 高级持续性威胁检测设备 | 详见10.2.3 | 套 | 2 | **●** |
| 1.3 | 攻击诱捕系统（蜜罐） | 详见10.2.4 | 套 | 1 | **●** |
| 1.4 | API应用安全审计设备 | 详见10.2.5 | 套 | 1 | **●** |
| 1.5 | 交换机 | 详见10.2.7 | 台 | 2 | **●** |
| 1.6 | 网络管理系统 | 详见10.2.28 | 套 | 1 | **●** |
| 1.7 | 安全设备光模块 |  | 个 | 38 |  |
| 1.7.1 | 边界防火墙光模块 | 适配本项目采购交换机及采购人提供设备1.1参数详见3.15.1 | 块 | 8 |  |
| 1.7.2 | 入侵检测设备光模块 | 适配本项目采购交换机及采购人提供设备1.2参数详见3.15.1 | 块 | 4 |  |
| 1.7.3 | 网络行为审计设备光模块 | 适配本项目采购交换机及采购人提供设备1.3参数详见3.15.1 | 块 | 4 |  |
| 1.7.4 | 数据库审计设备光模块 | 适配本项目采购交换机及采购人提供设备1.5参数详见3.15.1 | 块 | 4 |  |
| 1.7.5 | 管理&业务防火墙光模块 | 适配本项目采购交换机及采购人提供设备1.6参数详见3.15.1 | 块 | 8 |  |
| 1.7.6 | 日志审计设备光模块 | 适配本项目采购交换机及采购人提供设备1.7参数详见3.15.1 | 块 | 4 |  |
| 1.7.7 | 设备安全运维与审计设备光模块 | 适配本项目采购交换机及采购人提供设备1.8参数详见3.15.1 | 块 | 4 |  |
| 1.7.8 | 网络脆弱性扫描设备光模块 | 适配本项目采购交换机及采购人提供设备1.9参数详见3.15.2 | 块 | 2 |  |
| 1.8 | 采购人提供设备的特征库/软件升级及对接 | 包含2套边界防火墙、2套入侵检测设备、2套网络行为审计设备、2套WEB应用防火墙、2套数据库审计、2套管理&业务防火墙、2套设备安全运维与审计设备、1套网络脆弱性扫描设备的三年特征库/软件全功能升级、SDK对接 | 项 | 1 |  |
| 1.9 | 日志审计存储设备 | 规格：标准机架，冗余电源；容量：40TB接口：2\*千兆电口 | 套 | 1 |  |
| 1.10 | 通用服务器磁盘 | 适用于通用服务器8TB 3.5吋 7200转 6Gbps SATA | 套 | 36 |  |
| **2** | **公安视频传输网加固升级** |
| 2.1 | 流量监测系统 | 详见10.2.1 | 套 | 2 | **●** |
| 2.2 | 高级持续性威胁检测设备 | 详见10.2.3 | 套 | 1 | **●** |
| 2.3 | 交换机 | 详见10.2.7 | 台 | 2 | **●** |
| 2.4 | 网络管理系统 | 详见10.2.28 | 套 | 1 | **●** |
| 2.5 | 安全设备光模块 |  | 个 | 36 |  |
| 2.5.1 | 边界防火墙光模块 | 适配本项目采购交换机及采购人提供设备2.1参数详见3.15.1 | 块 | 8 |  |
| 2.5.2 | 入侵检测设备光模块 | 适配本项目采购交换机及采购人提供设备2.2参数详见3.15.1 | 块 | 4 |  |
| 2.5.3 | 网络行为审计设备光模块 | 适适配本项目采购交换机及采购人提供设备2.3参数详见3.15.1 | 块 | 4 |  |
| 2.5.4 | 数据库审计设备光模块 | 适配本项目采购交换机及采购人提供设备2.5参数详见3.15.1 | 块 | 2 |  |
| 2.5.5 | 管理&业务防火墙光模块 | 适配本项目采购交换机及采购人提供设备2.6参数详见3.15.1 | 块 | 8 |  |
| 2.5.6 | 日志审计设备光模块 | 适配本项目采购交换机及采购人提供设备2.7参数详见3.15.1 | 块 | 4 |  |
| 2.5.7 | 设备安全运维与审计设备光模块 | 适配本项目采购交换机及采购人提供设备2.8参数详见3.15.1 | 块 | 4 |  |
| 2.5.8 | 网络脆弱性扫描设备光模块 | 适配本项目采购交换机及采购人提供设备2.9参数详见3.15.2 | 块 | 2 |  |
| 2.6 | 采购人提供设备的特征库/软件升级及对接 | 包含2套边界防火墙、2套入侵检测设备、2套网络行为审计设备、2套WEB应用防火墙、1套数据库审计、2套管理&业务防火墙、2套设备安全运维与审计设备、1套网络脆弱性扫描设备的三年特征库/软件全功能升级、SDK对接 | 项 | 1 |  |
| 2.7 | 日志审计存储设备 | 规格：标准机架，冗余电源；容量：40TB接口：2\*千兆电口 | 套 | 1 |  |
| 2.8 | 通用服务器磁盘 | 适配采购人提供设备2.108TB 3.5吋 7200转 6Gbps SATA | 套 | 36 |  |
| **3** | **互联网接入平台加固升级** |
| 3.1 | 流量监测系统 | 详见10.2.1 | 套 | 1 | **●** |
| 3.2 | 网络安全综合防护设备 | 详见10.2.9 | 套 | 1 | **●** |
| 3.3 | 设备安全准入控制系统 | 详见10.2.10 | 套 | 1 | **●** |
| 3.4 | 交换机 | 详见10.2.8 | 台 | 1 |  |
| 3.5 | 安全设备光模块 |  | 个 | 14 |  |
| 3.5.1 | 抗拒绝服务攻击设备光模块 | 适配本项目采购交换机及采购人提供设备3.1参数详见3.15.1 | 块 | 4 |  |
| 3.5.2 | 边界防火墙光模块 | 适配本项目采购交换机及采购人提供设备3.2参数详见3.15.1 | 块 | 4 |  |
| 3.5.3 | 入侵检测光模块 | 适配本项目采购交换机及采购人提供设备3.3参数详见3.15.1 | 块 | 2 |  |
| 3.5.4 | 管理&业务防火墙光模块 | 适配本项目采购交换机及采购人提供设备3.4参数详见3.15.1 | 块 | 2 |  |
| 3.5.5 | WEB应用防火墙光模块 | 适配本项目采购交换机及采购人提供设备3.5参数详见3.15.1 | 块 | 2 |  |
| 3.6 | 采购人提供设备的特征库/软件升级 | 包含1套抗拒绝服务攻击设备、1套边界防火墙、1套入侵检测设备、1套管理&业务防火墙、1套WEB应用防火墙的三年特征库/软件全功能升级 | 项 | 1 |  |
| 3.7 | 宽带接入服务器BRAS | 详见10.2.11 | 台 | 1 | **●** |
| 3.8 | Radius硬件平台 | 详见10.2.12 | 套 | 2 | **●** |
| 3.9 | 数据库存储盘阵 | 详见10.2.13 | 台 | 1 | **●** |
| 3.10 | 汇聚交换机 | 详见10.2.14 | 台 | 6 | **●** |
| 3.11 | 派出所接入交换机 | 详见10.2.15 | 台 | 31 | **●** |
| 3.12 | 出口转接交换机 | 详见10.2.16 | 台 | 2 | **●** |
| 3.13 | 核心交换机 | 详见10.2.17 | 台 | 1 | **●** |
| 3.14 | 网管接入交换机 | 详见10.2.18 | 台 | 3 | **●** |
| 3.15 | 交换机接口模块 |  |  | 93 |  |
| 3.15.1 | 万兆多模光模块 | 类型：SFP+，标准：10Gbase-SR，接口：LC，光纤类型：多模，传输距离：>=300M | 个 | 11 |  |
| 3.15.2 | 千兆多模光模块 | 类型：SFP，标准：1000Base-X，接口：LC，光纤类型：多模，传输距离：>=300M | 个 | 2 |  |
| 3.15.3 | 万兆单模SFP+光模块10km | 类型：SFP+，标准：10Gbase-LR，接口：LC，光纤类型：单模，传输距离：>=10KM | 个 | 4 |  |
| 3.15.4 | 万兆单模SFP+光模块40km | 类型：SFP+，标准：10Gbase-LR，接口：LC，光纤类型：单模，传输距离：>=40KM | 个 | 6 |  |
| 3.15.5 | 千兆单模SFP光模块10km | 类型：SFP，标准：1000Base-X，接口：LC，光纤类型：单模，传输距离：>=10KM | 个 | 50 |  |
| 3.15.6 | 千兆单模SFP光模块40km | 类型：SFP，标准：1000Base-X，接口：LC，光纤类型：单模，传输距离：>=40KM | 个 | 16 |  |
| 3.15.7 | 千兆SFP电口模块100m | 类型：SFP，标准：1000Base-T，接口：RJ45，传输距离：>=100m | 个 | 4 |  |
| 3.16 | 电源PDU | 16A--8联PDU，10A-万用孔插口6个，16A插孔2个，3米线，带16A工业连接器 | 处 | 34 |  |
| **4** | **交通专网加固升级** |
| 4.1 | 交换机 | 详见10.2.8 | 台 | 1 |  |
| 4.2 | 安全设备光模块 |  | 块 | 24 |  |
| 4.2.1 | 边界防火墙光模块 | 适配本项目采购交换机及采购人提供设备4.1参数详见3.15.1 | 块 | 8 |  |
| 4.2.2 | 网闸光模块 | 适配本项目采购交换机及采购人提供设备4.2参数详见3.15.1 | 块 | 8 |  |
| 4.2.3 | 网络行为审计设备光模块 | 适配本项目采购交换机及采购人提供设备4.3参数详见3.15.1 | 块 | 2 |  |
| 4.2.4 | 管理区防火墙光模块 | 适配本项目采购交换机及采购人提供设备4.4参数详见3.15.1 | 块 | 2 |  |
| 4.2.5 | 设备安全运维与审计设备光模块 | 适配本项目采购交换机及采购人提供设备4.5参数详见3.15.1 | 块 | 2 |  |
| 4.2.6 | 日志审计设备光模块 | 适配本项目采购交换机及采购人提供设备4.6参数详见3.15.1 | 块 | 2 |  |
| 4.3 | 采购人提供设备的特征库/软件升级 | 包括2套边界防火墙、1套网络行为审计、1套管理区防火墙、 1套设备安全运维与审计的三年特征库/软件全功能升级  | 项 | 1 |  |
| **5** | **公安移动信息网加固** |
| 5.1 | 网络安全综合防护设备 | 详见10.2.9 | 套 | 1 | **●** |
| 5.2 | API应用安全审计设备 | 详见10.2.5 | 套 | 1 | **●** |
| 5.3 | 流量监测系统 | 详见10.2.2 | 套 | 1 | **●** |
| 5.4 | 交换机 | 详见10.2.7 | 台 | 1 |  |
| 5.5 | 边界防火墙光模块 | 适配本项目采购交换机及采购人提供设备5.1参数详见3.15.1 | 块 | 4 |  |
| 5.6 | 边界防火墙特征库 | 适配采购人提供设备5.1三年全功能升级 | 套 | 2 |  |

**说明：上表中“●”标记的内容为本项目拟采购的核心设备，投标人在做投标方案时对该部分设备的数量不得进行缩减，并在分项报价明细表中详细列出。**

**上表中若有产品原厂授权的承诺由原厂提供SDK，并提供相应的调试服务的，可在投标文件中提供。**

**9.1.2网络安全边界建设**

| **序号** | **项目** | **技术参数** | **单位** | **数量** | **备注** |
| --- | --- | --- | --- | --- | --- |
| **1** | **公安信息网与视频传输网边界** |
| 1.1 | 接入交换机 | 详见10.2.8 | 台 | 1 |  |
| 1.2 | 边界安全网关 | 详见10.2.19 | 项 | 1 | **●** |
| 1.3 | 集控探针 | 详见10.2.20 | 台 | 2 | **●** |
| 1.4 | 互联交换机 | 详见10.2.8 | 台 | 2 |  |
| 1.5 | 视频安全交换系统（前/后置） | 详见10.2.21 | 套 | 2 | **●** |
| 1.6 | 数据安全交换系统（前/后置） | 详见10.2.22 | 套 | 2 | **●** |
| 1.7 | 边界安全集中监控管理系统 | 详见10.2.23 | 套 | 1 | **●** |
| 1.8 | 边界流量监测系统 | 详见10.2.24 | 套 | 1 | **●** |
| 1.9 | 边界汇聚交换机 | 详见10.2.7 | 台 | 1 |  |
| 1.10 | 防火墙（含IPS）光模块 | 适配本项目采购交换机及采购人提供设备6.1参数详见3.15.1 | 块 | 4 |  |
| 1.11 | 防火墙（含IPS）特征库 | 适配采购人提供设备6.1三年全功能升级 | 套 | 2 |  |
| 1.12 | 网闸（视频交换链路）光模块 | 适配本项目采购交换机及采购人提供设备6.2参数详见3.15.1 | 块 | 4 |  |
| 1.13 | 单向光闸（数据交换链路）光模块 | 适配本项目采购交换机及采购人提供设备6.3参数详见3.15.1 | 块 | 8 |  |
| **2** | **公安信息网与电子政务外网边界**  |
| 2.1 | 接入交换机 | 详见10.2.8 | 台 | 1 |  |
| 2.2 | 边界安全网关 | 详见10.2.19 | 项 | 1 | **●** |
| 2.3 | 集控探针 | 详见10.2.20 | 台 | 1 | **●** |
| 2.4 | 互联交换机 | 详见10.2.8 | 台 | 1 |  |
| 2.5 | 高级持续性威胁检测（APT） | 详见10.2.3 | 套 | 1 | **●** |
| 2.6 | 数据安全交换系统（前/后置） | 详见10.2.22 | 套 | 2 | **●** |
| 2.7 | 边界流量监测系统 | 详见10.2.24 | 套 | 1 | **●** |
| 2.8 | 边界汇聚交换机 | 详见10.2.7 | 台 | 1 |  |
| 2.9 | 防火墙（含IPS）光模块 | 适配本项目采购交换机及采购人提供设备7.1参数详见3.15.1 | 块 | 2 |  |
| 2.10 | 防火墙（含IPS）特征库 | 适配采购人提供设备7.1三年全功能升级 | 套 | 1 |  |
| 2.11 | 单向光闸（数据交换链路）光模块 | 适配本项目采购交换机及采购人提供设备7.2参数详见3.15.1 | 块 | 8 |  |
| **3** | 视频传输网与政务外网（视频层）边界 |
| 3.1 | 接入交换机 | 详见10.2.8 | 台 | 1 |  |
| 3.2 | 设备准入控制 | 详见10.2.25 | 套 | 1 | **●** |
| 3.3 | 集控探针 | 详见10.2.20 | 台 | 1 | **●** |
| 3.4 | 互联交换机 | 详见10.2.8 | 台 | 1 | **●** |
| 3.5 | 视频安全交换系统（前/后置） | 详见10.2.21 | 套 | 2 | **●** |
| 3.6 | 数据安全交换系统（前/后置） | 详见10.2.22 | 套 | 2 | **●** |
| 3.7 | 边界流量监测系统 | 详见10.2.24 | 套 | 1 | **●** |
| 3.8 | 边界安全集中监控管理系统 | 详见10.2.23 | 套 | 1 | **●** |
| 3.9 | 边界汇聚交换机 | 详见10.2.7 | 台 | 1 |  |
| 3.10 | 防火墙（含IPS）光模块 | 适配本项目采购交换机及采购人提供设备8.1参数详见3.15.1 | 块 | 2 |  |
| 3.11 | 防火墙（含IPS）特征库 | 适配采购人提供设备8.1三年全功能升级 | 套 | 1 |  |
| 3.12 | 网闸（视频交换链路）光模块 | 适配本项目采购交换机及采购人提供设备8.2参数详见3.15.1 | 块 | 4 |  |
| 3.13 | 网闸（数据交换链路）光模块 | 适配本项目采购交换机及采购人提供设备8.3参数详见3.15.1 | 块 | 4 |  |
| **4** | 视频传输网与VPDN边界 |
| 4.1 | 接入交换机 | 详见10.2.8 | 台 | 1 |  |
| 4.2 | 设备准入控制 | 详见10.2.25 | 套 | 1 | **●** |
| 4.3 | 集控探针 | 详见10.2.20 | 台 | 1 | **●** |
| 4.4 | 互联交换机 | 详见10.2.8 | 台 | 1 | **●** |
| 4.5 | 视频安全交换系统（前/后置） | 详见10.2.21 | 套 | 2 | **●** |
| 4.6 | 数据安全交换系统（前/后置） | 详见10.2.23 | 套 | 2 | **●** |
| 4.7 | 边界流量监测系统 | 详见10.2.24 | 套 | 1 | **●** |
| 4.8 | 边界汇聚交换机 | 详见10.2.7 | 台 | 1 |  |
| 4.9 | 防火墙（含IPS）光模块 | 适配本项目采购交换机及采购人提供设备9.1参数详见3.15.1 | 块 | 2 |  |
| 4.10 | 防火墙（含IPS）特征库 | 适配采购人提供设备9.1三年全功能升级 | 套 | 1 |  |
| 4.11 | 单向光闸（视频交换链路）光模块 | 适配本项目采购交换机及采购人提供设备9.2参数详见3.15.1 | 块 | 8 |  |
| 4.12 | 单向光闸（数据交换链路）光模块 | 适配本项目采购交换机及采购人提供设备9.3参数详见3.15.1 | 块 | 8 |  |

**说明：上表中“●”标记的内容为本项目拟采购的核心设备，投标人在做投标方案时对该部分设备的数量不得进行缩减，并在分项报价明细表中详细列出。**

**上表中若有产品原厂授权的承诺由原厂提供SDK，并提供相应的调试服务的，可在投标文件中提供。**

**9.1.3安全管理平台建设**

| **序号** | **项目** | **技术要求** | **单位** | **数量** | **备注** |
| --- | --- | --- | --- | --- | --- |
| 1.1 | 数据采集子系统 | 详见10.1.3.1 | 项 | 1 | **●** |
| 1.2 | 分析识别子系统 | 详见10.1.3.2 | 项 | 1 | **●** |
| 1.3 | 安全防护子系统 | 详见10.1.3.3 | 项 | 1 | **●** |
| 1.4 | 检测评估子系统 | 详见10.1.3.4 | 项 | 1 | **●** |
| 1.5 | 监测预警子系统 | 详见10.1.3.5 | 项 | 1 | **●** |
| 1.6 | 主动防御子系统 | 详见10.1.3.6 | 项 | 1 | **●** |
| 1.7 | 事件处置子系统 | 详见10.1.3.7 | 项 | 1 | **●** |
| 1.8 | 态势可视化子系统 | 详见10.1.3.8 | 项 | 1 | **●** |
| 1.9 | 系统管理子系统 | 详见10.1.3.9 | 项 | 1 | **●** |
| 1.10 | 信息互通管理子系统 | 详见10.1.3.10 | 项 | 1 | **●** |
| 1.11 | 安全风险警示服务子系统 | 详见10.1.3.11 | 项 | 1 | **●** |
| 1.12 | 安全管理平台密码改造 | 详见10.1.3.12 | 项 | 1 | **●** |
| 1.13 | 安管平台部署 | 在公安信息网和公安视频传输网内各部署1套 | 项 | 1 | **●** |

**说明：上表中“●”标记的内容为本项目拟采购的核心内容，投标人在做投标方案时对该部分开发内容不得进行缩减，并在分项报价明细表中详细列出。**

**9.1.4密码应用建设**

| **序号** | **项目** | **技术参数** | **单位** | **数量** | **备注** |
| --- | --- | --- | --- | --- | --- |
| **一** | **公安信息网密码应用** |
| 1.1 | 安全门禁系统 | 详见10.2.26 | 套 | 1 | **●** |
| 1.2 | 视频监控国密改造系统 | 详见10.2.27 | 套 | 1 | **●** |
| 1.3 | SSL VPN授权 | 适配采购人提供设备10.3 | 个 | 200 |  |
| 1.4 | 公安信息网密码应用改造 | 详见10.1.4 | 项 | 1 |  |
| **二** | **公安视频传输网密码应用** |
| 2.1 | SSL VPN授权 | 适配采购人提供设备11.3 | 个 | 200 |  |
| 2.2 | 公安视频传输网密码应用改造 | 详见10.1.4 | 项 | 1 |  |

**说明：上表中“●”标记的内容为本项目拟采购的核心内容，投标人在做投标方案时对该部分开发内容不得进行缩减，并在分项报价明细表中详细列出。**

**9.1.5与相关设备、系统的界面**

（1）与网络内已有设备界面

本项目与现有网络中已有设备的硬件界面（物理界面）在各机房节点交换机；

本项目新建设备需接入在用交换机侧的，由本项目负责实施，交换机维护单位配合。

（2）与采购人提供设备界面

本项目与采购人提供设备的硬件界面（物理界面）在采购人提供设备的网络接口。

（3）与上级相关平台/系统的数据界面

与上级单位网络安全管理平台的数据对接由本项目负责实施。

与上级单位网络管理系统的数据对接由本项目负责实施。

与上级单位边界安全监测平台的数据对接由本项目负责实施。

**9.1.6关于本项目工作量的进一步说明**

本项目新增设备的安装位置、供电、通信网络等由采购人负责提供，本项目负责设备的安装、调试与开通；

本项目新增设备以及配套线缆和辅材等附属设施的采购、安装及调试的建设内容均由本项目负责实施；

需要特别说明的是，根据市局下发文件和区委对于信息化系统项目验收的要求，本项目投标人的投标报价中应包含完成本项目竣工验收所需的软件测试、边界评测等全部费用，以及项目免费运维期限内的商用密码应用安全性评估费，相关测评报告应由具备测评资质的第三方测评机构出具。

**9.1.7采购人提供设备清单**

**采购人提供设备清单**

| **序号** | **设备名称** | **技术参数** | **单位** | **数量** | **备注** |
| --- | --- | --- | --- | --- | --- |
| **1** | **公安信息网安全加固** |
| 1.1 | 边界防火墙 | 规格：标准机架安装；冗余电源；性能：网络层吞吐量≥80Gbps；并发连接≥3000万；每秒新建TCP连接数70万；接口：万兆光口≥8个，千兆电口≥8个，千兆光口≥8个，40G QSFP光口≥2个，1个HA接口；内存：32GB ；硬盘：1TB； | 台 | 2 |  |
| 1.2 | 入侵检测设备 | 规格：标准机架安装，冗余电源性能：IDS满检速率≥40Gbps接口：万兆光口≥4个，千兆光口≥4个，千兆电口≥4个；内存：32GB ；硬盘：≥8TB | 台 | 2 |  |
| 1.3 | 网络行为审计设备 | 规格：标准机架安装，冗余电源性能：应用层吞吐≥2.5Gbps，事件记录能力≥2.5万接口：万兆光口≥2个，千兆光口≥4个，千兆电口≥4个内存：16GB ；硬盘：≥1TB | 台 | 2 |  |
| 1.4 | WEB应用防火墙 | 规格：标准机架安装，冗余电源性能：HTTP应用层吞吐量≥9Gbps，HTTP最大并发连接数260万，HTTP最大请求速率 6万/秒；接口： 万兆光口≥2个，千兆光口≥4个，千兆电口≥6个内存：32GB 硬盘：SSD 64G+1T SATA | 台 | 2 |  |
| 1.5 | 数据库审计设备 | 规格：标准机架安装，冗余电源性能：SQL处理性能≥40000 条/s ，入库速率≥5000条/秒接口： 万兆光口≥2个，千兆光口≥4个，千兆电口≥6个内存：16GB 硬盘：4TB | 台 | 2 |  |
| 1.6 | 管理&业务防火墙 | 规格：标准机架安装；冗余电源；性能：网络层吞吐量≥80Gbps；并发连接≥3000万；每秒新建TCP连接数70万；接口：万兆光口≥8个，千兆电口≥8个，千兆光口≥8个，40G QSFP光口≥2个，1个HA接口光模块：万兆多模≥4个内存：32GB ；硬盘：1TB； | 台 | 2 |  |
| 1.7 | 日志审计设备 | 规格：标准机架安装，冗余电源；性能：日志处理能力5000EPS；接口：万兆光口≥2个，千兆电口≥4个 ，千兆光口≥4个 内存：16GB ；硬盘：4TB； | 台 | 2 |  |
| 1.8 | 设备安全运维与审计设备（堡垒机） | 规格：标准机架安装，冗余电源；性能：最大图形并发会话1000，最大字符并发数1000；接口：万兆光口≥2个，千兆电口≥4个 ，千兆光口≥4个 内存：16GB ；硬盘：256GBSSD+4TB SATA； | 台 | 2 |  |
| 1.9 | 网络脆弱性扫描设备（漏扫） | 规格：标准机架安装，冗余电源；性能：扫描IP地址无限制，最大并发任务数5，最大并发扫描主机数100；接口：千兆电口≥4个 ，千兆光口≥4个 内存：64GB ；硬盘：2TB； | 台 | 1 |  |
| 1.10 | 通用服务器 | CPU：主频2.6GHz 核数：64核 路数：2路内存：128G 系统盘：2x480GB SSD网卡：2x双口10G含双模块光纤网卡，2xPCI-E 千兆双口RJ45网卡 | 套 | 6 |  |
| 1.11 | 操作系统 | 国产linux操作系统，配套通用服务器 | 套 | 6 |  |
| 1.12 | 中间件 | 国产中间件软件 | 套 | 2 |  |
| 1.13 | 数据库软件 | 国产关系型数据库 | 套 | 3 |  |
| **2** | **公安视频传输网加固升级** |
| 2.1 | 边界防火墙 | 规格：标准机架安装；冗余电源；性能：网络层吞吐量≥80Gbps；并发连接≥3000万；每秒新建TCP连接数70万；接口：万兆光口≥8个，千兆电口≥8个，千兆光口≥8个，40G QSFP光口≥2个，1个HA接口；内存：32GB ；硬盘：1TB； | 台 | 2 |  |
| 2.2 | 入侵检测设备 | 规格：标准机架安装，冗余电源性能：IDS满检速率≥40Gbps接口：万兆光口≥4个，千兆光口≥4个，千兆电口≥4个；内存：32GB ；硬盘：≥8TB | 台 | 2 |  |
| 2.3 | 网络行为审计设备 | 规格：标准机架安装，冗余电源性能：应用层吞吐≥2.5Gbps，事件记录能力≥2.5万接口：万兆光口≥2个，千兆光口≥4个，千兆电口≥4个内存：16GB ；硬盘：≥1TB | 台 | 2 |  |
| 2.4 | WEB应用防火墙 | 规格：标准机架安装，冗余电源性能：HTTP应用层吞吐量≥9Gbps，HTTP最大并发连接数260万，HTTP最大请求速率 6万/秒；接口： 万兆光口≥2个，千兆光口≥4个，千兆电口≥6个内存：32GB 硬盘：SSD 64G+1T SATA。 | 台 | 2 |  |
| 2.5 | 数据库审计设备 | 规格：标准机架安装，冗余电源性能：SQL处理性能≥40000 条/s ，入库速率≥5000条/秒接口： 万兆光口≥2个，千兆光口≥4个，千兆电口≥6个内存：16GB 硬盘：4TB | 台 | 1 |  |
| 2.6 | 管理&业务防火墙 | 规格：标准机架安装；冗余电源；性能：网络层吞吐量≥80Gbps；并发连接≥3000万；每秒新建TCP连接数70万；接口：万兆光口≥8个，千兆电口≥8个，千兆光口≥8个，40G QSFP光口≥2个，1个HA接口光模块：万兆多模≥4个内存：32GB ；硬盘：1TB； | 台 | 2 |  |
| 2.7 | 日志审计设备 | 规格：标准机架安装，冗余电源；性能：日志处理能力5000EPS；接口：万兆光口≥2个，千兆电口≥4个 ，千兆光口≥4个 内存：16GB ；硬盘：4TB； | 台 | 2 |  |
| 2.8 | 设备安全运维与审计设备（堡垒机） | 规格：标准机架安装，冗余电源；性能：最大图形并发会话1000，最大字符并发数1000；接口：万兆光口≥2个，千兆电口≥4个 ，千兆光口≥4个 内存：16GB ；硬盘：256GBSSD+4TB SATA； | 台 | 2 |  |
| 2.9 | 网络脆弱性扫描设备（漏扫） | 规格：标准机架安装，冗余电源；性能：扫描IP地址无限制，最大并发任务数5，最大并发扫描主机数100；接口：千兆电口≥4个 ，千兆光口≥4个 内存：64GB ；硬盘：2TB； | 台 | 1 |  |
| 2.10 | 通用服务器 | CPU：主频2.6GHz 核数：64核 路数：2路内存：128G 系统盘：2x480GB SSD网卡：2x双口10G含双模块光纤网卡，2xPCI-E 千兆双口RJ45网卡 | 套 | 6 |  |
| 2.11 | 操作系统 | 国产linux操作系统，配套通用服务器 | 套 | 6 |  |
| 2.12 | 中间件 | 国产中间件软件 | 套 | 2 |  |
| 2.13 | 数据库软件 | 国产关系型数据库 | 套 | 3 |  |
| **3** | **互联网接入平台加固升级** |
| 3.1 | 抗拒绝服务攻击设备 | 规格：标准机架安装；冗余双电源性能：防御能力10Gbps，最大并发连接数800万，最大每秒新建连接数40万网络接口：4个千兆电口、4个万兆光口内存：32GB | 台 | 1 |  |
| 3.2 | 边界防火墙 | 格：标准机架安装；冗余电源；性能：网络层吞吐量≥80Gbps；并发连接≥3000万；每秒新建TCP连接数70万；接口：万兆光口≥8个，千兆电口≥8个，千兆光口≥8个，40G QSFP光口≥2个，1个HA接口内存：32GB ；硬盘：1TB； | 台 | 1 |  |
| 3.3 | 入侵检测设备 | 规格：标准机架安装，冗余电源性能：IDS满减速率≥10Gbps接口：万兆光口≥4个，千兆光口≥4个，千兆电口≥4个内存：32GB ；硬盘：≥8TB | 台 | 1 |  |
| 3.4 | 管理&业务防火墙 | 规格：标准机架安装；冗余电源；性能：应用层吞吐量≥8Gbps；并发连接≥400万；每秒新建TCP连接数8万；接口：万兆光口≥2个，千兆电口≥4个，千兆光口≥4个，1个HA接口光模块：万兆多模≥2个内存：32GB ；硬盘：1TB； | 台 | 1 |  |
| 3.5 | WEB应用防火墙（WAF） | 规格：标准机架安装，冗余电源性能： HTTP应用层吞吐量≥9Gbps，HTTP最大并发连接数260万，HTTP最大请求速率 6万/秒接口： 万兆光口≥2个，千兆光口≥4个，千兆电口≥6个内存：32GB 硬盘：SSD 64G+1T SATA。 | 台 | 1 |  |
| **4** | **交通专网加固升级** |
| 4.1 | 边界防火墙 | 规格：标准机架安装；冗余电源；性能：网络层吞吐量≥80Gbps；并发连接≥3000万；每秒新建TCP连接数70万；接口：万兆光口≥8个，千兆电口≥8个，千兆光口≥8个，40G QSFP光口≥2个，1个HA接口内存：32GB ；硬盘：1TB； | 台 | 2 |  |
| 4.2 | 网闸 | 规格：标准机架安装，冗余电源；功能：双向隔离应用层吞吐量≥8Gbps，应用层并发性能≥20万条；内存 ：16GB，硬盘：64GB +4TB网络接口： ≥4\*GE（电）、4\*GE（光）、4\*10GE（光） | 台 | 2 |  |
| 4.3 | 网络行为审计设备 | 规格：标准机架安装，冗余电源性能：应用层吞吐≥2.5Gbps，时间记录能力≥2.5万接口：万兆光口≥2个，千兆光口≥4个，千兆电口≥4个光模块：万兆多模≥2个内存：16GB ；硬盘：≥1TB | 台 | 1 |  |
| 4.4 | 管理区防火墙 | 规格：标准机架安装；冗余电源；性能：应用层吞吐量≥8Gbps；并发连接≥400万；每秒新建TCP连接数8万；接口：万兆光口≥2个，千兆电口≥4个，千兆光口≥4个，1个HA接口内存：32GB ；硬盘：1TB； | 台 | 1 |  |
| 4.5 | 设备安全运维与审计设备（堡垒机） | 规格：标准机架安装，冗余电源；性能：最大图形并发会话1000，最大字符并发数1000；接口：万兆光口≥2个，千兆电口≥4个 ，千兆光口≥4个 内存：16GB ；硬盘：256GBSSD+4TB SATA； | 台 | 1 |  |
| 4.6 | 日志审计设备 | 规格：标准机架安装，冗余电源；性能：日志处理能力5000EPS；接口：万兆光口≥2个，千兆电口≥4个 ，千兆光口≥4个 内存：16GB ；硬盘：4TB； | 台 | 1 |  |
| **5** | **公安移动信息网加固** |
| 5.1 | 边界防火墙 | 规格：标准机架安装；冗余电源；性能：网络层吞吐量≥80Gbps；并发连接≥3000万；每秒新建TCP连接数70万；接口：万兆光口≥8个，千兆电口≥8个，千兆光口≥8个，40G QSFP光口≥2个，1个HA接口支持：IPSec VPN、SSLVPN内存：32GB ；硬盘：1TB； | 台 | 2 |  |
| **6** | **公安网与视频传输网边界** |
| 6.1 | 防火墙 | 规格：标准机架安装；冗余双电源。性能：网络层吞吐量≥80Gbps；并发连接≥1200万/s；TCP新建连接数≥30万/s；网络接口≥4\*GE（电）、4\*GE（光）、4\*10GE（光）和1HA接口，硬盘：≥512G；含应用控制、URL过滤、病毒防护、入侵防御、威胁情报检测、IPSec VPN、SSL VPN等功能。 | 台 | 2 |  |
| 6.2 | 网闸（视频交换链路） | 规格：标准机架安装，冗余电源；功能：双向隔离应用层吞吐量≥8Gbps，应用层并发性能≥20万条；内存 ：16GB，硬盘：64GB +4TB网络接口： ≥4\*GE（电）、4\*GE（光）、4\*10GE（光） | 台 | 1 |  |
| 6.3 | 单向光闸（数据交换链路） | 规格：标准机架安装，冗余电源；功能：单向导入性能：应用层吞吐量≥6Gbps；网络接口： ≥4\*GE（电）、2\*GE（光）、4\*10GE（光） | 台 | 2 |  |
| 7 | **公安网与电子政务网边界**  |
| 7.1 | 防火墙 | 规格：标准机架安装；冗余双电源。性能：网络层吞吐量≥80Gbps；并发连接≥1200万/s；TCP新建连接数≥30万/s；网络接口≥4\*GE（电）、4\*GE（光）、4\*10GE（光）和1HA接口，硬盘：≥512G；含应用控制、URL过滤、病毒防护、入侵防御、威胁情报检测、IPSec VPN、SSL VPN等功能。 | 台 | 1 |  |
| 7.2 | 单向光闸（数据交换链路） | 规格：标准机架安装，冗余电源；功能：单向导入性能：应用层吞吐量≥6Gbps；网络接口： ≥4\*GE（电）、2\*GE（光）、4\*10GE（光） | 台 | 2 |  |
| 8 | **视频传输网与政务外网边界** |
| 8.1 | 防火墙 | 规格：标准机架安装；冗余双电源。性能：网络层吞吐量≥80Gbps；并发连接≥1200万/s；TCP新建连接数≥30万/s；网络接口≥4\*GE（电）、4\*GE（光）、4\*10GE（光）和1HA接口，硬盘：≥512G；含应用控制、URL过滤、病毒防护、入侵防御、威胁情报检测、IPSec VPN、SSL VPN等功能。 | 台 | 1 |  |
| 8.2 | 网闸（视频交换链路） | 规格：标准机架安装，冗余电源；功能：双向隔离应用层吞吐量≥8Gbps，应用层并发性能≥20万条；内存 ：16GB，硬盘：64GB +4TB网络接口： ≥4\*GE（电）、4\*GE（光）、4\*10GE（光） | 台 | 1 |  |
| 8.3 | 网闸（数据交换链路） | 规格：标准机架安装，冗余电源；功能：双向隔离应用层吞吐量≥8Gbps，应用层并发性能≥20万条；内存 ：16GB，硬盘：64GB +4TB网络接口： ≥4\*GE（电）、4\*GE（光）、4\*10GE（光） | 台 | 1 |  |
| 9 | **视频传输网与VPDN边界** |
| 9.1 | 防火墙 | 规格：标准机架安装；冗余双电源。性能：网络层吞吐量≥80Gbps；并发连接≥1200万/s；TCP新建连接数≥30万/s；网络接口≥4\*GE（电）、4\*GE（光）、4\*10GE（光）和1HA接口，硬盘：≥512G；含应用控制、URL过滤、病毒防护、入侵防御、威胁情报检测、IPSec VPN、SSL VPN等功能。 | 台 | 1 |  |
| 9.2 | 单向光闸（视频交换链路） | 规格：标准机架安装，冗余电源；功能：单向导入性能：应用层吞吐量≥6Gbps；网络接口： ≥4\*GE（电）、2\*GE（光）、4\*10GE（光） | 台 | 2 |  |
| 9.3 | 单向光闸（数据交换链路） | 规格：标准机架安装，冗余电源；功能：单向导入性能：应用层吞吐量≥6Gbps；网络接口： ≥4\*GE（电）、2\*GE（光）、4\*10GE（光） | 台 | 2 |  |
| 10 | **公安信息网密码应用** |
| 10.1 | 服务器密码机 | SM4加/解密速率为68.38Mbps/70.48Mbps;SM2密钥对生成速率为2906.98对/秒，加/解密速率为46.51Mbps/49.92Mbps,签名速率为2785.52次/秒，验签速率为2283.10次/秒，SM3运算速率为22.82Mbps | 台 | 2 |  |
| 10.2 | 安全认证网关 | 最大并发用户数6090，最大并发连接数为5848，每秒新建连接数为107.79，加解密吞吐率为58.68Mbps | 台 | 2 |  |
| 10.3 | SSL VPN设备 | 最大并发用户数10066，最大并发连接数为10275，每秒新建连接数为789.58，加解密吞吐率为46.29Mbps | 台 | 2 |  |
| 10.4 | 签名验签服务器 | SM2签名速率为2468.26次/秒，验签速率为1460.28次/秒 | 台 | 2 |  |
| 10.5 | 密钥管理系统 | 密钥对生成速率为326.68对/秒。 | 台 | 1 |  |
| 10.6 | 服务器 | 国产CPU 配套密钥管理系统 | 台 | 1 |  |
| 10.7 | 服务器操作系统 | 国产Linux | 台 | 1 |  |
| 11 | **公安视频传输网密码应用** |
| 11.1 | 服务器密码机 | SM4加/解密速率为68.38Mbps/70.48Mbps;SM2密钥对生成速率为2906.98对/秒，加/解密速率为46.51Mbps/49.92Mbps,签名速率为2785.52次/秒，验签速率为2283.10次/秒，SM3运算速率为22.82Mbps | 台 | 2 |  |
| 11.2 | 安全认证网关 | 最大并发用户数6090，最大并发连接数为5848，每秒新建连接数为107.79，加解密吞吐率为58.68Mbps | 台 | 2 |  |
| 11.3 | SSL VPN设备 | 最大并发用户数10066，最大并发连接数为10275，每秒新建连接数为789.58，加解密吞吐率为46.29Mbps | 台 | 2 |  |
| 11.4 | 签名验签服务器 | SM2签名速率为2468.26次/秒，验签速率为1460.28次/秒 | 台 | 2 |  |
| 11.5 | 密钥管理系统 | 密钥对生成速率为326.68对/秒。 | 台 | 1 |  |
| 11.6 | 服务器 | 国产CPU 配套密钥管理系统 | 台 | 1 |  |
| 11.7 | 服务器操作系统 | 国产Linux | 台 | 1 |  |

**9.2具体技术质量需求**

**9.2.1建设要求**

**（1）网络安全加固建设要求**

公安信息网、公安视频传输网网络安全加固，需通过具有资质的第三方检测机构检测，达到三级等保评测“75分”所需的相应技术要求，并通过等保评测。等保测评费用由采购人另行支出。

参照网络安全等级保护二级相应技术要求，互联网接入平台、交通专网、公安移动信息网，通过项目整体安全评测。安全测评费用由采购人另行支出。

**（2）网络安全边界建设要求**

公安信息网与公安视频传输网的安全边界，通过公安部指定的专业技术评测机构实施的检测。

公安信息网与电子政务外网的安全边界，通过公安部指定的专业技术评测机构实施的检测。

公安视频传输网与电子政务外网（视频层）的安全边界，通过具备CMA或CNAS认证证书的第三方检测机构检测。

公安视频传输网与VPDN专网边界的安全边界，通过具备CMA或CNAS认证证书的第三方检测机构检测。

上述边界测评费用应包含在本项目报价中，由中标人负责支出。

**（3）安全管理平台建设要求**

安全管理平台的服务能力，应达到等保三级中的“安全管理中心”的相应技术要求，通过具有测评资质的第三方软件测试，并通过项目整体安全测评。其中，软件测试费用应包含在本项目报价中，由中标人负责支出。安全测评费用由采购人另行支出。

**（4）密码应用建设要求**

公安信息网、视频传输网通过具有资质的第三方检测机构的商用密码应用安全性评估。项目免费运维期内的商用密码应用安全性评估费应包含在本项目报价中，由中标人负责支出。项目验收时需要通过密码测评工作的密码测评费用由采购人另行支出。

**9.2.2施工要求**

**（1）硬件部分**

项目实施中，对于有质量异议的设备、材料、构配件等物料，将由监理方对上述设备、材料、构配件等物料进行质量及性能检测，如质量确实不符合招标要求的。中标人需无条件将不符合招标要求的产品设备更换为满足招标要求的产品设备；

对于因不符合招标要求而需更换的产品及设备，需根据政府审计要求决定被更换的原投标产品的权属，且在审计结束前此部分产品及设备不得挪作他用；

项目建设和验收过程中，若发现工程及相关内容未达到招标需求的目标、任务和要求，中标人需自行改进，直至达到招标需求的目标、任务和要求，所产生的额外费用由中标人承担；

对于满足招标需求的中标产品，中标人不得以任何借口，改变中标产品的品牌型号或减少中标产品数量；

因上述几类原因而造成的费用增加，不得计算在工程费用内。最终更换的产品价格以审计为准，但报审价格不得超过原产品投标价；

项目中出现单项产品在使用中无法达到招标需求中的要求，且数量超该项产品总量10%以上的，将认为该批次产品质量不合格，中标人需整批更换符合招标质量标准的新产品。如因此拖延工程进度，采购人可向中标人提出赔偿要求。

中标人的设备购买及到货计划需经项目管理方确认后实施。

对于本次项目采购的联网设备，投标人中标后需提供原厂方相应的软件开发工具包（sdk）及调试服务。

**（2）软件部分**

项目实施中，采购人将对中标人所提供的成果组织检测。若成果存在不符合招标要求的情况，中标人需无条件修改或重新开发，直至满足招标要求；

项目建设和验收过程中，若发现工程及相关内容未达到招标需求的目标、任务和要求，中标人需自行改进，直至达到招标需求的目标、任务和要求，并不得影响项目整体进度，所产生的额外费用由中标人承担；

中标人需保证所配置的软件产品有合法的使用权；

中标人应在合同规定的时间内按采购人要求完成软件开发、调试、验收工作；

中标人就应用软件操作、维护，对用户方的相关技术人员和使用人员进行现场技术培训，达到正确使用与维护的水平。采购人受训人员的培训费用由中标人承担；

中标人应就应用软件提供完整的安装调试、系统配置、操作说明等相关技术文档。中标人需向采购人公开本系统有关技术细节，提供必要的技术资料；中标人需无推诿承诺公开接口规范、程序源代码等。

最终软件及系统需求以确认后的《需求规格说明书》为准。

**（3）其他要求**

所选用的设备、材料的各项指标、以及施工工艺等应符合本文件要求。本文件未提及的，应符合相关国家和行业最新规范要求；

施工必须遵守政府有关建设的相关规定，中标人在采购人的配合下，自行解决施工办证、协调相关单位及时解决本项目所需的一切事项；

中标人必须按规定落实各项安全生产措施，不发生有责安全生产事故；

考虑到兼容性和长期运维的便利性，应尽量提高设备品牌集中度；

中标人应组织对建设单位运维管理人员和最终用户进行针对所选设备提供有效的专业技术培训，‘有效培训’必须满足人数、场地、时间要求，确保培训效果，使培训人员掌握‘应知应会’，具备使用、查排故障能力。

**10 技术指标要求**

**10.1系统功能与技术指标**

**10.1.1 网络安全加固**

**10.1.1.1 公安信息网网络安全加固**

公安信息网必须符合等保三级有关安全防护的要求，投标人应进行针对性的网络安全策略配置优化实施，主要需求如下（包含且不仅限于如下内容）：

1. 增强网络边界的安全防护能力。
2. 对应用服务器区域进行安全加固，实现对新型网络攻击行为的检测、发现，引诱攻击流量脱靶，确保对核心业务和网络的隐藏保护；实现对Web访问应用级防护；实现对数据库操作的安全审计；API应用安全审计。
3. 增强网络流量监测能力，具备识别恶意流量和高级威胁，增强威胁的发现能力；对网络入侵行为和网络层病毒进行检测和阻断；实现对用户访问行为的审计；对各区域边界的访问控制。
4. 增强网络脆弱性问题的发现能力，有效防止各类恶意入侵及破坏性攻击。
5. 通过安全管理平台，对定级系统的安全策略及安全机制的进行统一管控，实现与上级平台对接；
6. 实现安全设备和重要信息设备的日志审计，日志留存分析时间不少于6个月。
7. 实现对网内重要信息设备的集中管理和运维审计。
8. 增强网络管理能力，具备网络设备发现、拓扑管理、设备监控、故障管理、统计分析报表等功能。

**10.1.1.2 公安视频传输网网网络安全加固**

公安视频传输网必须符合等保三级有关安全防护的要求，投标人应进行针对性的网络安全策略配置优化实施，具体需求如下（包含且不仅限于如下内容）：

1. 增强网络边界的安全防护能力。
2. 对应用服务器区域进行安全加固，实现对新型网络攻击行为的检测、发现，确保对核心业务和网络的隐藏保护；实现对Web访问应用级防护。
3. 增强网络流量监测能力，具备识别恶意流量和高级威胁，增强威胁的发现能力；对网络入侵行为和网络层病毒进行检测和阻断；实现对用户访问行为审计；对各区域边界的访问控制。
4. 增强网络脆弱性问题的发现能力，有效防止各类恶意入侵及破坏性攻击。
5. 通过安全管理平台，对定级系统的安全策略及安全机制的进行统一管控，实现与上级平台对接；
6. 实现安全设备和重要信息设备的日志审计，日志留存分析时间不少于6个月。
7. 实现对网内重要信息设备的集中管理和运维审计。
8. 增强网络管理能力，具备网络设备发现、拓扑管理、设备监控、故障管理、统计分析报表等功能。

**10.1.1.3 互联网接入平台安全加固与网络升级改造**

互联网接入平台的安全防护能力，参照等保二级的相应技术要求进行安全建设。投标人应进行针对性的网络安全策略配置优化实施，具体需求如下(包含且不仅限于如下内容）：

1. 增强网络边界的安全防护能力。实现边界访问控制、现恶意代码防护、应用攻击防护等；抵御互联网DDoS攻击；支持入侵检测功能；识别恶意流量和高级威胁；用户访问行为审计等；
2. 对应用服务器区域进行安全加固，实现对Web访问应用级防护；
3. 增强网络防病毒能力，及时识别入侵和病毒行为有效阻断免受恶意代码攻击，确保网络重要应用系统的关键设备的防病毒能力。
4. 增强安全管理能力，具备日志审计功能，漏洞扫描，设备集中管理和运维审计，安全态势感知，实现全网安全设备日志和安全事件的统一分析和告警。
5. 提升网络可靠性和身份认证能力。将互联网平台从北片区扩展到南片区，统一互联网出口访问方式；核心区升级身份认证、网络准入设备、核心交换设备， 在南片区新增3个汇聚节点、31个接入节点，与北片区原平台融合（融合链路2条），适应不断增长的出口带宽资源以及满足南片区用户的接入。
6. 汇聚节点冗余保护，具备高性能和高可靠性。
7. 融合链路冗余保护、流量负载均衡，上连链路通道达到万兆。
8. 新增汇聚节点之间互联链路通道达到万兆。
9. 终端用户接入Radius认证系统应具备冗余保护能力，具备错误检测和纠正机制；
10. 互联网出口链路冗余备份；
11. 支持多出口链路的综合带宽达到万兆。
12. 支持8000虚拟拨号用户同时在线。
13. 用户上网认证、计费等历史记录数据保存时间大于1年。

**10.1.1.4 交通专网安全加固安全加固**

交通专网的安全防护能力，参照等保二级的相应技术要求进行安全建设。投标人应进行针对性的网络安全策略配置优化实施，具体需求如下(包含且不仅限于如下内容）：

1. 增强网络边界的安全防护能力。实现边界安全隔离，访问控制、入侵防范、恶意代码和垃圾邮件防范、用户访问审计等功能；
2. 增强安全管理能力，具备日志审计功能，设备集中管理和运维审计等功能。

**10.1.1.5 公安移动信息网安全加固**

公安移动信息网应符合等保二级的要求。投标人应充分了解既有网络和安全设备基本情况，充分发挥本项目采购设备和已集中采购设备的功能特点，进行针对性的网络安全策略配置优化实施，具体需求如下(包含且不仅限于如下内容）：

1. 设置联网控制区，增强安全防护措施。实现访问控制、设备准入和统一威胁防护，包括网络入侵防护和网络恶意代码防护等安全能力。
2. 设置安全管控区，具备日志审计，漏洞扫描，设备集中管理和运维审计，主机防病毒，安全态势感知等功能，实现全网安全设备日志和安全事件的统一分析和告警。

**10.1.2 网络安全边界建设**

**10.1.2.1 公安信息网与公安视频传输网边界**

公安信息网与公安视频传输网之间边界，对标对表公安信息通信网边界接入平台安全规范(试行)--视频接入安全部分要求进行建设。实现视频流和图像数据（包括图片、特征值及其结构化描述信息等）从视频传输网至公安信息网的单向传输。

在网络安全防护和数据安全防护方面应满足以下能力要求(包含且不仅限于如下内容）:

1）身份认证,对接入对象必须进行身份认证，身份认证方式基于公安机关颁发的定制类型数字身份证书。认证协议应基于安全的双向认证协议。

2）访问控制,通过身份认证的接入终端只能访问接入平台内的指定设备，并且只能进行允许的操作，非授权的访问应被阻断。

3）机密性与完整性,保证传输过程中应采用密码技术确保数据机密性和完整性，并具备防止重放攻击、篡改和伪造等功能。

4）网络入侵防御,能够对源/目的地址及端口进行控制，实现会话状态检测及内部网络地址隐藏。实时发现入侵行为及病毒、蠕虫传播，并及时报警。

5）数据检查过滤,应能够对流入流出的文件格式、协议格式、字段类型、编码类型、长度大小等进行检查和过滤。

6）应用攻击防护,应能够对应用服务区的爬虫攻击、文件上传攻击、拒绝服务攻击、网络扫描攻击、命令注入攻击、CC攻击等行为进行防护。

7）安全隔离,通过采用安全隔离技术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通信网，确保公安信息通信网的安全。

8）应用安全

视频数据与视频控制信令必须按照不同的安全策略严格区分，分别进行处理和传输，其中视频数据采用单向传输。禁止公安信息网内数据资源通过视频接入链路向外传出，严防敏感数据外泄。

在与公安信息通信网进行视频单向传输之前，要按照预先注册的视频控制信令的类型、格式和内容，对控制信令进行“白名单”方式的格式检查和内容过滤，只允许符合格式要求的控制信令数据通过，对不符合格式的数据进行阻断和报警。视频传输协议格式检测按照预先注册的视频数据格式，对所传输的视频数据进行实时分析和过滤，对不符合格式的视频协议进行阻断和报警。

9）安全管理

为保障边界接入平台的安全和稳定运行，需要对网络系统中的安全设备、网络设备、应用系统及其运行状况进行全面的监测、分析、评估，及时掌握平台的流量情况，追溯历史记录，需对整个数据采集和传输平台进行管理。主要包括：对接入的业务情况进行管理、审计；对平台的安全问题进行监测、报警；对平台的日志信息进行分析、处理。

10）数据级联，边界集中监控管理系统应级联采购人上级单位的边界集中监控管理系统。

11）视频交换链路吞吐量应≥8Gbps，数据交换链路吞吐量应≥6Gbps。

**10.1.2.2 公安信息网与电子政务外网边界**

公安信息网与电子政务外网（其他党政军机关网络）之间边界，按照公安信息通信网边界接入平台安全规范和全国公安机关“一网通办”建设规划进行建设。实现公安信息网与电子政务外网（其他党政军机关网络）以文件交换方式进行双单向文件导入。

在网络安全防护和数据安全防护方面应满足以下能力要求(包含且不仅限于如下内容）:

1）身份认证，对接入对象必须进行身份认证，身份认证方式基于公安机关颁发的定制类型数字身份证书。认证协议应基于安全的双向认证协议。

2）访问控制，通过身份认证的接入终端只能访问接入平台内的指定设备，并且只能进行允许的操作，非授权的访问应被阻断。

3）机密性与完整性，保证传输过程中应采用密码技术确保数据机密性和完整性，并具备防止重放攻击、篡改和伪造等功能。

4）网络入侵防御，能够对源/目的地址及端口进行控制，实现会话状态检测及内部网络地址隐藏。实时发现入侵行为及病毒、蠕虫传播，并及时报警。

5）数据检查过滤，应能够对流入流出的文件格式、协议格式、字段类型、编码类型、长度大小等进行检查和过滤。

6）应用攻击防护，应能够对应用服务区的爬虫攻击、文件上传攻击、拒绝服务攻击、网络扫描攻击、命令注入攻击、CC攻击等行为进行防护。

7）安全隔离，单向隔离传输设备交互的数据内容采用文件落地交换的方式，事先约定文件格式，在交互过程中进行白名单方式的格式检查；在交互过程中对交换内容进行病毒和木马查杀。对于双向的数据交换则采用两个独立的单向通道，通过双单向通道的形式实现。

 8）文件加密监管，对于公安信息网与电子政务外网交换的文件，都需要采用国产密码加密，以验证数据的完整性以及数据来源的可靠性，边界应能具备对明文传输文件进行监测、告警与阻止功能。

 9）通道安全监测，对于公安网数据进出的两个单向通道，都需要进行通道安全监测，监测文件的完整性。对于公安信息网传出数据通道需要做数据防泄露、防篡改监测；对于公安网传入数据通道，需要进行病毒木马监测、APT监测等。

10）安全审计，对于跨网交互平台上传输数据的整个流程，都需要进行审计记录。审计记录需至少保存一年时间，并按照要求将审计记录上报。

11）安全管理。对网络系统中的安全设备、网络设备、应用系统及其运行状况进行全面的监测、分析、评估，及时掌握平台的流量情况，追溯历史记录，需对整个数据采集和传输平台进行管理。主要包括：对接入的业务情况进行管理、审计；对平台的安全问题进行监测、报警；对平台的日志信息进行分析、处理。

12）数据级联，边界集中监控管理系统应级联采购人上级单位的边界集中监控管理系统。

13）数据交换链路吞吐量应≥4Gbps。

**10.1.2.3 公安视频传输网与电子政务外网（视频层）边界**

公安视频传输网与电子政务外网（视频层）之间边界，对标对标公安视频图像信息系统安全技术要求建设。该边界包括视频交换链路和数据交换链路，实现视频流和图像数据（包括图片、特征值及其结构化描述信息等）的双向传输。

在网络安全防护和数据安全防护方面应满足以下能力要求(包含且不仅限于如下内容）：

1）访问控制

应支持通过防护规则实现网络访问控制。对不符合规则的访问，系统应进行拦截并发出告警。

2）设备准入控制

应支持对外部接入设备的准入控制，满足以下需求：

支持对具有唯一性标识的设备进行认证；

支持对具有数字证书的设备进行认证；

支持设备注册，注册信息应包括设备IP/MAC、设备ID、设备属性等信息；

支持采集外部接入设备的硬件信息、操作系统补丁状态、病毒库、进程、注册表、账户等信息，为信任评估提供实时准确的设备环境信息。

3）统一威胁防护

应支持通过检测、阻断、限流、审计报警等防御手段，对蠕虫、后门、木马、间谍软件、Web攻击、拒绝服务等攻击形式进行有效防御。

4）签名验签

签名验签满足以下需求：

支持签名验证，确保交换数据的真实性、完整性和不可抵赖性；

支持对无签名或签名验证不通过的数据进行拦截丢弃，并进行日志报警。

5）协议识别

支持对指定协议的信令和数据流数据基于安全策略进行格式检查，对不符合格式的信令和数据流数据进行拦截丢弃，并进行日志报警。

6）内容过滤

内容过滤满足以下需求：

支持对指定协议的信令和数据流数据基于安全策略进行内容过滤，对含有敏感信息的信令和数据流数据进行拦截丢弃，并进行日志报警；

支持对文本文件基于安全策略进行内容过滤，对含有敏感信息的文件进行拦截丢弃，并进行日志报警；

支持对数据库内格式化数据基于安全策略进行内容过滤，对含有敏感信息的数据库数据进行拦截丢弃，并进行日志报警。

支持对API请求/响应报文数据基于安全策略进行内容过滤，对含有敏感信息的API报文数据进行拦截丢弃，并进行日志报警。

7）流量管控

支持对视频和数据流量进行监测，以规则或统计基线判定异常并实施控制。

8）服务认证

支持通过鉴权方式对服务调用方进行身份认证，认证凭证包括数字证书、口令密码、动态令牌、Token等；

支持对服务调用方进行权限控制，确保最小授权；

支持对服务提供注册、编目、查询、变更、注销等功能。

9）信令安全

支持采用信令签名或信令加密等技术保证信令协议自身安全，抵御信令被篡改、夹带、窃听等安全风险。

10）媒体安全

支持采用媒体流签名或媒体流加密等技术保证媒体流自身安全，抵御媒体流被篡改、夹带、窃听等安全风险。

11）双向隔离

支持根据事先定义安全策略对协议头剥离，支持根据事先定义安全策略对协议头进行再生；

支持通过协议隔离方式断开内部TCP/IP连接，并在数据摆渡过程中不同时连接两侧主机；

支持对数据摆渡传输过程记录日志。

12）业务审计

支持以Syslog、JDBC、FTP、API接口等方式采集业务日志数据；

支持对采集到的日志数据进行范式化、标准化处理；

支持将采集到的所有安全组件日志向相关系统进行报送。

13）集中监控与级联管理

支持边界安全交互系统资产管理，实现信息注册、资产维护、知识管理、漏洞管理等功能；

支持对边界安全交互系统内核心关键设备运行状态进行检测和展现；支持对业务运行状态进行统计；支持依据业务审批信息设置业务监控报警值；支持流量和流速异常告警、违规业务告警和应用访问异常告警等业务监控报警功能；

支持边界安全交互系统策略管理，实现安全策略配置下发、策略变更、策略删除、策略查询等功能；

支持边界安全交互系统的安全反制，能够持续改进安全策略，实现动态安全防御，反制手段包括阻断非合规访问、阻断后续访问等；

支持边界安全交互系统的服务配置管理，支持使用通用数据交换、接口服务、指定协议等交换服务接口申请服务对象，并审核申请合规性；支持通过审核服务的发布、变更和注销等功能。

支持级联采购人上级单位的边界集中监控管理系统，实现数据报送、审批、通报等功能。

14）视频交换链路吞吐量应≥8Gbps，数据交换链路吞吐量应≥6Gbps。

**10.1.2.4 公安视频传输网与VPDN专网边界**

公安视频传输网与VPDN专网之间边界，按照公安视频图像信息系统安全技术要求建设。该边界包括视频交换链路和数据交换链路，实现视频流双单向传输、图像数据（包括图片、特征值及其结构化描述信息等）从VPDN专网向公安视频传输网的单向传输。

在网络安全防护和数据安全防护方面应满足以下能力要求(包含且不仅限于如下内容）：

1）访问控制

应支持通过防护规则实现网络访问控制。对不符合规则的访问，系统应进行拦截并发出告警。

2）设备准入控制

应支持对外部接入设备的准入控制，满足以下需求：

支持对具有唯一性标识的设备进行认证；

支持对具有数字证书的设备进行认证；

支持设备注册，注册信息应包括设备IP/MAC、设备ID、设备属性等信息；

支持采集外部接入设备的硬件信息、操作系统补丁状态、病毒库、进程、注册表、账户等信息，为信任评估提供实时准确的设备环境信息。

3）统一威胁防护

应支持通过检测、阻断、限流、审计报警等防御手段，对蠕虫、后门、木马、间谍软件、Web攻击、拒绝服务等攻击形式进行有效防御。

4）签名验签

签名验签满足以下需求：

支持签名验证，确保交换数据的真实性、完整性和不可抵赖性；

支持对无签名或签名验证不通过的数据进行拦截丢弃，并进行日志报警。

5）协议识别

支持对指定协议的信令和数据流数据基于安全策略进行格式检查，对不符合格式的信令和数据流数据进行拦截丢弃，并进行日志报警。

6）内容过滤

内容过滤满足以下需求：

支持对指定协议的信令和数据流数据基于安全策略进行内容过滤，对含有敏感信息的信令和数据流数据进行拦截丢弃，并进行日志报警；

支持对文本文件基于安全策略进行内容过滤，对含有敏感信息的文件进行拦截丢弃，并进行日志报警；

支持对数据库内格式化数据基于安全策略进行内容过滤，对含有敏感信息的数据库数据进行拦截丢弃，并进行日志报警。

支持对API请求/响应报文数据基于安全策略进行内容过滤，对含有敏感信息的API报文数据进行拦截丢弃，并进行日志报警。

7）流量管控

支持对视频和数据流量进行监测，以规则或统计基线判定异常并实施控制。

8）服务认证

支持通过鉴权方式对服务调用方进行身份认证，认证凭证包括数字证书、口令密码、动态令牌、Token等；

支持对服务调用方进行权限控制，确保最小授权；

支持对服务提供注册、编目、查询、变更、注销等功能。

9）信令安全

支持采用信令签名或信令加密等技术保证信令协议自身安全，抵御信令被篡改、夹带、窃听等安全风险。

10）媒体安全

支持采用媒体流签名或媒体流加密等技术保证媒体流自身安全，抵御媒体流被篡改、夹带、窃听等安全风险。

11）单向导入

支持数据物理单向传输，确保无任何反向通道

支持对导入数据传输过程记录日志。

12）单向导出

支持数据物理单向传输，确保无任何反向通道

支持对导出数据传输过程记录日志。

13）业务审计

支持以Syslog、JDBC、FTP、API接口等方式采集业务日志数据；

支持对采集到的日志数据进行范式化、标准化处理；

支持将采集到的所有安全组件日志向相关系统进行报送。

14）集中监控与级联管理

支持边界安全交互系统资产管理，实现信息注册、资产维护、知识管理、漏洞管理等功能；

支持对边界安全交互系统内核心关键设备运行状态进行检测和展现；支持对业务运行状态进行统计；支持依据业务审批信息设置业务监控报警值；支持流量和流速异常告警、违规业务告警和应用访问异常告警等业务监控报警功能；

支持边界安全交互系统策略管理，实现安全策略配置下发、策略变更、策略删除、策略查询等功能；

支持边界安全交互系统的安全反制，能够持续改进安全策略，实现动态安全防御，反制手段包括阻断非合规访问、阻断后续访问等；

支持边界安全交互系统的服务配置管理，支持使用通用数据交换、接口服务、指定协议等交换服务接口申请服务对象，并审核申请合规性；支持通过审核服务的发布、变更和注销等功能。

支持边界安全交互系统级联管理，实现数据报送、审批、通报等功能。

支持级联采购人上级单位的边界集中监控管理系统，实现数据报送、审批、通报等功能。

15）视频交换链路吞吐量应≥8Gbps，数据交换链路吞吐量应≥6Gbps。

**10.1.3安全管理平台开发**

按照三级等保中“安全管理中心”的技术要求和浦东公安分局网络安全管理需要，安全管理平台应具备提供资产、威胁、脆弱性等相关管理，并具备对威胁的事前监测预警、事中发现处置和事后回溯总结的能力，对网络威胁进行全生命周期管理。具体功能主要包括(包含且不仅限于如下内容）：

**10.1.3.1 数据采集子系统**

1）数据采集

对接入的采集设备、数据的解析规则和策略提供统一的管理，并对数据源采集状态、采集速率和趋势、安全管理平台系统安全状态、集群节点数和健康状态进行实时监控。采集对象包括安全类和重要信息系统设备日志数据，以及网内流量监测系统所采集数据。

数据采集对象（包括且不仅限于此）：流量监测系统、日志审计设备、数据库审计设备、防火墙、网络脆弱性扫描设备、终端安全管理设备、入侵检测/防御设备、API应用安全审计设备、高级持续性威胁检测设备、攻击诱捕系统（蜜罐）、网络管理系统、设备准入系统、网络交换设备、重要服务器等。

2）数据治理

平台可接入多种来源的异构数据，进行数据清洗实现数据格式的统一化；范式解析对数据进行统一格式化处理，满足存储层数据格式定义要求；数据装载将数据统一存储，为后续的在、离线分析提供数据支撑；数据富化通过关联补齐之后形成完整一致的数据；数据标签对数据进行灵活分类，为基于标签的数据快速检索与安全分析模型奠定基础。

3）数据存储

建立安全事件主题库并分类存储；数据存储支持大数据分布式存储架构，支持数据时存储和实时检索；数据留存时间，威胁告警信息、设备日志信息、平台自身日志信息保存6个月，资产静态基础信息及威胁情报保存最新数据；数据检索，支持分布式全文检索方式和分析引擎，具备处理PB级别以上的海量数据能力，支持任务化搜索。

**10.1.3.2分析识别子系统**

**（1）资产管理**

1）资产识别管理

识别包括安全设备、网络设备、服务器、终端等不同类型的资产信息；能对大规模资产数据进行管理（增删改查）；支持文件方式导入资产数据；对纳入平台的产静态信息展示，构建包括设备与系统归属关系；支持IP地址、操作系统、 端口、服务、应用、物理位置（机房、 机架等）、在安全域中的逻辑部署位置等多维度的资产信息指纹库。

2）资产测绘

具备资产发现能力，实现对全网资产探查。主动发现资产：支持与资产管理系统进行对接，下发资产探查扫描任务；被动发现资产：支持从网络流量传感器获取通过网络流量发现的资产信息。

3）资产拓扑

支持自定义编辑资产拓扑，资产拓扑支持增加、修改、查询、删除操作；需内置资产拓扑画布和主机设备、网络设备、安全设备等多种图元，支持通过拖拽连接的方式实现资产拓扑的编辑；资产拓扑中的图元信息可以与实际资产IP进行绑定；支持选择设定布局模式、数据接口、连接状态等信息。

**（2）资产风险**

1）资产风险

基于资产等级、资产威胁、资产脆弱性等数据建立资产风险评级模型；定量计算分析资产风险值，及定性评估资产风险等级，并对资产风险进行统计分析

2）资产基线分析

能够对操作系统、数据库、网络设备、中间件、DNS设备等的配置合规分析； 并按时间、业务系统、违规类别等维度统计分析配置不合规数据情况。

3）资产威胁分析

能够基于资产数据、设备日志、主机系统日志、安全系统数据、威胁情报库等多源数据的关联分析，对资产遭受威胁进行检测分析。

能够对系统攻击包括但不限于：日志破坏检测、系统提权检测、错误日志检测、暴力破解等进行资产威胁统计分析及趋势分析。

4）资产漏洞分析

基于资产漏扫报告，或资产主机系统、应用版本和CVE漏洞库等的关联分析，分析资产漏洞信息；

通过资产漏洞扫描结果和安全设备检测结果进行关联分析，实现漏洞情况分析，包括主机漏洞分析和 Web 漏洞分析；

主机漏洞分析支持对常用的主机操作系统、数据库、网络设备操作系统、常规互联网应用、常见应用开发中间件、网络安全客户端、常用应用软件的漏洞检测结果进行分析；

Web 漏洞分析包括对 SQL 注入漏洞、Cookie 注入漏洞、跨站攻击漏洞、CSRF 漏洞、目录遍历漏洞等常见网页系统应用层安全漏洞检测结果进行分析；

资产漏洞信息统计分析，包括但不限于：按区域、业务系统维度，按漏洞类型维度，按网络和系统类型，按漏洞等级维度来进行统计分析。

5）资产暴露面分析

对资产暴露面、资产安全防护技术手段、安全防护措施部署情况、安全防护策略开启情况进行检测分析；同时需对资产暴露面、资产安全防护技术手段部署情况、安全防护策略开启情况进行统计分析。

6）脆弱性分析

实现对重要资产的漏洞、弱口令、配置核查和Web漏洞的收集和管理，并将漏洞、弱口令和配置核查的结果自动同步到风险模块中，参与风险计算。脆弱性管理方式，支持联动第三方扫描器、导入第三方脆弱性报告、API接口或数据库同步、自动关联漏洞知识库。

**10.1.3.3 安全防护子系统**

**（1）威胁检测**

1）攻击情况检测

支持对常见攻击总体情况的检测及统计，分析当前攻击情况的趋势变化；支持基于多源数据的网络攻击检测功能；支持类网络攻击情况统计和趋势变化统计分析；支持网络异常流量检测及趋势变化统计分析。

2）恶意程序传播情况检测

支持对病毒、蠕虫、木马等恶意程序传播情况进行检测，分析当前恶意程序传播情况的趋势变化。

3）恶意网址访问情况检测

支持DGA域名、钓鱼网址、色情网址等恶意网址及其家族的检测，可对恶意网址的访问传播情况进行统计，分析网络中恶意网址的趋势变化。

4）僵尸网络情况检测

支持对僵尸网络CC主机及肉鸡主机的检测以及统计，并能分析僵尸网络传播情况、趋势变化情况。

5）DDoS攻击溯源

支持对DDoS攻击溯源及趋势变化分析，溯源分析信息包括不限于攻击源地址、攻击源城域网、攻击目的地址、攻击目的城域网、攻击类型、攻击等级、攻击时长、攻击流量大小等信息，并支持分析DDoS攻击特征及趋势变化。

6）Web攻击检测

支持基于Web中间件日志、WAF事件日志等数据源检测分析网站遭受Web应用层攻击情况，并可对Web攻击总体情况的统计，分析Web攻击的变化趋势。

7）扫描行为检测

支持扫描行为检测，通过分析相关数据，发现内外网的信息刺探行为、恶意网站链接等异常行为。

8）攻击链检测

能对高风险攻击事件的攻击链进行检测，将安全攻击事件关联分析，形成攻击链，对攻击行为在防护体系内外部的路径进行分析。

**（2）威胁建模**

1）行为基线建模

行为基线建模，支持模型：日志行为模型、统计行为模型，支持计算单元：日志过滤、行为统计、基线学习和基线比较。基于模型学习行为基线，实时发现偏离基线的行为，产生行为异常事件。行为异常事件可关联资产进行风险评估和风险统计。可查看发生异常行为的实体对象，根据发生异常的实体对象进行处置。

2）关联规则建模

关联规则建模，支持规则：统计规则、日志关联规则和序列规则，支持计算单元：日志过滤、日志关联、聚类统计、阈值比较和序列分析。

**（3）威胁分析**

能够对威胁事件进行调查分析，将所有与调查问题相关的告警、日志、漏洞、配置核查、弱口令、文本和图片信息关联至威胁事件任务。支持通过时间线展示、标注等功能回溯并记录威胁事件的发展过程和相关影响。支持完整的攻击链分析，可还原整个攻击过程。

1）告警分析

至少包含告警名称分析视角、攻击者分析视角、失陷情报分析视角、挖矿木马分析视角、勒索软件分析视角等。

2）场景化分析

至少支持邮件安全、账号安全、异常访问3大分析场景，从多维度多视角进行分析并采用可视化技术进行展现。

**10.1.3.4 检测评估子系统**

（1）等保管理

 实现对等保信息系统的定级备案管理、等保信息系统的自我评价、等保信息系统等保测评管理。支持对等保信息系统全命周期管理和分析。

（2）横向渗透检测

基于WAF、防火墙、流量设备、IDS/IPS、蜜罐等设备日志，通过定义规则，如特定时间内，某系统被攻击后，该系统又发生针对内网的攻击行为，如勒索病毒、挖矿木马、蠕虫横向传播，进行横向进攻检测，方式包括横向渗透探测扫描、横向渗透入侵。然后进行安全策略和攻击分析。

**10.1.3.5 监测预警子系统**

**（1）安全监控**

支持告警状态分布、攻击成功的告警列表、更新资产趋势、威胁命中情报TOP10、全网平均风险值、工单状态分布、攻击者数量、受害者数量、受攻击资产数量等监控视图，实现多维度监测。

支持新增自定义仪表板，通过可视化建模工具制作统计图。

支持按照时间和空间维度持续的反映出当前网络所存在的安全问题报表。

支持BI视图，具备列表、指标卡、折线图、堆积面积图、柱状图、堆积柱状图、条形图、堆积条形图、饼图、词云图等多种视图类型。

**（2）安全预警**

1）资产安全威胁预警

展示资产安全高危威胁信息，并针对高危资产威胁事件提供攻击链追溯分析及展示功能；

2）高危用户行为预警

实时滚屏展示高危用户行为预警信息，高危用户行为预警信息包括事件类型、源IP、目的IP、账号名、时间等；支持历史高危用户行为预警信息查询；

3）资产高风险脆弱性预警

支持资产高危漏洞预警、资产基线不合规预警、资产开放未备案端口数据等，并可查询详情。

支持对外预警接口且可配置，具备向上级部门相关系统上报预警信息能力。

**10.1.3.6 主动防御子系统**

**（1）攻击发现和阻断**

1）攻击发现

支持与防火墙、入侵检测、网络行为审计、终端安全管理系统、应用防火墙等类型设备联动，实时获取各类网络攻击信息。开展威胁情报分析，包括但不限于外部威胁分析、横向威胁分析、多源威胁情报去重合并、外连威胁分析等功能。

2）联动阻断

支持对关联分析后确认的失陷主机、恶意IP、域名、URL和问题帐号等下发联动处置任务的功能。

**（2）攻防演练**

应能提供攻防演练活动中的管理与运营能力,提供攻防演练态势大屏,展示攻防演练中防守方安全管理、系统建设、威胁运营等信息.

1）攻击源监控

分别从外部网络、内部网络的角度进行展示受到哪些攻击。

2）威胁监控

展示攻击数量、攻击手段等。

3）目标资产监控

展示遭遇攻击后哪些资产受到了影响以及受影响的资产信息。

4）演练管理

支持演练项目的管理维护。

**（3）重要时期安全保障**

用于在重要会议或重大活动期间，加强网络安保人员调度，全方位全天候掌握活动相关的单位、系统和网站安全状况，及时通报预警网络安全隐患，高效处置网络安全事件。

1）重保预案

支持重大活动保障预案，提供预案管理。

2）重保值守

建立重保活动活动日历，展现重保活动时间节点。

重大活动保障任务前期、中期、后期分阶段的任务管理、执行详情查看；

支持设置保障监控拓扑；

提供重保大屏，对重保期间安全态势进行实时监测；

云管端、边界、应用、安全设备等多维度监测。

**（4）安全运营支持**

1）监测运营

提供可视化的运营工具，快速发现安全威胁、分析问题、确诊问题、协调各类资源解决问题，覆盖监测、预警、分析及应急处置全业务流程。

2）应急运营

实现突发应急安全事件的发现、分析、处置、关闭的闭环管理，提供用于用户跟踪和协调安全威胁事件处置进度的可视化工具。

**10.1.3.7 事件处置子系统**

**（1）事件报告**

包括安全日报、安全周报、安全月报、安全年报等报告生成功能，体现系统监测的阶段化结果，进行安全分析与态势感知的工作总结。

内置安全报告模板内容应至少包括系统的资产信息、安全告警、监测结果、处置建议等信息。

**（2）应急预案**

可根据告警类型设置对应的预案剧本，在满足触发条件时，能够触发并完成自动化处置。

默认展示所有告警类型与剧本的关联信息，列表字段有：告警类型名称、剧本、状态、更新时间及操作，支持关联对应剧本，执行编排的处置流程。

**（3）响应处置**

 1）事件响应

针对常见告警场景，可制定出标准的处理流程规范，通过安全编排功能，编排好半自动化的剧本流程，实现半自动化的告警响应处置，自动化的执行一些重复性工作，进一步提升告警的处置效率和经验（剧本）沉淀。

2）自动化编排（SOAR）

在实现全面的安全态势感知与主动性安全处置防护的基础上，平台应能站在安全运维与运营的业务需求角度考虑，向更智能化的领域拓展安全运维处置的功能边界。系统应充分利用自动化处置技术，实现基于安全编排能力来构筑自动化运维功能。包括：

对业务逻辑流程所需要的节点的可视化编排；

预定义人工处置节点，设置指定审批人；

标准自动化的节点配置；

判断型（排他性网关、并行网关）的节点配置；

在节点中引入插件并关联插件实例，及配置前后节点关系、输入输出参数；

在节点中引入子剧本，及配置前后节点关系、输入输出参数。

3）联动处置

联动处置为安全运营人员提供的处置闭环的能力。通过与其他安全产品进行联动对接，实现安全威胁及时有效的处置。支持协同处置的设备类型如下（包括且不仅限于）：

防火墙：可对防火墙下发联动处置命令，命令包含：阻断内部对指定外部IP的访问、阻断指定外部IP对内部的访问、阻断指定内部IP对外部的访问、阻断内部对指定URL的访问、阻断内部对指定域名的访问、审计内部对指定外部IP的访问、审计内部对指定域名的访问、审计内部对指定URL的访问；

网络行为审计：可对网络行为审计设备下发的联动处置命令，命令包含：审计内部对指定外部IP的访问、审计内部对指定域名的访问、审计内部对指定URL的访问；

终端安全管理系统：可对终端安全管理系统下发的联动处置命令，命令包含：全网终端隔离特定文件，特定终端隔离特定文件和终端隔离（被隔离终端只能访问控制中心）。

终端安全准入系统：可对NAC联动设备下发的联动处置命令，命令包含：禁止指定内部IP入网、全网禁用问题帐号。

Web应用防火墙：支持对WAF联动设备下发的联动处置命令，命令包含： 阻断指定外部IP对内部的访问、阻断内部对指定外部IP的访问。

4）工单管理

安全管理平台应提供流程化的工单管理功能，能够派发或接收针对威胁告警和漏洞的处置工单，并对与责任人相关的工单流转状态及处置进展进行跟踪。同时安全管理平台支持根据待处置内容定义工单的级别及通知方式，可查看、编辑处置内容和工单任务，也可对处置中的工单任务进行撤销及根据查询条件批量导出工单列表。

**10.1.3.8 态势可视化子系统**

实现信息安全状况和安全运营工作的全局性实时风险掌控，将所有态势大屏进行集中展示，可快速预览大屏的关键指标项。

1）综合安全态势

引用资产、脆弱性和威胁告警数据，分析全局风险等级，能够直观呈现综合安全态势以及各资产分组安全态势，通过综合安全态势，直观了解当前安全运营水平，快速识别安全短板。

2）攻击者视角态势

能够持续监控攻击者、攻击手段和受害者情况，能够直观的呈现攻击者分布情况、近期攻击者信息、攻击类型统计情况以及攻击链阶段统计情况，快速获取攻击者信息，在网络攻防过程中占据主动权。

3）资产外联风险态势

将资产信息统一呈现，直观展示内网资产数量、资产注册情况、资产分布情况、资产发现来源。

4）安全告警态势

实时展示全网最新告警数据并作统计展示，包含告警数量统计、等级统计、变化趋势以及实时告警列表。在列表上优先展示最受关注告警内容，助力运营人员对全网告警情况进行实时监控及处置。

5）脆弱性态势

能够持续监控网络内部漏洞、弱口令和配置弱点情况，展现内网脆弱性分布、趋势、被攻击者利用的情况，协助有效地管理资产脆弱性，消除安全隐患。

6）外部威胁态势

实时呈现网络外部攻击威胁，轻松掌握外部威胁的主要分类、来源地区和攻击源IP，快速感知外部威胁。

7）威胁预警态势

能够持续监测网络内部应对重大安全事件的预警态势，展示当前预警事件中攻击者、受害者的关系，展示受影响资产统计以及受影响资产的影响面趋势，完整呈现预警事件中关键里程碑节点，掌握预警事件的整体态势。

8）安全运营态势

统计展示各类服务器、存储设备、各类安全设备的日志接入情况和资产接入情况。实时展示规则运营、威胁检测和威胁处置情况，掌握整体安全运营态势。

9）态势大屏定制

支持大屏定制流程和接口框架，包含新增大屏、获取权限/菜单、新增背景图片和简介、获取大屏的通用配置以及针对单个大屏单独进行配置。提供定制大屏开发指导手册，对定制流程、接口进行说明。

**10.1.3.9 系统管理子系统**

支持用户进行安全知识的积累和集中管理，提供知识库、失陷IOC情报库。安全知识库应至少可提供洞知识库、IP地理位置信息库和事件日志知识库，支持自定义知识库。失陷IOC情报库，能够对发现的可疑IP、域名、文件MD5、邮箱、证书指纹SHA1进行深入的情报判定。

支持对安全部署和权限控制的管理要求，提供权限管理、系统审计和级联管理功能。

支持安管平台主机监控，监控主机存储、CPU、内存使用指标，可设置告警阈值；实现对大数据组件运行状态的监控与管理；提供可视化的状态监控页面。

**10.1.3.10信息互通管理子系统**

**（1）数据对接**

1）上下级平台数据对接

系统应能支持安全管理平台上下级分级部署能力。

具备向采购人上级安全管理平台上报历史和实时数据能力，支持自定规则上报告警、资产、脆弱性、风险信息等数据；

预留下级安全管理平台接入接口，提供可SDK二次开发包，满足在多级部署环境下进行数据整合、情报共享和统一管理的要求。具备向下级平台下发关联分析规则实现相同威胁检测能力，可向下级平台发送风险预警和安全事件通报。

2）两网平台离线对接

安全管理平台在公安信息网和公安视频传输网内两网内各部署一套，需实现两网安管平台的告警、资产、脆弱性、风险信息等数据定期离线同步功能，预留两网实时同步的能力。

**（2）外部数据集对接**

安全管理平台应支持定期（可调）与外部威胁情报中心同步更新威胁情报数据。

实现离线导入情报功能，预留数据接口调用外部威胁情报中心数据功能。

部署在公安视频图像网内安管平台还需实现与网内终端准入系统的数据对接。

**10.1.3.11 安全风险警示服务子系统**

微服务架构模式，与安全管理平台之间进行数据整合、情报共享，实现在移动网络环境下及时获取网络安全态势分析、告警信息、工作提示以及业务指导等功能，并符合公安移动应用建设相关标准。

**（1）移动端应用**

1） 安全态势

网络信息安全态势总览展示，包含信息安全排名，各类安全事件分类展示，可对每一大类安全事件详细展示细分事项的详情。

登陆用户身份鉴权，按照权限范围可见授权范围内信息安全态势信息。

2）工作提示

工作提示栏集中展示待处置、及时阅读的事项在。对未阅读消息进行提醒。对于未处置的题，可在移动端处置和提交处置结果，根据提示处置状态区分展示。

3）办事指南

用户可在移动端发布各类流程指引、规章制度、学习资料。发布内容支持文字、图片和视频多种方式进行展示。

4） “走马灯”消息提示

重要通知，以“走马灯”形式滚动播放提示。

**（2）网络信息安全警示服务管理台**

1）数据导入

在管理台支持导入各类网络信息安全事件，导入文件支持csv、xls、xlsx类型。导入数据具备信息校验功能。导入数据表单最少支持20类表单的导入。

数据导入后，系统可预留缓冲时间（可设定）。不起效时可删除数据。

2）数据填报

 支持页面数据填报，填报事项种类最少支持20类。

3）事件处置

可查看各类推送事件的清单以及处置进展。事件清单具备过滤检索功能。

对于已经提交反馈的问题，在管理台可进行核实并对问题闭环或者驳回操作。

4）办事指南信息维护

可从管理台发布各类办事指南，支持文本、图片、视频类型。管理台支持信息设置生效或者失效，失效信息仅在管理台可见，移动端将不再显示。

5）人员基础信息维护

可查看本单位的人员信息，在单位内部可调整人员对应的科室。

6）单位服务级别调整

可设置服务单位的级别，调整后页面按照不同颜色显示服务单位的服务级别。

7）信息安全评估模型

可设定模型评估参数，并根据设定参数对单位信息安全进行评估。

**（3）移动端信息安全态势可视化**

1）本月态势

对本月安全事件进行汇总，统计月度事件总数以及截止目前问题闭环率。

2）服务对象

从月度接入数据中进行统计，统计出目前服务的单位数量、主机数量和分控机房的数量。

3）分级服务

按照分级分色，分布展示各级服务单位的数量。支持在地图上按照颜色进行撒点。

4）办事指南

统计目前在生效的各类办事指南数量并展示，包含流程指引、规章制度、学习资料等。

5）最新通知

可进行通知发布，在移动端页面可以看到通知内容。

6）安全态势统计分析

按照月度来展示当年每个月的安全事件数量，可以进行详情展示。

详情展示时，可对年度全部的安全事件使用饼状图进行占比展示；月度内各类安全事件闭环率进行可视化展示；本月各单位的安全事件数量和处置闭环率可视化展示；本年每月各类安全事件趋势和月度闭环率展示；当月安全事件占比分布展示；近期热点问题展示。

安全事项展示，统计各类安全事件累计数量以及问题处理数量

问题处置展示，展示各安全事件的处置进展，包含事件类型、责任单位、每个问题各环节的时间。

**（4）数据对接**

1）内部安全数据对接

和公安信息网内安全管理平台对接，获取报表数据。

2）上级管理单位支撑系统对接

和上级管理单位各支撑系统对接，满足公安信息网、II类区应用规范要求。

**10.1.3.12安全管理平台密码改造**

基于在采购人提供的服务器密码机、安全认证网关、SSL VPN、签名验签服务器，密钥管理系统等密码服务以及系统的应用功能，对接开发安全管理平台的密码应用功能模块，实现网络和通信、设备和计算、应用和数据等层面的各密码应用功能。

**（1）公安信息网安管平台密码对接开发**

1）用户身份认证机制模块

实现用户身份认证机制模块，调用密码产品的相关接口，实现对PC端和服务端身份的鉴别。

2）业务重要数据安全传输模块

实现业务重要数据安全传输模块，调用密码产品的相关接口，实现应用系统通信数据的机密性和完整性保护。

3）服务器设备日志/访问控制信息完整性模块

实现服务器设备日志/访问控制信息完整性模块，调用密码产品的相关接口，实现访问控制信息的完整性保护。

4）重要可执行程序签名验签模块

实现重要可执行程序签名验签模块，调用密码产品的相关接口，实现重要可执行程序的完整性、来源真实性保护。

5）用户访问控制信息签名验签模块

实现用户访问控制信息签名验签模块，调用密码产品的相关接口，实现应用系统登录用户的访问控制列表完整性保护。

6）应用系统重要数据加解密模块

实现应用系统重要数据加解密模块，调用密码产品的相关接口，实现结构化数据的存储机密性保护。

**（2）公安视频传输网安管平台密码对接开发**

同公安信息网安管平台密码对接开发。

**10.1.4网络密码应用**

网络密码应用建设，从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等四个层面采用密码技术措施，建立安全的密钥管理方案，并采取有效的安全管理措施，对信息系统进行保护。

**（1）物理和环境安全**

实现对公安信息网和公安视频传输网内信息系统所在机房等重要区域的物理防护。

1）确认进入各重要区域人员的身份，防止无关和假冒人员进入；

2）保护电子门禁系统进出记录和视频监控音像记录的存储完整性，防止被非授权篡改。

**（2）网络和通信安全**

 实现对公安信息网和公安视频传输网内信息系统与外部实体之间网络通信的安全防护。

 1）确认通信实体的身份，防止与假冒实体进行通信；

 2）保护通信过程中的数据，防止数据被非授权篡改，防止敏感数据泄露。

**（3）设备和计算安全**

实现对公安信息网和公安视频传输网内信息系统中各类设备和计算环境的安全防护。

1）对设备的特权用户（含系统管理员、安全管理员、审计管理员等，以下简称管理员）和普通用户的身份进行识别和确认，防止假冒人员登录；

2）在远程管理时，对远程管理通道进行保护。在远程管理通信过程中，防止与假冒实体进行通信，防止数据被非授权篡改，防止敏感数据泄露；

3）保护计算机、服务器等设备中的系统资源访问控制信息（如设备配置信息、安全策略、资源访问控制列表等）、重要信息资源安全标记（如数据标签等）、日志记录（如系统日志、数据库日志等）和重要可执行程序（如重要应用程序等），防止被非授权篡改；保护重要可执行程序的来源真实性，防止假冒程序文件的加载。

**（4）应用和数据安全**

实现对公安信息网和公安视频传输网内信息系统中应用及其数据的安全防护。

1）确认应用系统的管理员和普通用户的身份，防止假冒人员登录；

2）对应用系统的访问控制策略（如安全策略、资源访问控制列表等）、数据库表访问控制信息（如用户身份信息、数据库安全策略、用户权限列表等）、重要信息资源安全标记（如数据标签）等进行保护，防止被非授权篡改；

3）保护客户端与服务端之间、应用系统之间在非安全网络信道中传输的重要数据（包括但不限于鉴别数据、重要业务数据、重要用户信息等），防止数据泄露、非授权篡改；

4）保护存储的重要数据（包括但不限于鉴别数据、重要业务数据、重要用户信息、业务审计日志等），防止数据泄露、非授权篡改；

5）保护应用系统中可能涉及法律责任认定的数据发送和接收操作，确保发送方和接收方无法否认已经发生的操作行为。

**（5）密钥管理方案**

建立完整的密钥管理方案，明确采用的密钥种类及管理环节，并设计安全的技术实现方式，确保密钥的产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等生存周期的安全。

**（6）安全管理措施**

依据《密码应用基本要求》，协助采购人开展安全管理措施，包括管理制度、人员管理、建设运行和应急处置 等4 个方面。

**10.2产品技术指标要求**

**10.2.1 流量监测系统（类型1）**

功能：采集网络流量和威胁数据，对流量协议类型、行为、域名等进行流量还原生成对应的网络日志，并对流量进行恶意文件、入侵行为等威胁检测；具备基于威胁情报数据进行最新威胁检测，生成威胁日志；支持流量采集上下行载荷长度调整；支持KAFKA、SYSLOG等通信模式，支持多路外发；具备与安全管理平台兼容能力。

规格：标准机架安装，冗余电源

性能：最大流量处理能力≥10Gbps，HTTP并发连接数800万，HTTP新建连接速率30万/秒。

接口：万兆光口≥4个，千兆电口≥4个

光模块：万兆多模≥4个

内存：64GB ；

硬盘：≥12 TB

服务指标：三年维保服务、特征库升级。

如有有效期内的《计算机信息系统安全专用产品销售许可证》或《网络关键设备和网络安全专用产品安全认证证书》，请提供。

**10.2.2 流量监测系统（类型2）**

功能：全流量采集、流量识别与解析、文件还原、智能分析、威胁情报、态势感知展示。

规格：标准机架安装，冗余电源；

性能：整机吞吐量≥1Gbps；

接口：万兆光口≥2个，千兆电口≥4个

内存：16GB ；

硬盘：4TB SATA；

服务：三年维保服务、特征库升级。

如有有效期内的《计算机信息系统安全专用产品销售许可证》或《网络关键设备和网络安全专用产品安全认证证书》，请提供。

**10.2.3 高级持续性威胁检测设备**

功能：具备网络流量的监听，实现对客户端应用中已知漏洞和未知0day漏洞的攻击利用进行检测，并发现Webshell攻击、SQL注入、暴力猜测、DDOS攻击、扫描探测、蠕虫病毒、木马后门、间谍软件等各类攻击和恶意流量；检测出APT事件、僵尸网络、勒索软件、流氓推广、窃密木马、网络蠕虫、远控木马、黑市工具等各类网络威胁，基于威胁情报，流量实时匹配IOC，实现相关威胁告警和响应措施；具有多种响应方式，可针对不同的威胁类型采取相应的措施。

规格：标准机架安装，冗余电源

性能： 吞吐性能≥2Gbps，文件检测50000文件/天，沙箱个数：50个

检测接口： 万兆光口≥2个，千兆电口≥2个，含光模块

内存：32GB

硬盘：2T SATA

服务指标：三年维保服务、特征库升级。

如有有效期内的《计算机信息系统安全专用产品销售许可证》或《网络关键设备和网络安全专用产品安全认证证书》，请提供。

**10.2.4 攻击诱捕系统（蜜罐）**

功能：攻击流量的识别和牵引、攻击欺骗响应、场景化攻击反制、模拟脆弱系统，支持与流量监测系统、安全管理平台联动。

规格：标准机架安装；冗余电源；

性能：主机检测数量≥1800台，同时模拟运行14个高交互服务

接口：万兆光口≥2个，千兆电口≥4个

内存：16GB ；

硬盘：4TB；

服务：三年维保服务，虚拟蜜罐授权100个。

如有有效期内的《计算机信息系统安全专用产品销售许可证》或《网络关键设备和网络安全专用产品安全认证证书》，请提供。

**10.2.5 API应用安全审计设备**

功能：API 检测与识别、API 资产管理、风险 API 识别、威胁统计、敏感数据统计、应用系统访问行为审计（包括：用户登录/注销审计、威胁告警审计、涉敏访问审计、文件传输审计等），API资产可视化、API风险可视化、API行为可视化、API数据泄露可视化、数据安全分析、报表管理。

采集能力：支持至少10个数据源接入；

规格：标准机架安装，冗余电源；

性能：检测吞吐量≥5Gbps；

接口：万兆光口≥2个，千兆电口≥2个

内存：256GB ；

硬盘：48TB SATA；

服务：三年维保服务、特征库升级。

如有有效期内的《计算机信息系统安全专用产品销售许可证》或《网络关键设备和网络安全专用产品安全认证证书》，请提供。

**10.2.6 日志审计存储设备**

规格：标准机架安装，冗余电源；

容量：40TB SATA；

接口：2\*千兆电

**10.2.7 交换机（类型1）**

功能：支持静态路由、RIPv1/2、ECMP、支持URPF、OSPF、IS-IS、BGP、VRRP、路由策略、策略路由；支持堆叠；支持SNMPv1/v2/v3、Telnet远程维护、网管系统管理。

规格：标准机架安装，冗余电源；

性能：包转发率：1620Mpps；交换容量：2.56T/25.6Tbps；

接口：48 个万兆接口，6 个 40G 接口；

光模块：万兆多模≥12个；

服务：三年维保服务。

**10.2.8 交换机（类型2）**

功能：支持静态路由、RIPv1/2、ECMP、支持URPF、OSPF、IS-IS、BGP、VRRP、路由策略、策略路由；支持堆叠；支持SNMPv1/v2/v3、Telnet远程维护、网管系统管理。

规格：标准机架安装，冗余电源；

性能：包转发率：≥480Mpps；

交换容量：≥1.28/12.8Tbps；

接口：16个千兆光电SFP，8个万兆光电SFP+；

光模块：万兆多模≥4个，千兆多模≥8个；

服务：三年维保服务。

**10.2.9 网络安全综合防护设备**

功能：日志审计，网络资产脆弱性扫描（漏扫）、运维安全管理、终端安全管理、数据库安全审计、网络行为审计、集成安全管理平台。上述各项功能应满足采购人实际环境需求。

规格：标准机架安装，内存：512G，硬盘容量：960GB SSD+32TB SATA，电源：冗余电源，接口：4千兆电口+4万兆光口SFP。

漏洞扫描：系统漏扫最大并发IP数：50，WEB漏扫最大并发URL数：5；

数据库日志检索：15000条/s，数据库流量：100M;

服务：三年维保服务，版本升级。

如有有效期内的《计算机信息系统安全专用产品销售许可证》或《网络关键设备和网络安全专用产品安全认证证书》，请提供。

**10.2.10 设备安全准入控制系统**

功能：设备入网管控；支持识别PC、手机、Pad、随身wifi、Windows网络共享、蓝牙网络共享、无线路由器共享等；支持禁止上网、禁止访问业务、禁止入网管控措施生成下达，且无需客户端代理另安装；支持串接和旁路部署；

规格：标准机架安装，冗余电源；

性能：应用层吞吐量1.5Gbps；支持用户数3000，准入终端数5000.

接口：千兆电口≥4个 ，万兆光口≥2个

内存：16GB ；

硬盘：480GB SSD+2TB SATA；

服务：三年维保服务，版本升级。

**10.2.11 宽带接入服务器BRAS**

功能：支持PPPOE/L2TP二层隧道功能；支持radius认证/计费/审计功能。可以根据radius服务器配置的用户信息，可对拨号终端身份鉴别，进行不同等级的速率控制，授予不同的网络访问权限，支持新、旧设备PPPOE/L2TP功能的平滑切换，支持新、旧设备终端身份鉴别、等级速率控制、网络访问权限控制功能的平滑切换。

双主控，双交换结构，冗余交流电源。

接口配置应不小于4个万兆光口、10个千兆光口、10个千兆电口。

交换容量>=115 Tbps。

包转发率>=14400Mpps

业务槽位>=6。

支持全三层路由功能。

支持L2tp LNS功能，8000个l2tp客户许可。

支持QoS机制，提供流量监管和流量整形功能

服务：三年维保服务

**10.2.12 Radius硬件平台**

功能：具备认证、授权及审计（计费）功能，支持双机主备冗余工作模式。

规格：标准机箱2-4U，冗余电源；

CPU：2.5G 16C\*2；

内存：DDR4 32G\*2；

硬盘：2T 3.5吋 7.2K SATA 6Gb硬盘\*4；480G 2.5 SATA 6Gb R SSD\*2。

冗余电源模块\*2，电压范围100- 240Vac。

对外提供1个1 Gbps RJ45管理口，支持Redfish、SNMP、IPMI2.0等标准接口。

双口千兆RJ45网卡。

服务：三年维保服务，硬盘不返还。

**10.2.13 数据库存储盘阵**

功能：用户信息数据存放；用户上网历史数据存放；支持千兆、万兆多种主机接口；提供FC-SAN、IP-SAN、CIFS、NFS、HTTP、FTP等多种协议访问方式；支持冗余控制器；控制器支持热插拔功能，支持Active－Active工作方式；支持硬盘全局热备、专有热备功能；支持在线容量扩展。

支持SAS/ISCISI盘阵

双交流电源

8块2T硬盘，支持Raid5。

2个万兆多模SFP+

用户上网认证、计费等历史记录数据保存时间大于1年。

服务：三年维保服务，硬盘不返还。

**10.2.14 汇聚交换机**

整机配置千兆光口>=24个，千兆电口>=8个，SFP+万兆光口>=4个，2个专用堆叠口。

支持模块化可插拔双电源，配置双交流电源模块。

包转发率>=171Mpps。

交换容量>=672Gbps。

支持静态路由、RIPv1/2、RIPng、OSPF、OSPFv3、ECMP、ISIS、ISISv6、BGP、BGP4+、路由策略、策略路由。

支持堆叠，主机堆叠数不小于9台，配置专用堆叠线缆。

支持SNMPv1/v2/v3、Telnet远程维护、网管系统管理。

服务：三年维保服务。

**10.2.15 接入交换机**

整机配置千兆光口>=4个，千兆电口>=48个，交流电源。

包转发率>=166Mpps。

交换容量>=672Gbps。

支持静态路由、RIPv1/2、RIPng、OSPF、OSPFv3、路由策略、策略路由。

支持SNMPv1/v2/v3、Telnet远程维护、网管系统管理。

服务：三年维保服务。

需与汇聚交换机同品牌。

**10.2.16 出口转接交换机**

整机配置千兆光口>=24个，千兆电口>=8个，SFP+万兆光口>=4个，2个专用堆叠口。

支持模块化可插拔双电源，配置双交流电源模块。

包转发率>=171Mpps。

交换容量>=672Gbps。

支持静态路由、RIPv1/2、RIPng、OSPF、OSPFv3、ECMP、ISIS、ISISv6、BGP、BGP4+、路由策略、策略路由。

支持堆叠，主机堆叠数不小于9台，配置专用堆叠线缆。

支持SNMPv1/v2/v3、Telnet远程维护、网管系统管理。

服务：三年维保服务。

需与汇聚交换机同品牌。

**10.2.17 核心交换机**

模块化交换机，业务板卡插槽数量>=4。

双引擎，双交换网板，双交流电源。

配置万兆光口>=24个，千兆光口>=24个，10/100/1000M电口>=48个。

交换容量>=387Tbps。

包转发率>=115200Mpps。

支持端口镜像功能，支持至少4个端口镜像会话，每组端口镜像会话的观察端口数量>=4。

支持静态路由、RIPv1/2、RIPng、OSPF、OSPFv3、ECMP、ISIS、ISISv6、BGP、BGP4+。

支持MPLS L3VPN、MPLS L2VPN(VPLS，VLL)、MPLS-TE。

支持SNMPv1/v2/v3、Telnet远程维护、网管系统管理。

服务：三年维保服务。

需与汇聚交换机同品牌。

**10.2.18 网管接入交换机**

整机配置千兆电口>=48个，SFP+万兆光口>=4个，2个专用堆叠口。

支持模块化可插拔双电源，配置双交流电源模块。

包转发率>=207Mpps。

交换容量>=672Gbps。

支持静态路由、RIPv1/2、RIPng、OSPF、OSPFv3、ECMP、ISIS、ISISv6、BGP、BGP4+、路由策略、策略路由。

支持堆叠，主机堆叠数不小于9台，配置专用堆叠线缆。

支持SNMPv1/v2/v3、Telnet远程维护、网管系统管理。

服务：三年维保服务。

**10.2.19 边界安全网关**

规格：标准机架安装；冗余双电源。

功能：基于公安数字证书的身份认证；基于802.1x协议的链路认证；基于终端特征的设备认证；基于细粒度授权管理策略的公安信息通信网内信息资源及应用系统强制访问控制；基于公安PKI/PMI系统的认证、授权、审计等；支持应用代理。

性能：吞吐量≥8Gbps；SSL VPN加密吞吐量≥2Gbps

接口：≥4个千兆电口，4个万兆光口

服务：三年维保服务

光模块：2个万兆多模

符合《公安信息通信网边界接入平台安全规范》规范

**10.2.20 集控探针**

功能：支持Syslog、SNMP、SNMP trap、ICMP方式采集日志，支持将日志统一报送集中监控管理系统。

规格：标准机架安装；冗余双电源。

处理能力：吞吐量≥800Mbps，日志采集速率≥800EPS

接口：≥4个千兆电口

服务：三年维保服务。

**10.2.21 视频安全交换系统（前/后置）**

功能要求：

支持集群部署和横向扩展，集群对外提供统一虚拟IP地址入口；

支持对RTSP、SIP、GB/T28181、GB35114、RTP等指定协议的信令和数据流数据基于安全策略的格式检查，不符合的行拦截丢弃并进行日志报警；

支持对指定协议的信令和数据流数据基于安全策略进行内容过滤，对敏感信息进行拦截丢弃并进行日志报警；

支持基于GB 35114 的设备认证准入控制、信令签名验证、加密视频流传输；

支持对接入的视频摄像头、视频平台、信令网关等设备进行认证，支持IP/MAC认证、口令密码认证、GB/T28181设备ID认证准入；

支持访问用户限制、访问内容限制、访问动作限制、访问时间限制、访问地址限制、访问次数限制等访问控制；

支持视频访问日志审计，审计内容包括时间、源IP、源端口、目标IP、目标端口、设备编码、操作动作等信息，支持日志数据存储空间报警和转发报送。

具备对集群媒体流提供负载均衡功能；支持会话保持；具备集群容灾功能，在集群节点故障情况下，业务不受影响。

具备不少于1万路视频巡检功能。

支持用户自定义水印。

兼容IPV4和IPV6网络环境

上述功能若有第三方检测机构报告可提供。

规格：标准机架安装，冗余电源；

性能：应用层单向吞吐量≥8Gbps;视频并发数≥500路（8M码流）；

网络接口≥4\*GE（电）、4\*GE（光）、4\*10GE（光）；

服务：三年维保服务。

光模块：4个万兆多模。

如有有效期内的《计算机信息系统安全专用产品销售许可证》或《网络关键设备和网络安全专用产品安全认证证书》，请提供。

如有CMA或CNAS认证证书的第三方检测机构出具的依据GA/T1788.3 标准检测报告，请提供。

**10.2.22 数据安全交换系统（前/后置）**

功能要求：

支持集群扩展，具备高可用和负载均衡能力；

支持数据库同步；支持FTP、SMB、NFS文件同步；

支持对服务调用方进行身份认证；支持对方服务调用方授权管理；

支持数据签名验证，确保交换数据的真实性、完整性和不可抵赖性；

支持访问控制：支持基于IP、端口、协议、时间、流量、频次的访问控制；

支持对文本文件基于安全策略进行内容过滤，支持对含有敏感信息的文件进行拦截丢弃并报警；

支持数据库库表数据脱敏，支持对敏感信息字段进行数据脱敏，防止数据共享泄漏；

兼容IPV4和IPV6网络环境。

上述功能若有第三方检测机构报告可提供。

规格：标准机架安装，冗余电源；

性能：应用层吞吐量≥6Gbps；数据库交换数量（100Kb/条）≥3000条/秒；数据库交换最大并发数无限制；文件数据处理数量（100Kb/个）≥5000个/秒；

接口：≥4个万兆光口；

服务：三年维保服务。

光模块：4个万兆多模。

如有有效期内的《计算机信息系统安全专用产品销售许可证》或《网络关键设备和网络安全专用产品安全认证证书》，请提供。

如有CMA或CNAS认证证书的第三方检测机构出具的依据GA/T1788.3 标准检测报告，请提供。

**10.2.23 边界安全集中监控管理系统**

规格：标准机架安装，冗余电源；

功能：网络边界的信息注册、资产管理、资产发现、拓扑管理、运行监控、异常行为监控、态势感知、策略管理、预警通报、级联管理。纳入市局集中管控平台开展统一监测。

支持通过获取边界安全设备、网络设备、应用的状态信息、告警信息；

支持边界安全交互系统资产管理，支持页面表单注册、模版上传注册等方式；

支持对边界安全交互系统内设备运行状态进行检测和展现；支持对业务运行状态进行统计，可设置业务监控报警阈值；支持流量和流速异常告警、违规业务告警和应用访问异常告警等业务监控报警功能；

支持边界安全交互系统策略管理；

支持边界安全交互系统级联管理；

支持主动扫描探测方式获取边界设备资产的状态、类型、开放端口、运行服务、脆弱性等信息；

支持安全事件管理，支持安全事件分类分级、安全事件分布、安全事件趋势、安全事件关联、时间序列关系等态势展现；

支持集中审计，可对设备的配置操作、视频交换行为、数据交换行为进行审计，审计内容至少包括：日期、时间、IP、端口、协议、用户（应用）、字节数、URL、操作动作、操作结果等；

支持通过接口对数据安全交换系统、视频安全交换系统进行配置，下发策略配置、业务配置等信息；支持与被管理系统进行基于令牌的双向认证。

具备边界中断、业务中断、设备超负荷、数据拥塞等故障指标监控功能。

兼容IPV4和IPV6网络环境。

 以上功能若有第三方检测机构报告可提供。

性能要求：稳定性运行时间(MTBF) >50,000小时；内存≥128G；4TB\*2 SATA盘；数据库容量≥200GB；支持业务数量≥1000个；监控设备数≥1000个；监控链路数≥50个；业务审计记录数≥10,000,000条。

网络接口≥4\*GE（电）、2\*10GE（光）；

服务：三年维保服务。

光模块：2个万兆多模。

如有CMA或CNAS认证证书的第三方检测机构出具的依据GA/T1788.3 标准检测报告，请提供。

**10.2.24 边界流量监测系统**

功能要求：

支持对所接收的镜像流数据进行重组、关联，形成流量日志文件；

支持自动展现关系拓扑；

支持常用应用协议解析，包括HTTP、HTTPS、FTP、DNS、TFTP、Telnet、SMTP、NFS、SIP、Samba、POP3协议等；

支持自定协议类型、端口、流量大小、IP作为监控条件，对命中规则进行告警；

支持对网络流量的应用层数据进行还原，恢复完整附件；

支持获取有关网络性能指标，包括抖动、时延、丢包、重传等；

支持将数据通过支持文件压缩、加密报送至指定边界安全集中监控管理系统。

规格：标准机架安装，冗余电源

性能：最大流量处理能力≥8Gbps

接口：万兆光口≥2个，

光模块：万兆多模≥2个

内存：32GB ；

硬盘：≥12TB

服务：三年维保服务、特征库升级。

**10.2.25 设备准入控制**

功能要求：

符合GA/T1788公安视频图像信息系统安全规范。

支持对具有唯一性标识的设备进行认证；

支持对具有数字证书的设备进行认证；

支持设备注册，注册信息应包括设备IP/MAC、设备ID、设备属性等信息；

支持使用双因子认证，保证认证强度；

支持串联部署、旁路部署，仅允许通过认证的设备，可授权数据交换。

上述功能若有第三方检测机构报告可提供。

性能：吞吐量≥800Mbps

接口：≥4个千兆电口

规格：标准机架安装，双电源。

服务：三年维保服务

如有CMA或CNAS认证证书的第三方检测机构出具的依据GA/T1788.3 标准检测报告，请提供。

**10.2.26 安全门禁系统**

功能要求：

采用国家密码管理局认证的国密算法芯片，支持国密算法；

支持利用真随机数产生256 位SM2 密钥对，2048 位RSA 密钥对，会话密钥、密钥加密密钥KEK等；

具有融合的系统架构，能实现国际加密算法，国密算法的同步支持，以便与各种不同密码体系的应用进行无缝对接；

用户密钥对/设备密钥对/密钥加密密钥KEK 使用系统保护密钥加密保护，以密文的形式存储在密码卡的存储芯片中。

系统配套发卡器、国密标准CPU用户卡、国密读卡器、国密门禁控制器、门磁锁等设备及配件。

如有商用密码产品认证证书，请提供。

服务：三年维保服务

**10.2.27 视频监控国密改造系统**

功能要求：

可对前端设备采集的视频数据进行签名，保证数据的真实性和完整性；

可接入不小于48路前端视频设备；

可对目标数据进行验签，验证目标数据的真实性和完整性；

符合国家密码局颁布的SM1、SM2、SM3、SM4国产密码算法；

支持前端设备通过GB/T 28181协议接入；

支持RTSP协议，支持对H.26X码流数据做签名；

支持离线视频签名验证；

支持手动拉取视频流进行验签；

支持自动轮巡对视频进行验签；

支持多种格式视频文件；

支持CA证书链管理；

支持自身证书及设备证书管理；

支持对视频鉴定结果生成鉴定报告，鉴定报告中包括视频总帧数、关键帧总数、验证成功帧数、验证失败帧数、缺失帧数、无签名帧数、长度异常帧数、视频总时长等详细信息；

如有商用密码产品认证证书，请提供。

 服务：三年维保服务

**10.2.****28网络管理系统**

网络管理系统，应采用主流B/S架构，能够适配国产化软硬件环境，实现安全浏览器应用，具备设备发现、拓扑管理、设备监控、故障管理、统计分析报表等功能。为公安信息网的安全管理平台提供网络运行数据，满足上海市公安局智能运维管理网络部分数据级联上报需要。

（1）网管监控门户

监控门户具备统一认证，可自定义首页工作界面。统一监控门户可集中展现网络监控管理的骨干网络拓扑、故障告警、故障设备并支持展现网络运行统计数据。

（2）拓扑管理

拓扑管理，通过自动发现物理设备和连接，生成局域网物理拓扑图；可以有效识别二级和三级拓扑，可直观清晰地显示所有网络设备、以及骨干网与子网之间互联关系。层次化的网络拓扑显示网络逻辑结构、同时关联设备性能和告警信息，便于故障隔离和快速定位。

1）拓扑发现

应具备自动发现网络拓扑的能力，采用网络拓扑发现算法和数据采集协议实现网络拓扑自动发现。自动发现网络拓扑可依据网络路由信息，自动查找整个网络的路由器、网络交换机、服务器等支持SNMP协议的设备，生成以图形化的网络拓扑结构。提供多种拓扑视图发现方式，可以用设备的IP地址，对设备进行多种视图的拓扑发现。系统能够基于路由层的连接生成三层逻辑网络拓扑图，基于网段的连接生产二层物理网络拓扑图；网络拓扑结构的显示可支持自行拖拽编排，以直观方式展示真实的网络结构。

2）拓扑绘制

能够根据用户网络的实际情况，灵活地定制网络拓扑视图。用户可以从地域或业务的角度来定制和管理网络拓扑视图，从不同的关注点对网络拓扑的整体情况进行管理，方便网络管理员的运维管理工作，及时掌握网络资源分布情况。

3）拓扑展示

提供拓扑视图上各种网络设备和关键线路的性能负载数据的动态展示，建立面向全网的运行维护和故障预警的网络性能视图。网络管理人员通过它可以充分了解和掌握被管网络的性能负载情况和分布状况，清除网络运行中的故障点，发现网络运行的瓶颈，及时地进行网络调优。

4）地图拓扑展示

地图拓扑可提供全国地图自动绘制功能，支持浦东新区地图展示。

支持对各级拓扑进行节点统计，分别统计可用、不可用的节点数。支持对各级拓扑链路流量进行排名展示；支持对不可用节点进行展示。支持地图上各地域节点与资源的一对一映射绑定，支持各地域节点间的核心链路绘制与运行状态监控，支持逐层钻取和投放大屏显示。

（3）网络设备管理

系统支持自动发现和手动添加两种方式监控网络设备，可支持所有满足SNMP V1/V2/V3方式的厂家路由器、交换机、安全设备、负载均衡等设备的性能指标采集和预警，系统需内置主流厂家型号及其对应指标模板，例如CPU利用率、内存利用率、Ping延时和丢包、端口状态、端口出入流量、入错误帧速、出错误帧速、广播入帧速、广播出帧速等指标。

（4）告警管理

系统提供统一的告警管理平台，通过性能指标采集轮询、调用告警接口、网元Trap/Syslog主动推送、第三方系统轮询获取等来源方式，获得整个网络系统中的各种事件、设备故障、网络异常等告警，当出现故障后能通过预置的web报警方式通知指定用户，并能生成告警分析统计报告，提供主动式的故障解决方式。

（5）报表统计分析

系统可通过报表分析能够有序地展现网络运维的所有管理指标，生成各种分析报告和图表，全面呈现IT系统的设备资源、告警统计、系统运行状况以及人员工作量、服务绩效等，为故障诊断、人员考核、领导决策提供科学的、可量化的依据。

（6）数据接口

1）与安全管理平台数据接口

网管系统需为本网内新建安全管理平台提供网络运维数据接口，包括网络资产数据、网络运行状态数据和网络运行故障告警数据。

2）与上级管理单位级联数据接口

网管系统实现与上级管理单位网管平台之间的数据级联接口功能，包括网络设备资产数据、骨干网络链路数据资产数据、网络运行状态数据、网络设备运行性能数据、网络链路运行性能数据、网络运行故障告警数据。

（7）系统性能：支持不少于150台设备的运行监测管理，设备数据采集周期小于3分钟。

（8）服务：三年维保服务

**11质量标准和验收方案**

**11.1质量标准**

11.1.1 中标人所交付的信息系统应满足本项目合同文件明确的功能性、使用性要求。信息系统的质量标准按照国家标准和招标需求确定，上述标准不一致的，以严格的标准为准。没有国家标准、行业标准和企业标准的，按照通常标准或者符合招标目的的特定标准确定。

11.1.2 中标人所交付的信息系统还应符合国家和上海市有关系统运行安全之规定。

**11.2系统测试及验收方案**

11.2.1 采购人应依据信息系统项目工程的条件和性质，按照招标文件明确的要求向中标人提供信息系统的施工、安装和集成环境。如采购人未能在该时间内提供该施工和安装环境，中标人可相应顺延交付日期。如对中标人造成经济损失，采购人还应依本合同规定承担违约责任。

11.2.2中标人应负责系统及系统设备在实施现场就位安装和调试、操作培训等的全部工作，按照合同文件工作与管理要求负责对项目进度的安排、现场的安全文明施工统一管理和协调，严格遵守国家、本市安全生产有关管理规定，严格按安全标准组织项目实施，采取必要的安全防护措施，消除安全事故隐患。由于中标人管理与安全措施不力造成事故的责任和因此发生的费用，由中标人承担。

11.2.3系统具备隐蔽条件或达到中间验收部位，中标人进行自检，并在隐蔽或中间验收前48小时以书面形式通知采购人、监理验收。通知包括隐蔽和中间验收的内容、验收时间和地点。中标人准备验收记录，验收合格，监理工程师在验收记录上签字后，中标人可进行隐蔽和继续施工。验收不合格，中标人在工程师限定的时间内修改后重新验收。

11.2.4 中标人应在进行系统交付前5个工作日内，以书面方式通知采购人并向采购人提供完整的竣工资料、竣工验收报告及竣工图。采购人应当在接到通知与资料的5个工作日内安排交付验收。中标人在交付前应当根据合同文件中的检测标准对本项目进行功能和运行检测，以确认本项目初步达到符合本合同交付的规定。

11.2.5中标人应按照合同及其附件所约定的内容进行交付，如果约定采购人可以使用或拥有某软件源代码的，中标人应同时交付软件的源代码并不做任何的权利保留。所交付的文档与文件应当是可供人阅读的书面和电子文档。

11.2.6 采购人在本项目交付后，应当在5个工作日内向中标人出具书面文件，以确认其初步达到符合本合同所约定的任务、需求和功能。如有缺陷，应向中标人陈述需要改进的缺陷。中标人应立即改进此项缺陷，并再次进行检测和评估。期间中标人需承担由自身原因造成修改的费用。

11.2.7自系统功能检测通过之日起，采购人拥有**不少于2个月**的系统试运行权利。系统验收通过的日期为实际竣工日期。

11.2.8如果由于中标人原因，导致系统在试运行期间出现故障或问题，中标人应及时排除该故障或问题。以上行为产生的费用均由中标人承担。

11.2.9如果由于采购人原因，导致系统在试运行期间出现故障或问题，中标人应及时配合排除该方面的故障或问题。以上行为产生的相关费用均由采购人承担。

11.2.10系统试运行完成后，采购人应及时进行系统验收。中标人应当以书面形式向采购人递交验收通知书，采购人在收到验收通知书后的5个工作日内，确定具体日期，由双方按照本合同的规定完成系统验收。采购人有权委托第三方检测机构进行验收，对此中标人应当配合。

11.2.11 如果属于中标人原因致使系统未能通过验收，中标人应当排除故障，并自行承担相关费用，同时延长试运行期**30**个工作日，直至系统完全符合验收标准。

11.2.12 如果属于采购人原因致使系统未能通过验收，采购人应在合理时间内排除故障，再次进行验收。

11.2.13 采购人根据信息系统的技术规格要求和质量标准，对信息系统验收合格，签署验收意见。

**11.3 项目验收要求**

**11.3.1 验收准备阶段**

1) 完工后一周内，依据施工图核对工程量、确保安装工艺质量及设备完好性，由中标人填写《工作量总表》、《交工验收记录》以及在完工后一周内提交竣工图，上报监理单位审核后提交采购人和代建方。

2) 遗留问题整改，对检查不合格的以及不符合设计、规范、标准的，按监理签发的整改意见对遗留问题进行改正，直至达标，并作好复查记录。

**11.3.2 验收阶段**

本项目验收阶段分为试运行及合同验收，项目整体验收等阶段。

（1）试运行及合同验收

自项目完成建设后进入试运行，试运行时间不少于2个月。在此期间由中标人负责故障排查和修复工作。施工点位需对故障处理做好记录。每月向采购人提交当月故障处理报告，包括故障事件、故障原因和处理结果。

因施工质量因素导致的一切费用由中标人承担。非施工质量因素导致的甲供设备、甲供材料修理、更换等费用由采购人承担。

试运行结束后，在中标人提供符合要求的验收资料后，开展合同验收。

（2）项目整体验收

新区相关部门将组织进行项目项目整体验收。

中标人应派熟悉本项目的人员参与，并根据采购人要求，提供试运行期间网络和设备的故障处理情况报告，包括故障清单、故障原因和处理结果。

中标人应根据采购人要求提供其它资料，并根据项目整体验收提出整改意见进行整改。

项目整体验收完成后，采购人将出具项目整体验收证明。

**11.4考核**

为促使中标人按本项目招投标文件要求做好相关实施工作，从而确保本项目中建设的内外场机电设施保质、保量的按时完成，现采购人以及所委托的代建单位和施工监理单位将定期（双周），采用日常旁站、随机检查、技术指标测试、文档资料检查等手段，结合以往建设项目的工作经验，制定如下考核内容及评分办法。

中标人应承诺：接受采购人根据投标书中的服务承诺，对考核内容和办法进行调整，如因自身原因造成整个项目无法按时完成整体验收，中标人将承担相关责任。

**11.4.1考核内容**

1）如果中标人没有按照合同规定的时间交货和提供服务，采购人应从货款中扣除误期赔偿费而不影响合同项下的其他补救方法，赔偿费按每周赔偿迟交货物的交货价或延期服务的服务费用的1%计收，直至交货或提供服务为止。但误期赔偿费的最高限额不超过合同价的5%。一周按七天计算，不足七天按一周计算。一旦达到误期赔偿的最高限额，甲方可考虑终止合同。

2）中标人应严格按照采购人所提出的时间进度安排，完成项目建设的相关工作。对于未完成项目建设相关节点进度的情况，每逾期1日，罚扣合同金额的0.1%。误期赔偿费的最高限额不超过合同价的5%，一旦达到误期赔偿的最高限额，采购人可考虑终止合同。

3）中标人收到施工监理单位下达的监理工程师通知单，未按监理工程师通知单整改的，经采购人确认，视情况每次罚扣合同金额的0.1%-1%不等。误期赔偿费的最高限额不超过合同价的5%，一旦达到误期赔偿的最高限额，采购人可考虑终止合同。

**11.4.2评分等级**

考核评分按工期具体实施进度拟定施工时间分阶段考核，考核总分为100分。

1）A级评分值≥相应考核周期总分值90%；（无安全责任事故的前提下，施工进度达到招投标文件、施工图纸、施工规范和施工计划要求, 施工质量优于合同及补充协议要求）：

2）B级评分值≥相应考核周期总分值80%；（无安全责任事故的前提下，施工进度达到招投标文件、施工图纸、施工规范和施工计划要求，施工质量符合合同及补充协议要求）：

3）C级评分值≥相应考核周期总分值70%；（无安全责任事故的前提下，施工进度未达到招投标文件、施工图纸、施工规范和施工计划要求，施工质量符合合同及补充协议要求）：

4）D级评分值＜相应考核周期总分值70%；（无安全责任事故的前提下，施工进度和质量均未达到招投标文件、施工图纸、施工规范和施工计划要求，施工质量不符合合同及补充协议要求）：

5）发生安全责任事故的，本阶段考核评分值为0分，立即停工整改。

**11.4.3考核评分**

本次考核周期为工程整体周期，考核内容划分为以下几点。

评分表（满分100分）

| **序号** | **考核内容** | **评分方法** | **评分值** |
| --- | --- | --- | --- |
| 1 | 完成项目准备阶段工作（项目实施方案编制与评审）（20分） | 按时完成，质量无问题得20分；质量有问题的每一处点位扣除1分，扣完为止 |  |
| 逾期完成得10分，每逾期一个自然日扣除1分，质量有问题的每一处点位扣除1分，扣完为止 |  |
| 2 | 完成设备到货，并通知监理单位进行开箱验收（20分） | 设备准时到货，质量无问题得20分；质量有问题的每一套设备扣除1分，扣完为止 |  |
| 设备逾期到货，质量无问题得15分，每逾期一个自然日扣除1分，扣完为止 |  |
| 设备逾期到货，且质量有问题得10分，每逾期一个自然日扣除1分，质量有问题的每一套设备扣除1分，扣完为止 |  |
| 3 | 完成设备安装及调试，配合完成联调工作（10分） | 按时完成，质量无问题得10分；质量有问题的每一处点位扣除1分，扣完为止 |  |
| 逾期完成得5分，每逾期一个自然日扣除1分，质量有问题的每一处点位扣除1分，扣完为止 |  |
| 4 | 完成软件设计、开发、部署和测试（含第三方测试报告）（25分） | 准时完成应用软件设计、开发、部署和测试得25分；每逾期一个自然日扣除1分，每缺一项规定内容的扣1分，扣完为止 |  |
| 5 | 完成项目验收及审计需要的相关内页资料工作（15分） | 准时完成合格的相关内页资料得15分；每逾期一个自然日扣除1分，每缺一项规定内容的扣1分，扣完为止 |  |
| 6 | 每个考核周期内均有10%分值为采购人主观评分，主要评定依据为中标人配合工作的时效性及工作态度（10分） | 采购人主观评分，每一次有效投诉扣5分，扣完为止 |  |

**12人员及设备配备要求**

12.1由于本项目工期紧张、设备种类繁多，数量庞大，为能确保安全有效的管理和施工，故采购人需投标人承诺在中标后对所有设备及附件，配置固定地点及专人管理。

12.2投标人需为本项目配备专职项目经理，该项目经理需具备相关类似项目管理建设经验，并提供相关证明（证书或参与项目合同）。项目经理在从事本项目期间不得从事其他项目，投标人不可随意更换项目经理，如需更换需征得采购人同意；

12.3投标人配置项目人员的专业和数量应满足本项目的需要，专业配套应齐全，

12.4要求整个服务团队人员10名（委派人员需是本单位职工，提供在职证明材料），服务团队中包含2名驻场人员；驻场人员应全天候响应，在接到用户要求后半个小时内到达现场进行服务。

**13安全生产、文明施工（安装）与环境保护要求**

13.1投标人应具备上海市或有关行业管理部门规定的在本市进行相关安装、调试服务所需的资质（包括国家和本市各类专业工种持证上岗要求）、资格和一切手续（如有的话），由此引起的所有有关事宜及费用由投标人自行负责。

13.2在项目安装、调试实施期间为确保安装作业区域及周围环境的整洁和不影响其他活动正常进行，中标人应严格执行国家与上海市有关安全文明施工（安装）管理的法律、法规和政策，积极主动加强和落实安全文明施工（安装）及环境保护等有关管理工作，并按规定承担相应的费用。中标人若违反规定野蛮施工、违章作业等原因造成的一切损失和责任由中标人承担。

13.3中标人在项目供货、安装实施期间，必须遵守国家与上海市各项有关安全作业规章、规范与制度，建立动用明火申请批准制度，安全用电等制度，确保杜绝各类事故的发生。

13.4中标人现场设备安装负责人应具有专业证书，安装人员必须持证上岗。中标人应对设备安装、调试期间自身和第三方安全与财产负责。

13.5中标人在组织项目实施时必须按安装施工计划协调好现场施工（安装）工作，在项目验收合格移交前对到场货物承担保管责任。中标人在项目实施期间必须保护好施工区域内的环境和原有建筑、装饰与设施，保证环境和原有建筑、装饰与设施完好。

13.6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安全文明施工（安装）和安全生产管理措施，同时应适当考虑购买自己员工和第三方责任保险，并在报价措施费中列支必须的费用清单。

**14售后服务要求（包括延伸服务要求）**

**14.1 售后服务机构或团队构成**

**项目合同验收通过后，中标人对整体项目提供3年免费维护。**中标人在上海设立常驻售后服务团队，提供全天候级别的售后服务。驻场人员在接到报修电话通知后半小时内响应并到底现场处置；其他服务人员在接到报修电话通知后1小时内响应；4小时内赶到现场处理故障，8小时内使系统恢复正常，对于48小时内不能恢复的产品需提供备品配件进行更换维修。

**14.2 具体服务承诺**

中标人负责所供软硬件设备及配套产品的售后服务，包括提供所供产品技术咨询、技术培训、设备检验、到货验收、安装调试以及负责所供产品的保修及其它售后技术服务。

中标人供货的系统软、硬件设备需承诺提供（除特殊说明外的）三年免费质保，投标文件中应详细列出质保期内的服务承诺。签订合同前提供证明材料。

中标人在合同验收后，应提供至少三年的免费维护期，按照用户方的实际要求，对系统进行相应的调整，确保设备正常运行。

中标人需作出无推诿承诺。即中标人应提供特殊措施，无论由于哪一方产生的问题而使系统发生不正常情况时，在得到用户方通知后，需立即派工程师到现场，全力协助用户方和其他供应商，使系统尽快恢复正常。

中标人应提供中文电话免费咨询服务。

在质保期结束前，由中标人工程师和用户代表进行一次全面检查，任何缺陷需由中标人负责修理，在修理之后，中标人应将缺陷原因、修理内容、完成修理及恢复正常的时间和日期等报告给用户方，报告一式两份。

需要在投标文件中对系统集成的任务内容进行详细罗列与界定，对于需要用户方面配合的内容也可同时加以说明。

需要在投标文件中对售后服务的任务内容和服务方式进行详细罗列与界定，对于需要用户方面配合的内容也可同时加以说明。

用户有权要求中标人、原产品制造厂家共同签署书面文件，就中标人向用户提供设备的售后服务内容、质量保证、各自责任和合作事项等达成协议并共同对用户的利益负责。

注：中标人在项目实施过程中，未能按照投标方案书中相应的售后服务承诺履行合同的，用户有权根据合同协议相关条款对中标人进行处罚。

14.2.1 免费质保期间的服务承诺

在货物的质保期内，如有制造质量的问题或质量缺陷，中标人应免费予以更换，保证用户工作及时正常运行。在用户使用的前三个月内，设备出现第二次质量问题，中标人应免费更换。中标人需在质保期内免费提供备件及维修。

中标人应保证按投标文件的承诺提供良好的售后服务。中标人应拥有完善的售后服务体系，包括到货开箱验收，安装、设备调试、日常维护以及故障排除等。中标人应提供三年免费质量保证和原厂备件。

中标人在接到用户方报修通知后，需立即做出响应。

14.2.2免费质保期后的服务承诺

在质保期后，根椐用户方运营的要求（包括对设备、材料更换、软件升级等）。中标人需以积极态度给予配和，并在维护过程中收取基本的人工、材料、服务的成本费用，最大限度的满足用户方要求。

**14.3 延伸服务内容**

项目服务期内，中标人应开展以下延伸服务：

1） 每月开展漏洞扫描工作，及时发现安全漏洞并协助整改工作。

2） 每月形成1份网络数据安全威胁情报分析研判及下步重点工作情况汇报。

3） 支持年度网络安全总结报告编制工作。

3） 支持人工渗透及整改工作。

4） 支持专项安全扫描及整改工作。

5） 支持排查整改最新漏洞风险隐患。

6） 支持年度网络安全应急演练。

7） 支持网络安全应急响应工作。

8） 支持网络安全红蓝对抗活动。

9） 支持处置突发网络安全事件。

10） 支持网络安全检查工作。

11） 协助开展网络安全培训或政策宣贯。

**15 项目的保密和知识产权**

15.1 中标人保证对其提供的服务及出售的标的物享有合法的权利，应保证在其出售的标的物上不存在任何未曾向采购人透露的担保物权，如抵押权、质押权、留置权等。

15.2采购人委托开发软件的知识产权归采购人所有。中标人向采购人交付使用的信息系统已享有知识产权的，采购人可在合同文件明确的范围内自主使用。

15.3在本合同项下的任何权利和义务不因中标人发生收购、兼并、重组、分立而发生变化。如果发生上述情形，则中标人的权利随之转移至收购、兼并、重组后的企业继续履行合同，分立后成立的企业共同对采购人承担连带责任。

15.4 中标人应遵守合同文件约定内容的保密要求。如果采购人提供的内容属于保密的，应签订保密协议，且双方均有保密义务。中标人不得利用工作之便外泄资料或做其他用途，否则中标人需承担由此引起的法律责任和赔偿采购人的经济损失。本款规定的效力适用于中标人及中标人的所有雇用人员。

15.5采购人具有源代码修改权和永久使用权。采购人对本次开发的软件拥有产权，具有软件开发平台的永久使用权，中标人在售后维护期内（包括续签的售后服务期）应提供软件开发平台的后续升级及因开发平台升级导致的应用软件升级服务。

15.6 如采购人使用该标的物构成上述侵权的，则中标人承担全部责任。

15.7 项目保密要求

15.7.1 明确专门机构和工作人员，负责采购项目保密管理工作。

15.7.2 明确保密责任和人员分工，建立文件材料管理、向国际联网的站点（互联网）提供或发布信息及其他信息公开的保密审查等各项保密管理制度，落实采购项目业务工作与保密工作同步开展。

15.7.3 相关文件材料向国际联网的站点（互联网）提供、发布或其他方式信息公开、提供给第三方前，应书面告知甲方拟发布（提供）文件材料的网站或渠道、文件材料种类和内容、时间节点、发布（提供）目的等信息，并得到甲方相关材料已经过信息公开保密审查并属于主动公开的文件材料，同意公开的书面确认（须具备签名、日期和公章）。未经甲方书面确认，不得以任何方式公开采购项目文件材料或将采购项目文件材料提供给第三方。明确知悉并理解采购项目文件材料中以灰色背景突出显示的文本或标题以灰色背景突出显示的图片（表格）属于不宜公开内容；任何情况下，不得以任何方式公开采购项目材料内明确不宜公开的内容。

15.7.4 明确知悉并理解提供给甲方的材料可能上传至国际联网的站点（互联网）主动公开。落实材料保密审查，保证所提供的材料中不包含国家秘密、工作秘密或敏感信息。应对商业秘密等其他不宜公开内容最大限度作隐蔽处理；确属无法隐蔽的，应在材料中以灰色背景突出显示不宜公开内容的文本或图片（表格）的标题。

15.7.5 根据甲方要求，提供所有拟参加项目人员的背景资料，对拟参与采购项目的人员进行审查、开展保密教育并组织签订保密协议。保密协议内容应征求甲方意见，并向甲方提供协议的副本等相关资料。甲方根据审核情况有权提出人员变更要求。

15.7.6 参加项目人员严格保守在工作中所涉及的国家秘密、警务工作秘密和各类敏感信息。

15.7.7 参加项目人员不得擅自记录、复制、拍摄、摘抄、收藏、泄露在工作中涉及的国家秘密、警务工作秘密和各类敏感信息；严禁将公安机关内部会议、谈话内容泄露给无关人员；严禁将工作中涉及的相关合作内容及实施规划透露给无关人员。

15.7.8 参加项目人员应服从甲方的安排，依照有关法律、法规和协议规定工作，不得将工作过程中接触到的文件材料（包括内部发文、各类通知及会议记录等）内容泄露给无关人员；不得翻阅与工作无关的文件和资料，不得从事其他与合作无关的工作。

15.7.9 参加项目人员如需使用公安信息网，应认真学习和严格遵守公安信息网使用相关规定，严禁“一机两用”。不得将从公安信息网上获得的警务工作相关信息透露给无关人员；严禁私自下载、拷贝计算机内的各类信息；不得擅自携带保管涉及项目建设内容的各类载体；严禁将公安信息系统的程序、账号口令等泄露给无关人员。

15.7.10 参加项目人员不得带领无关人员参加项目或进入甲方办公场所。

15.7.11 不得泄露在工作中接触到的公安机关科研、发明、装备器材及其技术资料等信息；参加项目人员不得发表涉及合作过程中涉及的技术文档和论文，未经甲方同意，不得将合作具体内容或项目案例进行演示或宣传。

15.7.12 参加项目人员不得泄露甲方咨询的项目内容、技术措施、目的效果等信息，严格保管调研报告、技术参数等各类文件、材料。

15.7.13 参加项目人员在采购各流程环节中应严格保守国家秘密、警务工作秘密和各类敏感信息，严格保管采购活动记录、采购预算、招标文件、投标文件、评标标准、评估报告、定标文件、合同文本、验收证明等材料。

15.7.14. 参加项目的人员原则上最低服务期限为1年。

15.7.15 参与该采购项目的人员接受甲方的保密管理。

15.7.16 参加项目人员因服务期满或中途离岗的，不得泄露所知悉的国家秘密、警务工作秘密和各类敏感信息。

15.7.17 接受甲方就该采购项目的保密工作检查（调查）。

15.7.18 发生国家秘密、警务工作秘密或有关敏感信息泄露的，参加项目人员应立即向甲方报告并提交具体书面报告，积极协助甲方及有关保密部门进行查处。

15.7.19 落实保密法律法规和相关规范性文件规定明确的其他保密管理要求。

15.7.20 未充分履行保密责任而造成失泄密或敏感信息泄露，须承担法律责任，并赔偿甲方相应经济损失；构成犯罪的，将依法追究刑事责任。

15.7.21 对本协议的任何修改，必须采取书面形式，并有双方法定代表人（或委托授权人）签字。

**16 技术培训**

**16.1技术文件**

中标人提供本系统的详细技术文件。

**16.2技术服务**

中标人应提供现场技术培训，就设备的安装、调试、使用和维护，培训用户方技术人员，直到用户方工作人员全部掌握运行操作、保养技术，并能达到正确维护、排除一般故障为止。根据设备技术要求向用户方提供厂方维修技术人员培训和2名甲方工作人员与中标设备相关的设备或安全认证培训，用户方受训人员的培训费用由中标人承担。中标人需针对本项目提供详细的培训方案和计划。

（1）投标人应在投标文件中详细说明技术指导和技术支持的范围和程度。

（2）投标人应在投标文件中提出保修期之后的设备返修流程，包括返修时间，替用设备，以及返修价格。｝

**四、投标报价须知**

**17 投标报价依据**

17.1 投标报价计算依据包括本项目的招标文件（包括提供的附件）、招标文件答疑或修改的补充文书、工作量清单、项目现场条件等。

17.2招标文件明确的项目范围、实施内容、实施期限、质量要求、售后服务、管理要求与标准及考核要求等。

17.3工作量清单说明

17.3.1 工作量清单应与投标人须知、合同条件、项目质量标准和要求等文件结合起来理解或解释。

17.3.2采购人提供的工作量清单是依照采购需求测算出的主要工作内容，允许投标人对工作量清单内非核心工作内容进行优化设计，并依照优化后的方案进行报价。各投标人应认真了解招标需求，如发现核心工作内容和实际采购需求不一致时，应立即以书面形式通知采购人核查，除非采购人以答疑文件或补充文件予以更正，否则，应以工作量清单为准。

**18****投标报价内容**

18.1 本项目报价为全费用报价，是履行合同的最终价格，除投标需求中另有说明外，投标报价（即投标总价）应包括项目前期调研、数据收集和分析、方案设计、项目研发、基础环境集成实施、智能化安装工程、硬件集成实施、软件开发和集成实施、安全集成实施、系统调试及试运行、验收和评估、操作培训、售后服务、投入使用这一系列过程中所包含的所有费用。

18.2 投标报价中投标人应考虑本项目可能存在的风险因素。投标报价应将所有工作内容考虑在内，如有漏项或缺项，均属于投标人的风险，其费用视作已分配在报价明细表内单价或总价之中。投标人应逐项计算并填写单价、合计价和总价。

18.3在项目实施期内，对于除不可抗力因素之外，人工价格上涨以及可能存在的其它任何风险因素，投标人应自行考虑，在合同履约期内中标价不作调整。

18.4 投标人按照投标文件格式中所附的表式完整地填写《开标一览表》及各类投标报价明细表，说明其拟提供服务的内容、数量、价格、时间、价格构成等。

**19投标报价控制性条款**

19.1 投标报价不得超过公布的预算金额或最高限价，其中各分项报价（如有要求）均不得超过对应的预算金额或最高限价。

19.2 本项目只允许有一个报价，任何有选择的报价将不予接受。

19.3 投标人提供的服务应当符合国家和上海市有关法律、法规和标准规范，满足合同约定的服务内容和质量等要求。不得违反法规标准规定或合同约定，不得通过降低服务质量、减少服务内容等手段进行恶性低价竞争，扰乱正常市场秩序。

★19.4经评标委员会审定，投标报价存在下列情形之一的，该投标文件作无效标处理：

19.4.1减少工作量清单中核心工作内容数量；

19.4.2 投标报价和技术方案明显不相符的。

**五、政府采购政策**

**20 节能产品政府采购**

20.1 按照财政部、发改委发布的《财政部发展改革委生态环境部市场监管总局关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9号）的要求，采购人采购的产品属于“节能产品品目清单”中的，在技术、服务等指标同等条件下，应当优先采购节能产品。采购人需购买的材料产品属于政府强制采购节能产品品目的，投标人必须选用节能产品。

20.2投标人如选用节能产品的，则应在投标文件中提供国家确定的认证机构出具的、处于有效期之内的节能产品的认证证书；反之，该产品在评标时不被认定为节能产品。

**21环境标志产品政府采购**

21.1 按照财政部、环保总局联合印发的《财政部发展改革委生态环境部市场监管总局关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9号）的要求，采购人采购的产品属于“环境标志产品品目清单”中的，在性能、技术、服务等指标同等条件下，应当优先采购环境标志产品。

21.2投标人如选用环境标志产品的，则应在投标文件中提供国家确定的认证机构出具的、处于有效期之内的环境标志产品的认证证书；反之，该产品在评标时不被认定为环境标志产品。

**22 促进中小企业发展**

22.1 中小企业（含中型、小型、微型企业，下同）的划定按照《中小企业划型标准规定》（工信部联企业【2011】300号）执行，参加投标的中小企业应当提供《中小企业声明函》（具体格式见“投标文件格式”），反之，视作非中小企业，不享受相应的扶持政策。如项目允许联合体参与竞争的，则联合体中的中小企业均应按本款要求提供《中小企业声明函》。

22.2 依据市财政局2015年9月发布的《关于执行促进中小企业发展政策相关事宜的通知》，事业单位、团体组织等非企业性质的政府采购供应商，不属于中小企业划型标准确定的中小企业，不得按《关于印发中小企业划型标准规定的通知》规定声明为中小微企业，也不适用《政府采购促进中小企业发展管理办法》。

22.3 如项目允许联合体参与竞争的，组成联合体的大中型企业和其他自然人、法人或者其他组织，与小型、微型企业之间不得存在投资关系。

22.4对于小型、微型企业，按照《政府采购促进中小企业发展管理办法》（财库【2020】46号）和《关于进一步加大政府采购支持中小企业力度的通知》（财库【2022】19号）规定，其报价给予**10%**的扣除，用扣除后的价格参与评审。

22.5如项目允许联合体参与竞争的，且联合体各方均为小型、微型企业的，联合体视同为小型、微型企业，其报价给予**10%**的扣除，用扣除后的价格参与评审。反之，依照联合体协议约定，小型、微型企业的协议合同金额占到联合体协议合同总金额30%以上的，给予联合体**4%**的价格扣除，用扣除后的价格参与评审。

22.6供应商如提供虚假材料以谋取成交的，按照《政府采购法》有关条款处理，并记入供应商诚信档案。

**23** **促进残疾人就业（注：仅残疾人福利单位适用）**

23.1 符合财库【2017】141号文中所示条件的残疾人福利性单位视同小型、微型企业，享受促进中小企业发展的政府采购政策。残疾人福利性单位属于小型、微型企业的，不重复享受政策。

23.2 残疾人福利性单位在参加政府采购活动时，应当按财库【2017】141号规定的《残疾人福利性单位声明函》（具体格式详见“投标文件格式”），并对声明的真实性负责。