

采购需求

一、项目概况

1. 项目名称：公安边界安全交互平台建设项目
2. 项目编号：HNSH2022-1201
3. 预算金额：¥1685898.00 元（采购预算包含成本、运费、包装费等与本项目相关的所有费用）
4. 最高限价：¥1685898.00 元，供应商报价超过最高限价金额的按无效响应处理。
5. 资金来源：财政资金

二、采购需求

序号	货物名称	技术参数及要求	数量	单位
1	设备准入控制系统	<p>1、2U 标准机架式设备；冗余电源；配置 10 个 10/100M/1000M 电口,8 个千兆光口,1 个 Console 口；2 个 USB 口；另支持 1 扩展插槽；吞吐量≥8Gbps；支持接入设备数量：2500 个；每秒事务数（TPS）：≥6000 次/秒；</p> <p>2、提供 3 年设备原厂保修服务；</p> <p>3、通过主动监听与被动监听方式相结合，实现对终端的资产的发现与识别；通过多种准入控制技术的复用，实现对终端的入网控制；</p> <p>4、通过与第三方认源的联动，实现对终端入网的用户认证，并提供用户、IP 地址、MAC 地址等多元素绑定；</p> <p>5、提供终端入网流程化管理，包括终端入网认证、注册、安检、授权，并基于角色进行访问控制；通过客户端管理功能，对终端入网进行合规检查，提供多种安全检查策略；</p>	1	台

序号	货物名称	技术参数及要求	数量	单位
		<p>6、▲支持网络内部 NAT 设备探测发现、告警、阻断，并可以针对 NAT 设备下接终端进行准入控制，可设为可信、隔离、禁用端口操作；（提供功能截图并加盖厂商公章）</p> <p>7、支持网络资产自动采集功能，并能够自动分类网络中的接入设备，如交换路由设备、PC 设备、服务器、IP 电话、网络打印机等，同时能够及时发现网络中出现的新设备，对外来终端的接入行为进行告警；</p> <p>8、支持发现内网私接 hub、非网管交换机等，能够及时产生告警并阻断接入设备入网；支持 Hub 下多个终端需分别认证才能入网；</p> <p>9、支持全网监控统计功能，实时显示全网监控状态信息的资产动态、安全违规事件、设备信息、在线终端统计、终端类型统计、终端厂商分类统计、实时告警、终端安全分析统计等信息；</p> <p>10、▲支持对网络攻击行为，如 Smurf 入侵、LAND 攻击、WINNUK 攻击等，支持对攻击行为的发现和告警。（需提供国家认证认可的检测机构出具的检测报告并加盖厂商公章）；</p> <p>11、支持在 IPv4 和 IPv6 双栈环境下的终端准入控制；</p> <p>12、支持 IP/MAC、MAC/PORT 绑定功能，可自动检测不在 IP/MAC 绑定列表中的设备按 IP/MAC 违规处理进行阻断操作；</p> <p>13、产品具有《计算机信息系统安全专用产品销售许可证》（提供相关证书证明文件并加盖厂商公</p>		

序号	货物名称	技术参数及要求	数量	单位
		章)。		
2	集控探针	<p>1、1U 标准机架式设备；单交流电源；配置 6 个 10/100M/1000M 电口，1 个 Console 口；2 个 USB 口；另支持 1 扩展插槽；稳定性运行时间 (MTBF)>50,000 小时；通量≥600Mbps；最大探测设备≥100 个；</p> <p>2、提供 3 年设备原厂保修服务；</p> <p>3、支持采集交换机、路由器、防火墙、入侵检测、可信边界网关等边界接入链路外网侧常用设备的运行状态信息；</p> <p>4、支持 SYSLOG 协议；</p> <p>5、支持 SNMP v2/SNMP v3 协议；</p> <p>6、支持与同品牌边界接入平台外主机安全联动，以私有协议方式转发从外网采集到的设备和业务日志信息在集控服务器统一监控展示。</p>	1	台
3	集中监控与管理系统	<p>1、2U 标准机架式设备；冗余电源；≥4 个自适应千兆网络接口，4 个 USB 口；1 个 VGA 接口；最大支持业务数量：≥1000；</p> <p>最大监控并发用户数量：≥5000；最大审计用户数量：≥200000；最大日志存储时间：180 天；</p> <p>稳定性运行时间 (MTBF)：>50000 小时；</p> <p>2、提供 3 年设备原厂保修服务；</p> <p>3、能够对整个内外网数据交换平台的业务、应用、终端、服务器、网络设备监管；</p> <p>4、▲产品满足公安部边界安全规范要求，提供边</p>	1	台

序号	货物名称	技术参数及要求	数量	单位
		<p>界接入平台信息注册和管理功能模块，可以简便的录入边界接入平台的基本信息、建设信息、使用单位、运维信息等；（提供功能截图并加盖厂商公章）</p> <p>5、能够以拓扑图的形式直观实时视频安全接入链路、安全数据交换链路以及安全与隔离与单向导入链路设备当前的运行状态；</p> <p>6、支持与同品牌边界接入平台外主机安全联动，以私有协议方式转发从外网采集到的设备和业务日志信息在集控服务器统一监控展示；</p> <p>7、支持以标准 Syslog 方式来搜集边界接入点上各个服务器、前置机和网络设备（如交换机、路由器、防火墙、入侵检测、可信边界网关等）的日志信息；</p> <p>8、▲具备对接入业务的一键巡检功能，通过点击按钮可主动获取展示当前接入业务状态，并提供选件日志录入记录功能模块；（提供功能截图并加盖厂商公章）</p> <p>9、能够提供业务应用和数据交换审计，即业务应用系统信息、数据传输量、文件类型、传输时间、传输的文件名或主键值等内容详细的审计，支持审计日志周期性自动备份或清空，具备按一定日志空间的大小进行日志轮循的功能，以提高系统的性能；</p> <p>10、能与同一品牌的集控探针设备联动完成链路外网侧设备及业务的信息的安全采集；</p> <p>11、具有国家版权局颁发给产品的《计算机软件</p>		

序号	货物名称	技术参数及要求	数量	单位
		著作权登记证书》(提供相关证书证明文件并加盖厂商公章)。		
4	视频集中监控模块	<ol style="list-style-type: none"> 1、最大支持监控的视频接入设备数量≥ 32台 2、最大支持业务注册数量≥ 100个 3、最大注册终端数量≥ 5000个 4、支持对监管信息的上报。 5、支持查看视频设备的运行状态、硬件(硬盘、系统等)信息、性能指标等数据。 6、支持自制网络拓扑图,支持监控设备图形化拖拽,直观显示网络情况。 7、支持在统一界面上监控、统计、查询所有设备和业务。 8、支持报表、图形等多种展示方式,为决策分析提供支撑。 9、具有完善的日志存储和检索功能。支持自动接收并记录远程监控设备的报警、审计等信息。 10、支持异常故障报警与处理。 11、支持巡检功能。 12、支持上级平台浏览、综合查询、统计分析下级平台的注册管理、运行状态、安全审计等信息。 13、支持 SYSLOG、SNMP v2/v3 协议。 	1	套
5	视频接入认证服务器	<ol style="list-style-type: none"> 1、2U 标准机架式设备;单交流电源;≥ 6个千兆电口(其中包含 1 个管理口)、2 个万兆光口插槽、2 个 USB 接口;1 个 Console 口;硬盘$\geq 1\text{TB}$;另支持 1 扩展插槽; 稳定性运行时间(MTBF) > 50000 小时 	2	台

序号	货物名称	技术参数及要求	数量	单位
		<p>传输延时$\leq 15\text{ms}$</p> <p>视频传输能力≥ 2000路 D1 并发（250路 D4）</p> <p>数据吞吐量$\geq 4\text{Gbps}$</p> <p>并发用户数≥ 1000个</p> <p>单台设备接入不同视频监控系统厂商≥ 5个</p> <p>支持设备集群堆叠数量≥ 16个</p> <p>2、提供3年设备原厂保修服务。</p> <p>3、支持基于公安 U-key 的身份认证,只有通过 U-key 认证的用户才能做进一步操作;</p> <p>4、▲支持海康、大华、宇视、科达、互信互通、华为、先进视讯、天视、普天、中兴等不少于40多种视频控制协议 ; (提供功能截图并加盖厂商公章)</p> <p>5、能够符合跨区域视频监控联网共享技术规范 (DB33/T629-2007) 的要求,支持跨区域视频监控的联网共享要求;</p> <p>6、▲要求完全符合《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/T28181-2016) 标准,能够很好的实现视频系统间的互联互通;(需提供国家认证认可的检测机构出具的检测报告并加盖厂商公章)</p> <p>7、支持自主开发的终端认证机制,采用 AES 加密算法对视频客户端和视频终端设备进行认证;</p> <p>8、要求具备便利的视频协议白名单配置管理功能,支持新的视频类型可视化自助导入;</p> <p>9、可针对视频控制信令 SIPRTSP 以及视频流格式 RTP 等配置白名单过滤条件,支持正则表达式;</p>		

序号	货物名称	技术参数及要求	数量	单位
		<p>10、▲具有详细的传输审计功能，能按照时间记录客户端、服务器端 IP 及端口连入时间及连接时长等信息；（提供功能截图并加盖厂商公章）</p> <p>11、对用户行为进行审计，包括正常登录，非法登录，非法请求，退出等；</p> <p>12、产品具有《计算机信息系统安全专用产品销售许可证》（提供相关证书证明文件并加盖厂商公章）；</p> <p>13、具有公安部安全与警用电子产品质量检测中心 GB/T28181-2016 标准符合性检测报告；（提供相关证书证明文件并加盖厂商公章）；</p>		
6	视频安全隔离交换系统	<p>1、标准机架式机箱，采用“2+1”架构，即由两个主机系统和一个隔离交换专用硬件组成，冗余电源，正面提供 2 个显示液晶面板；网络吞吐量 $\geq 5\text{Gbps}$</p> <p>内网接口：6 个 10/100M/1000M 电口、4 个 1000M Base-FX 光口插槽、4 个 10000M Base-FX 光口插槽；1 个 Console 口；2 个 USB 接口；另支持 1 扩展插槽；</p> <p>外网接口：不少于 6 个 10/100M/1000M 电口（其中包含 1 个管理口）、4 个 1000M Base-FX 光口插槽、4 个 10000M Base-FX 光口插槽；1 个 Console 口；2 个 USB 接口；另支持 1 扩展插槽；</p> <p>2、提供 3 年设备原厂保修服务；</p> <p>3、支持数据库交换模块、文件交换模块、FTP 访问模块、安全浏览模块、邮件传输功能模块、消息传输模块、视频传输模块、安全通道模块；</p>	2	台

序号	货物名称	技术参数及要求	数量	单位
		<p>4、可对用户的客户端版本和进程进行检查，进行准入控制；</p> <p>5、▲支持对外开启 WEB 服务，供用户登录进行文件上传/下载操作；（提供功能截图并加盖厂商公章）</p> <p>6、支持病毒检测；支持 Oracle、SQLServer、Sybase、Db2、MySQL、MongoDB 等主流数据库；支持达梦、人大金仓、Gbase、神通数据库、博阳等主流国产数据库；</p> <p>7、支持 SIP、GB35114、GB/T28181、DB33、H. 323、ONVIF、RTSP、国电 B 类接口等通用协议；</p> <p>8、支持多个视频厂商(海康、大华、科达、中兴、迪威、东方网力等协议；</p> <p>9、支持视频服务器认证，有效保证非法视频服务器不能接入用户的内部网络；</p> <p>10、支持视频功能类型过滤，包括实时点播、历史回放、录像下载、云台控制、回放控制、录像检索、设备查询等；</p> <p>11、具备视频单向传输、信令双向传输能力；</p> <p>12、支持 HTTPS 的 Web 方式管理，实现了远程管理信息加密传输；</p> <p>13、▲支持主、备状态实时展示；（提供功能截图并加盖厂商公章）</p> <p>14、内/外网主机系统分别具有独立管理接口，而不是采用低安全的管理方式，如通过业务口管理或通过内网唯一管理接口完成全部管理等；</p> <p>15、业务状态监控功能，实时提供业务是否可用、</p>		

序号	货物名称	技术参数及要求	数量	单位
		<p>连接会话、流量统计等信息；</p> <p>16、产品具有《计算机信息系统安全专用产品销售许可证》（网络隔离-增强级）（提供相关证书证明文件并加盖厂商公章）；</p> <p>17、提供《网络关键设备和网络安全专用产品安全认证证书》和《中国国家信息安全产品认证证书》增强级（提供相关证书证明文件并加盖厂商公章）。</p>		
7	视频用户认证服务器	<p>1、2U 标准机架式设备；单交流电源；≥6 个千兆电口（其中包含 1 个管理口）、2 个万兆光口插槽、2 个 USB 接口；1 个 Console 口；硬盘≥1TB；另支持 1 扩展插槽；</p> <p>稳定性运行时间(MTBF) >50000 小时</p> <p>传输延时≤15ms</p> <p>视频传输能力≥2000 路 D1 并发（250 路 D4）</p> <p>数据吞吐量≥4Gbps</p> <p>并发用户数≥1000 个</p> <p>单台设备接入不同视频监控系统厂商≥5 个</p> <p>支持设备集群堆叠数量≥16 个</p> <p>2、提供 3 年设备原厂保修服务。</p> <p>3、支持基于 IP 地址的视频客户端流量控制管理功能，可设置客户端访问视频的最大带宽；</p> <p>4、满足《公安信息通信网公安边界接入平台安全规范（试行）-视频接入部分》以及公安《接入平台视频交换系统检查大纲》要求，具备限制视频信令与视频数据剥离，视频信令双向视频数据单向传输功能；</p>	2	台

序号	货物名称	技术参数及要求	数量	单位
		<p>5、可根据用户的 IP 将用户分为普通和特权用户，普通用户只能访问一个视频系统，特权可以自定义访问多个视频系统；</p> <p>6、▲具备系统白名单管理机制，可根据需要把指定客户端 IP 纳入白名单管理；（提供功能截图并加盖厂商公章）</p> <p>7、支持采用 SNMP 协议对外网接入设备做可信认证，支持 MD5、SHA 认证算法；</p> <p>8、▲满足《公共安全视频监控联网信息安全技术要求》GB35114-2017 标准定义的公共安全领域视频监控联网视频信息以及控制信令信息安全保护技术要求，确保视频传输安全；（需提供国家认证认可的检测机构出具的检测报告并加盖厂商公章）</p> <p>9、具备限制视频信令与视频数据剥离，视频信令双向视频数据单向传输功能；</p> <p>10、具备历史流量统计与小时峰值流量可视化展示功能；</p> <p>11、具备集控上报功能，能将系统日志以 Syslog 方式上报给内网集控系统；</p> <p>12、▲支持视频平台互联认证、视频信令认证、加密视频点播以及历史加密视频回放功能；（需提供国家认证认可的检测机构出具的检测报告并加盖厂商公章）</p> <p>13、具备详细的开机运行、管理员操作、访问阻断、系统告警等审计日志记录，并具备本机、本地内网侧半年以上审计日志硬盘存储功能；</p>		

序号	货物名称	技术参数及要求	数量	单位
		14、产品具有《计算机信息系统安全专用产品销售许可证》(提供相关证书证明文件并加盖厂家公章);		
8	三层交换机	1、24 个 10/100/1000 以太网端口, 4 个 SFP 千兆位以太网端口 (Combo); 包转发速率: 216/426Mpps; 2、提供 3 年设备原厂保修服务。	1	台

本项目的核心产品：设备准入控制系统、视频用户认证服务器、视频接入认证服务器

三、★商务要求

1. 交货时间、服务地点和服务方式（履约时间、地点及方式）

- (1) 合同履行期限（交货时间）：合同签订之日起 15 天内交付。
- (2) 交货地点（履约地点）：采购人指定地点
- (3) 交货方式（履约方式）：由成交供应商免费运输至采购人指定地点。
- (4) 付款时间、方式及条件：

4.1 对于满足合同约定支付条件的，每次付款前成交供应商须向采购人提供合法、有效的发票，采购人收到发票后通过银行转账支付。

4.2 合同签订后支付合同总金额 50%作为预付款，安装调试完成通过验收后支付合同总金额 50%。

(5) 验收方法及标准：

5.1. 如成交供应商提供的货物存在质量不合格或与响应文件不相符合，采购人将拒绝验收并退货处理。

5.2 由采购人组织，供应商配合，根据对本项目采购需求响应情况及国家行业标准进行验收。

2. 其他：

- (1) 项目的实质性要求：按竞争性磋商文件要求实施。
- (2) 合同的实质性条款：采购人与成交供应商的名称和住所、标的、数量、

质量、价款或者报酬、履行期限及地点和方式、验收要求、违约责任、解决争议的方法等内容。

(3) 安全标准：符合国家、地方和行业的相关政策、法规。

(4) 质保期要求：磋商文件未明确的，按照厂家标准执行，需符合国家、地方和行业的相关政策、法规要求。

(5) 法律法规规定的强制性标准：无。

(6) 合同签订后，成交单位须在三个工作日内提供样机进行测试，如测试结果与响应文件中响应的技术指标不相符，采购人有权据此拒绝签收合同标的物，同时书面报告本级财政部门。

注：本章带“★”的要求（含小项）为实质性要求，供应商响应为负偏离的视为无效响应。